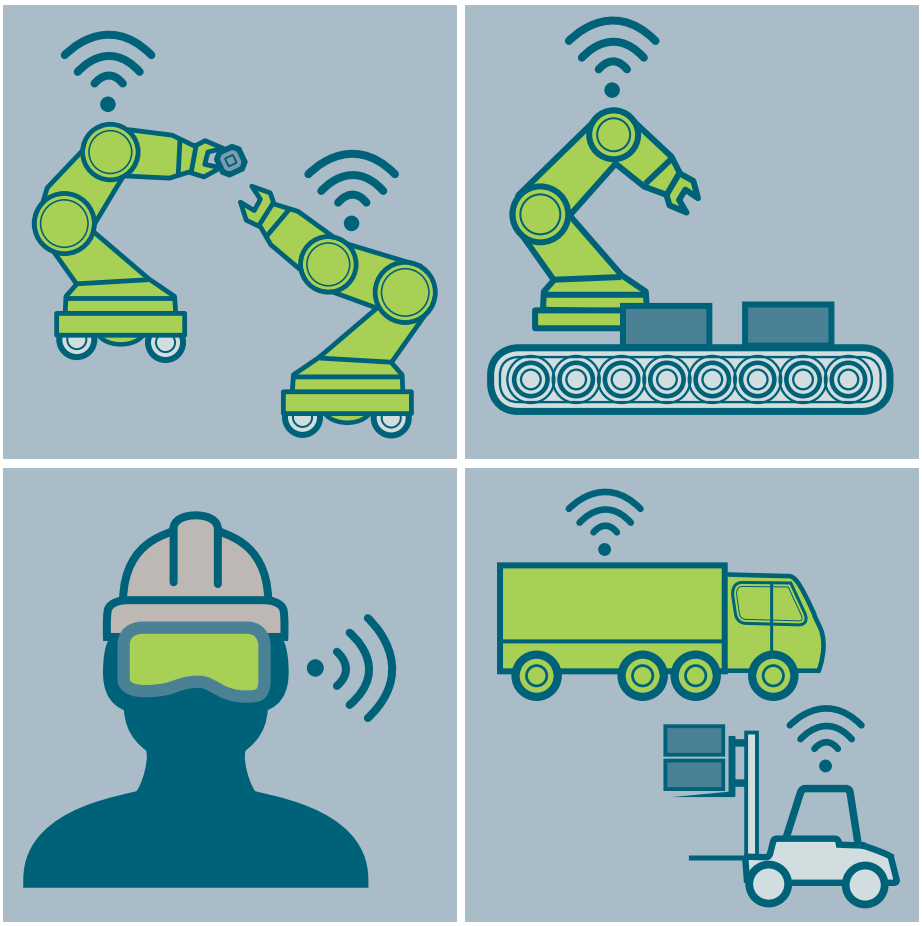
5G ACIA
5G Alliance for Connected Industries and Automation

White Paper

# 5G for Automation in Industry

## Primary use cases, functions and service requirements



July 2019

5G Alliance for Connected Industries and Automation


**5G for Automation in Industry**

Contact:
Email: info@5g-acia.org
www.5g-acia.org

Published by:
ZVEI – German Electrical and
Electronic Manufacturers' Association
5G Alliance for Connected Industries and Automation
(5G-ACIA), a Working Party of ZVEI
Lyoner Strasse 9
60528 Frankfurt am Main, Germany

www.zvei.org

July 2019

Graphics: ZVEI

# Contents

# 1 Introduction

This white paper examines how the 3GPP-defined 5G architecture will impact industry, in particular process and discrete manufacturing. It describes the most relevant use cases, and the corresponding 5G functions and service requirements. It is consciously an overview, and does not aspire to be fully comprehensive, for instance spectrum aspects are out of scope. Spectrum aspects are discussed in 5G-ACIA "5G for Connected Industries and Automation" white paper [10].

Consideration is primarily given to the needs of automation and robotics. These themes are naturally closely related to the fourth industrial revolution (also known as Industry 4.0), and the Industrial Internet of Things (IIoT).

This paper is intended to give ICT professionals a high-level overview of relevant 3GPP-supported operational technology (OT) use cases. Furthermore, it is designed to give OT companies (i.e. those companies in industry who will deploy 5G) high-level guidance on what is supported by the 3GPP-defined architecture, and to provide references where they can find more detailed information.

The main 3GPP technical reports (TR) related to industrial use cases are as follows:

- Study on Communication for Automation in Vertical Domains (FS_CAV) in TR 22.804,
- Feasibility Study on Business Role Models for Network Slicing (FS_BMNS) in TR 22.830 and
- Feasibility Study on LAN Support in 5G (FS_5GLAN) in TR 22.821.

These TRs are not normative (i.e. they are not prescriptive and they are non-binding). They cannot be used as the basis for implementation, and they cannot be referred to by 3GPP technical specifications (TS).

It should be noted that 3GPP often employs the term "vertical domain", i.e. a particular industry or group of enterprises in which similar products or services are developed, produced, and provided.

The TRs were primarily written by 3GPP to understand and summarize the high-level communication needs of the industrial community – which have since been described in the following normative and binding technical specifications (TS):

- Service requirements for cyber-physical control applications in vertical domains, TS 22.104 and
- Service requirements for the 5G system, TS 22.261.

Once finalized ("frozen"), the TRs given above are not updated. However, TSs are updated as the need arises. As a result, it is possible for the content of a TS to diverge increasingly from that of a TR over time. This should be taken into account when making references to any 3GPP TR/TS.

The functionality described in this white paper is proposed for implementation in 3GPP Rel-16 specifications, currently scheduled for completion in 2020.

# 2 3GPP

The 3rd Generation Partnership Project (3GPP) is a collaborative project that brings together standardization organizations from around the world to create globally acceptable specifications for mobile networks.

As its name implies, it was first created to establish such specifications for the third generation (3G) of mobile systems. It has continued its work for subsequent generations, including the one considered here, the fifth generation (5G).

# 3 5G-ACIA

The 5G Alliance for Connected Industries and Automation (5G-ACIA) was established to serve as the central and global forum for addressing, discussing, and evaluating relevant technical, regulatory, and business aspects with respect to 5G for the industrial domain. It reflects the entire ecosystem and all relevant stakeholder groups, ranging from operating industry (OT) players (industrial automation companies, engineering companies, production system manufacturers, end users, etc.), the ICT industry (chip manufacturers, network infrastructure vendors, mobile network operators, etc.), academia and other groups.

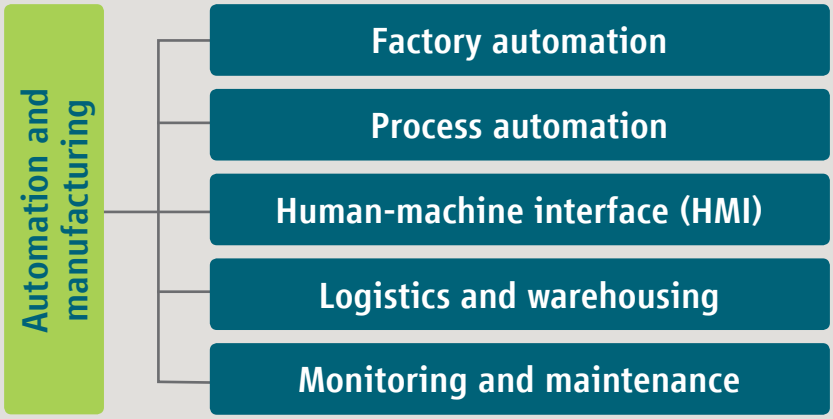
The paramount objective of 5G-ACIA is to ensure the best possible applicability of 5G technology and 5G networks for connected industries, particularly discrete manufacturing and the process industry. 5G-ACIA's mission is to ensure that the interests and needs of the industrial domain are adequately considered in 5G standardization and regulation. 5G-ACIA will further ensure that ongoing 5G developments are understood by and effectively transferred to the industrial domain.

# 4 Areas of application and use cases for automation in manufacturing

Manufacturing is diverse and heterogeneous, and is characterized by a large number of automation use cases. These can be divided into five distinct areas of application, as depicted in Figure 1:

1. Factory automation,
2. Process automation,
3. Human-machine interfaces (HMIs) and production IT,
4. Logistics and warehousing, and
5. Monitoring and predictive maintenance.

**Fig. 1: Automation areas in manufacturing**




Source: 5G-ACIA/ZVEI

Factory automation comprises the automated control, monitoring and optimization of processes and workflows within a factory. This includes closed-loop control applications (e.g. based on programmable logic or motion controllers), robotics, and aspects of computer-integrated manufacturing.

Example use cases (as described in [1]) for factory automation include motion control, control-to-control, mobile robots and massive wireless sensor networks. Communication services for factory automation need to fulfill stringent requirements, especially in terms of latency, communication service availability and determinism. Operation is limited to a relatively small service area, and typically no interaction is required with the public network (e.g. for service continuity, roaming, etc.).

Process automation refers to the control of production and handling of substances such as chemicals, foodstuffs and beverages, etc. The aim of automation is to streamline production processes, lower energy consumption and improve safety. Sensors measuring process parameters, such as pressures or temperatures, operate in a closed loop by means of central and/or local controllers in conjunction with actuators, e.g. valves, pumps, heaters, etc. A process-automated manufacturing facility may range in size from a few 100 $m^2$ to several $km^2$, or may be geographically dispersed within a specific region.

Example use cases [1] for process automation include mobile robots, massive wireless sensor networks, closed-loop process control, process monitoring and plant asset management. Communication services for process automation need to meet stringent requirements. For instance, low latency and determinism are crucial for closed-loop control. Interaction may be required with the public network (e.g. for service continuity, roaming, etc.).

Human-machine interfaces (HMIs) include many diverse devices for interaction between people and production systems. These can be panels mounted to a machine or production line, as well as standard IT devices, such as laptops, tablet PCs, smartphones, etc. In addition, augmented and virtual reality (AR/VR) systems are expected to play an increasingly important role in the future.

Production IT, on the other hand, encompasses IT-based applications, such as manufacturing execution systems (MES) and enterprise resource planning (ERP) systems. The primary

goal of an MES is to monitor and document how raw materials and/or basic components are converted into finished goods. An ERP system, by contrast, generally provides an integrated and continuously updated view of business processes. Both systems depend on the timely availability of large volumes of data from the production process.

Example use cases [1] for HMIs and production IT include mobile control panels and augmented reality systems. Communication services for HMIs and production IT need to meet stringent requirements. For example, very low latency is imperative for some use cases. Most HMI and production IT use cases are limited to a local service area, and typically no interaction is required with the public network (e.g. for service continuity, roaming, etc.).

Logistics and warehousing refers to the organization and control of the flow and storage of materials and goods in the context of industrial production. Intralogistics is logistics on a defined premises, for example to ensure the uninterrupted supply of raw materials to the factory floor by means of automated guided vehicles (AGVs), forklift trucks, etc. Warehousing refers to the storage of materials and goods, for example employing conveyors, cranes, and automated storage and retrieval systems. For practically all logistics use cases, the positioning, tracking and monitoring of assets are of high importance.

Example use cases [1] for logistics and warehousing include control-to-control and mobile robots. Communication services for logistics and warehousing need to meet very stringent requirements in terms of latency, communication service availability and determinism, and are limited to a local service area (both indoor and outdoor). Interaction is required with the public network (e.g., for service continuity, roaming, etc.).

Monitoring and predictive maintenance refers to the monitoring of certain processes and/or assets, but without immediately impacting the processes themselves (in contrast to a typical closed-loop control system in factory automation, for example). This includes, in particular, condition monitoring and predictive maintenance based on sensor data.

Example use cases [1] include massive wireless sensor networks, and remote access and maintenance. Communication services for monitoring and predictive maintenance are limited to a local service area (both indoor and outdoor). Interaction is required with the public network (e.g. for service continuity, roaming, etc.).

The primary manufacturing-domain use cases can therefore be regrouped into the following ten categories:

1. Motion control
2. Control-to-control
3. Mobile control panels
4. Mobile robots
5. Massive wireless sensor networks
6. Remote access and maintenance
7. Augmented reality
8. Closed-loop process control
9. Process monitoring
10. Plant asset management

The following table maps the various areas of application to the use case categories.

### Table 1: Areas of application and corresponding use cases

| | Motion control | Control-to-control | Mobile control panels | Mobile robots | Massive wireless sensor networks | Remote access and maintenance | Augmented reality | Closed-loop process control | Process monitoring | Plant asset management |
|---|---|---|---|---|---|---|---|---|---|---|
| Factory automation | X | X | | X | X | | | | | |
| Process automation | | | | X | X | | | X | X | X |
| HMIs and production IT | | | X | | | | X | | | |
| Logistics and warehousing | | X | | X | | | | | | X |
| Monitoring and maintenance | | | | X | X | X | X | | | |

Source: 5G-ACIA / ZVEI

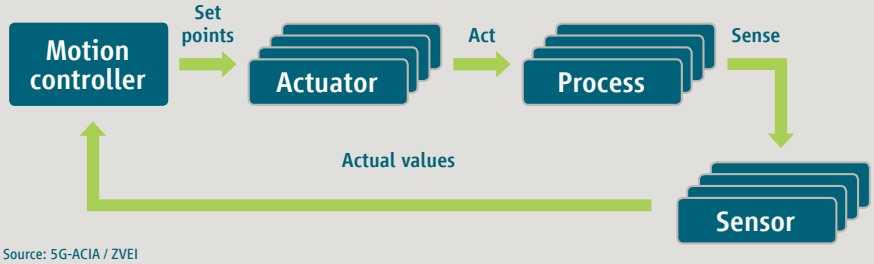
Each use case category is briefly described below, with examples.

## 4.1 Motion control

Motion control is one of the most challenging closed-loop control use cases in industry. A motion control system is responsible for controlling moving and/or rotating parts of machines in a clearly-defined way, for example for printing presses, machine tools and packaging equipment. A schematic of a motion control system is given in Figure 2. A motion controller periodically sends target set points to one or several actuators (e.g. a linear actuator or a servo drive) that then perform(s) a corresponding action for one or several processes (in this instance, generally the movement or rotation of a specific component). At the same time, sensors determine the current state of the process(es) (e.g. the current position and/or rotational position of one or multiple components) and send the actual (current) values back to the motion controller in a strictly cyclical and deterministic manner. For example, during each communication cycle, the motion controller sends updated set points to all actuators, and all sensors send their actual (current) values back to the motion controller. At present, motion control systems typically employ wired Industrial Ethernet technologies. Examples of these technologies include PROFINET IRT or EtherCAT – which support cycle times of less than 50 µs.

In general, motion control has the highest requirements in terms of latency and service availability. The service areas are usually comparatively limited in size, and no interaction with public networks is required.

### Fig. 2: Schematic of a motion control system




Source: 5G-ACIA / ZVEI

## 4.2 Control-to-control

Control-to-control (C2C) communication is between industrial controllers (e.g. programmable logic controllers or motion controllers). It is already established for a number of use cases, such as:

- Large items of equipment (e.g. newspaper printing presses), where several controllers are employed to cluster machine functions which need to communicate with each other. These controls typically need to be synchronized, and exchange real-time data. In general, this use case has very stringent requirements in terms of latency, integrity and service availability. Typically, to meet the need for low latency and high integrity, non-public networks are used.
- Multiple individual machines performing a shared task (e.g. machines on an assembly line) and that often need to communicate with each other, i.e. to control and coordinate the handover of components from one machine to another.

Protocols for today's C2C communication include Industrial Ethernet standards such as PROFINET, EtherCAT, OPC UA, and other protocols – which are often based on Fast Ethernet. C2C communication is expected to increase. In particular, there is likely to be a significant rise in the number of participating controllers in any given use case and in the volume of data being exchanged.

## 4.3 Mobile control panels

Mobile control panels are crucial to interaction between people and production equipment, and to interaction between people and mobile/portable devices. These panels are mainly used for configuring, monitoring, debugging, controlling and maintaining machines, robots, cranes or entire production lines.

In addition, (safety) control panels are typically equipped with an emergency stop button and an enabling device which an operator can activate when a dangerous situation arises in order to avoid injury to humans or damage to assets. When the emergency stop button is activated, the controlled equipment (and possibly neighboring machines) must immediately be placed in a safe, stationary position.

Similarly, with a "dead man's switch", the operator must manually keep the switch in a predefined position. If the operator, for example, inadvertently releases it, the corresponding equipment must again immediately come to rest in a safe, stationary position.

Due to the critical nature of these functions, safety control panels currently usually have a wired connection to the equipment. In a 5G radio scenario, a signal must be periodically sent – and received – in order to verify that the control panel is still connected. The verification cycle time always depends on the corresponding process/equipment. For a fast-moving robot, for example, the cycles are shorter than for a slow-moving linear actuator.

The service area is usually limited in size, as each mobile control panel is associated with a single, individual item of equipment.

## 4.4 Mobile robots

Mobile robots and mobile platforms, such as AGVs, are employed widely in diverse use cases in industrial and intralogistics environments. A mobile robot is essentially a programmable machine capable of executing multiple operations, traveling along preprogrammed routes to perform a large variety of tasks.

A mobile robot is able, for example, to move goods, materials and other objects, and can have a significant range of movement within a given industrial environment. Mobile robot systems are able to perceive their surroundings, i.e. they can sense and react to their environment.

AGVs are a sub-group within the mobile robot category. AGVs are driverless vehicles that are steered automatically. They are employed to efficiently move goods and materials within a defined area.

Mobile robots are monitored and controlled by a guidance control system. This control system is required to transmit real-time information to avoid collisions between robots, to assign tasks, and to manage robot traffic. The mobile robots are track-guided by means of markings or wires in the floor, or guided by their own surround sensors, such as cameras or laser scanners.

Mobile robots and AGV systems must frequently interoperate with conveyor assets (cranes, lifts, conveyors, industrial trucks, etc.), and monitoring and control elements (sensors and actuators). They also need to exchange data for reporting, e.g. inventories, goods movements and throughput, for tracking and monitoring, and for forecasting. Service areas can be very large.

## 4.5 Massive wireless sensor networks

Sensor networks are designed to monitor the state or behavior of a particular environment. In the context of manufacturing, wireless sensor networks (WSN) monitor processes and equipment, and the corresponding parameters. This environment is typically monitored using diverse sensor types, such as microphones, $CO_2$ sensors, pressure sensors, humidity sensors, and thermometers. These sensors together typically form a distributed monitoring system.

The data captured in this way is leveraged to monitor diverse parameters, for example to detect anomalies.

5G has the potential to take these networks to the next level: massive machine-type communication (mMTC) will enable massive wireless sensor networks, featuring millions of devices per square kilometer, i.e. of a size and density far beyond today's wireless sensor networks.

Wireless sensor networks are highly dynamic in nature, changing significantly over time in terms of the type, number and position of sensors deployed. The position of sensors may be constrained by the available wireless sensor network hardware. Given that sensors are typically relatively simple devices, the corresponding functionality usually needs to be modeled in a centralized computing infrastructure. In certain instances, functionality may be supported within or shared with the sensor network.

In many scenarios, it is necessary to lay expensive cables to supply electrical power to sensors. Alternatively, the sensors are battery powered. In this latter instance, batteries must be capable of reliably supporting sensor operation, including the communication module, for extended periods, even years.

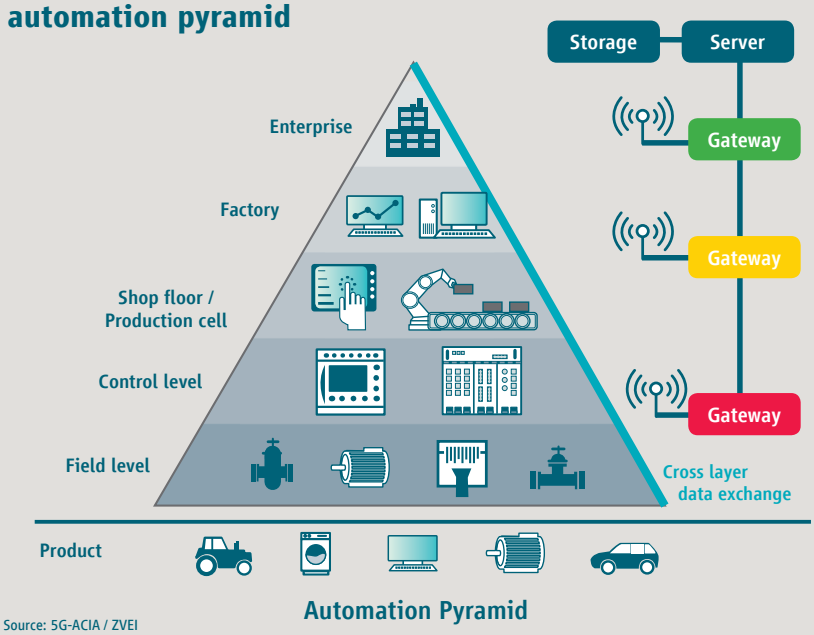
## 4.6 Remote access and maintenance

Remote access is the ability to establish contact and communicate with a device from a distant location, and this is often the means for performing remote maintenance. Although industrial networks are isolated from the internet, remote access is already possible, i.e. via peer-to-peer communication links between just two devices, fieldbuses with multiple devices and controllers, LANs or WLANs. However, this requires gateway functionality.
Remote access to device data requires mapping of data formats, addresses, coding, units, and status at each transition in the automation pyramid (see Figure 3). This can entail significant engineering effort. Moreover, data mapping implemented in the gateway(s) is relatively static.

An example use case is the inventorization of devices and periodic extraction of configuration data, event logs, version data, and predictive maintenance information. Generically, this is known as asset management, and tools for collecting and displaying data from multiple connected devices are called asset monitors.

A system of this type might operate autonomously (a set of configured periodic checks) or interact with a user ("show me the status of this device"). The remote diagnostics system might be operated by, for instance, a manufacturer for devices deployed in its factory. Or the system might be operated by the device vendor as a service for its customer(s).

**Fig. 3: Remote access to devices in existing systems through controllers via gateways at each transition point of the automation pyramid**




Source: 5G-ACIA / ZVEI

## 4.7 Augmented reality

Augmented reality (AR) is a technology that allows a computer-generated image to be superimposed on a user's view of the physical world, providing a composite view.

People will continue to play an important and substantial role in production. But factory-floor workers, for instance, need effective support, i.e. assistance that allows them to rapidly become familiar with and adept at new tasks, and that ensures they can work in an efficient, productive and ergonomic manner.

In this respect, head-mounted AR devices with see-through displays are especially attractive since they enable maximum ergonomics, flexibility and mobility, leaving the hands of workers free. However, if AR devices are worn for prolonged periods (e.g. an entire work shift), they need to be lightweight and highly energy-efficient. One way to achieve this is to offload complex processing tasks to the network (e.g. an edge cloud).

AR is expected to play a crucial role in the following use cases:

- Monitoring of processes and production flows
- Delivery of step-by-step instructions for specific tasks, for example for manual assembly
- Ad hoc support from a remote expert, for example for maintenance or service tasks

## 4.8 Closed-loop process control

With closed-loop process control, multiple sensors are installed in a production facility, and each sensor performs continuous measurements. The sensor-captured data are transferred to a controller which then decides whether and how to operate actuators. Latency and determinism are crucial.

In closed-loop process control, sensors distributed throughout the production facility continuously measure typical process parameters such as pressure, temperature, flowrate or pH value. Harnessing the sensor-captured data, the controllers operate actuators such as valves, pumps, and heaters/coolers to manage the production process in an optimized, safe and reliable way.

In these scenarios, determinism and availability are essential as these processes run continuously over extended periods.

## 4.9 Process monitoring

With process monitoring, multiple sensors are installed in a production facility to grant visibility into process or environmental conditions, or into inventories. Data are transmitted to displays for observation and/or to databases for logging and trend monitoring. The communication service must support high sensor density, and provide low latency and high service availability. In addition, any battery-driven sensors, including the communication module, must be highly energy-efficient.

## 4.10 Plant asset management

To keep a plant up and running, it is essential that assets such as pumps, valves, heaters, instruments, etc., are well maintained. Timely recognition of any degradation, and ongoing self-diagnosis, are used to support and plan maintenance work. This calls for sensors that provide visibility into process or environmental conditions.

Remote software updates modify and enhance components in line with changing conditions and advances in technology.

In plant asset use cases, positioning is an essential requirement. Latency and service availability are also requirements, but they are less critical than positioning.

# 5 Primary functions provided by 5G for factory and process automation

The primary functions provided by 5G for factory and process automation are summarized in Table 2. In the following sections we will describe those functions in detail.

### Table 2: Primary functions provided by 5G for factory and process automation

| Functionality | Type/ Component | Examples |
|---|---|---|
| Quality of service | Data traffic | • Periodic deterministic communication<br>• Aperiodic deterministic communication<br>• Non-deterministic communication<br>• Mixed traffic |
| | End-to-end latency | 0.5 ms to 500 ms |
| | Data rate | Up to several Gbit/s |
| | Time synchronicity | Down to 1 µs |
| Dependability | Communication service availability | Varies from 99.9 % to 99.999999 % |
| | Communication service reliability | Varies from 1 day to 10 years |
| Deployment | Non-public networks | Standalone: NPN and PLMN are deployed on separate network infrastructure<br>Hosted: NPN is hosted completely or in part on PLMN infrastructure<br>Integrated: NPN 5G network is integrated into a larger non-3GPP communication network such as an IEEE 802 based network |
| | Slicing and isolation | Based on a physical network that might be operated by a public operator or an enterprise 5G provides the means to run multiple virtual networks (called slices) for different communication purposes. 5G allows to run those slices independently and if desired, isolated from each other. |
| Interworking | Seamless integration | 5G can be integrated with wired technologies on the same machine or production line |
| | Service continuity between non-public and public 5G networks | 5G supports mobility between a 5G core network and an evolved packet core (EPC, the 4G core network) |
| Security | Availability | 20 years |
| | Integrity | Data received not tampered with and was transmitted by the sender |
| | Confidentiality | Optimizing and minimizing signaling overhead, particularly for small packet data transmissions<br>In-network caching and operating servers closer to the network edge |
| Positioning | | Between 0.2 m and 10 m |
| Efficiency | Spectrum, battery (power) and protocol efficiency | |
| Operation and maintenance | | • Fault management<br>• Configuration management, including provisioning and lifecycle management<br>• Accounting, including online and offline charging<br>• Performance management, including the definition of key performance indicators (KPIs)<br>• Security management |

Source: 5G-ACIA / ZVEI

## 5.1 Quality of service (QoS) for 5G communication services

For 3GPP, quality of service (QoS, known as communication service performance) comprises four parameters: communication service availability, communication service reliability, end-to-end latency, and user-experienced data rate. These are regarded as core 5G requirements (termed characteristic parameters by 3GPP).

3GPP also defines six secondary requirements (known as influence quantities or parameters): message size, transfer interval, survival time, user equipment (UE) speed, number of UEs, and service area.

3GPP has defined multiple key performance indicators (KPIs) for all the above parameters, reflecting the specific needs of various use cases.

3GPP also describes further requirements, such as timeliness, positioning and time synchronicity, again with corresponding KPIs.

All the above KPIs are given in TS 22.104 [2], which is specific to factory and process automation services.

In addition to KPI-defined requirements, 3GPP has described some general QoS service requirements in TS 22.261 [3] to help 5G support flexible service deployments. This specification is applicable to all communication services, including those in factory and process automation.

## 5.2 Data traffic characteristics

Due to the multitude of use cases, 3GPP has grouped and categorized certain traffic types based on similar KPIs. 3GPP has so far defined four traffic classes for factory and process automation. Each traffic class has a specific set of KPIs:

- Periodic deterministic communication: this has stringent requirements in terms of communication service timeliness and availability. For this kind of traffic, 3GPP has defined KPIs for some key characteristic parameters, such as
  - communication service availability,
  - communication service reliability measured as mean time between failures,
  - maximum end-to-end latency,
  - service bit rate/user experienced data rate, and
  - time synchronicity.

It has also defined influence parameters associated with these KPIs, such as
- message size,
- periodic transfer interval,
- survival time,
- user equipment (UE) speed,
- number of active UEs, and
- service area.

- Aperiodic deterministic communication: without a pre-set sending time, but still with stringent requirements in terms of communication service timeliness and availability. For this kind of traffic, 3GPP has defined KPIs for some key characteristic parameters, such as

- communication service availability,
- communication service reliability measured as mean time between failures,
- maximum end-to-end latency, and
- service bit rate/user experienced data rate.

3GPP has also defined influence parameters associated with these KPIs, such as

- message size,
- periodic transfer interval,
- survival time,
- UE speed,
- number of active UEs, and
- service area.

- Non-deterministic communication: this comprises all traffic types other than periodic/aperiodic deterministic communication. This includes periodic/aperiodic non-real-time traffic. For this kind of traffic, 3GPP has defined KPIs for some key characteristic parameters, such as
  - communication service reliability measured as mean time between failures, and
  - service bit rate/user experienced data rate.

It has also defined influence parameters associated with these KPIs, such as

- UE speed,
- number of active UEs, and
- service area.

- Mixed traffic: this comprises traffic that cannot be exclusively assigned to one of the other communication types. For mixed traffic, 3GPP has defined KPIs for some key characteristic parameters, such as
  - communication service reliability measured as mean time between failures, and
  - service bit rate/user experienced data rate.

And it has defined influence parameters associated with these KPIs, such as

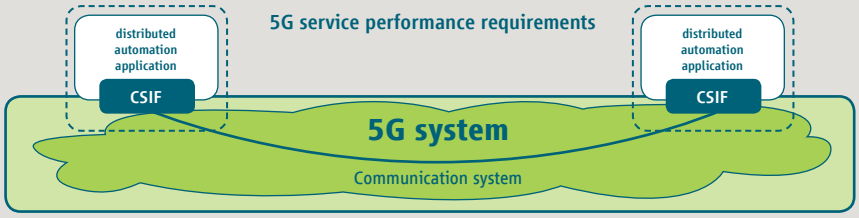
- UE speed,
- number of active UEs, and
- service area.

Taken together, these individual QoS KPIs and influence parameters allow a 5G system to support a complete solution that meets the QoS needs of factory and process automation. Certain KPIs, such as end-to-end latency, data rate, and time synchronicity, are presented below.

### 5.2.1 End-to-end latency

From the 3GPP 5G perspective, end-to-end latency is the time it takes to successfully transfer a given piece of information from a source to a destination, i.e. between the transmitting 5G communication service interface and the receiving 5G communication service interface(s), as shown in the following figure. For the purposes of this document, latency is always one-way latency rather than round-trip latency.

**Fig. 4: End-to-end latency measured between the CSIFs**




CSIF – communication service interface between distributed automation application/function and 5G system

Source: 5G-ACIA / ZVEI

In TR 22.804 [1] and TS 22.104 [2], latency generally includes only one wireless link (UE to network node or network node to UE) rather than two wireless links (UE to UE), except for certain specific use cases, such as electrical power distribution/automated switching for power isolation and restoration.

In the latest TR 22.804 [1] and TS 22.104 [2], the lowest maximum latency requirement for deterministic communication service is defined as 0.5 ms for small industrial environments (50 m x 10 m x 10 m) with small packet sizes for motion control. A higher maximum latency of 500 ms is given for periodic communication for standard mobile robot operation and communication services for CCTV surveillance cameras in mass rail transit with defined speeds of movement for each UE (UE speed < 50 km/h for mobile robots and ≤ 160 km/h in urban environments).

In a 3GPP-defined 5G system, if the packet is not delivered within the defined window (maximum latency), the packet is considered lost. Within this window, network layer packets may be retransmitted one or multiple times in order to meet the defined reliability requirement.

### 5.2.2 Data rate

TS 22.261 [3] describes 5G requirements from the user perspective, in particular the user experienced data rate: this is generally given as the minimum data rate required to achieve a user experience of sufficient quality, with the exception of broadcast-type services, where the value given is a maximum.

TR 22.804 [1] and TS 22.104 [2] define/specify the service bit rate. The rate is defined slightly differently for the various traffic classes:

#### a) Deterministic communication

For deterministic communication, 3GPP defines the user experienced data rate as the committed data rate requested by the communication service. In TS 22.104 [2], the highest data rate requirement for deterministic traffic is given as 10 Mbit/s for mobile robots with video streaming.

#### b) Non-deterministic communication

For non-deterministic communication, the rate at which data is transmitted must not fall below a defined lower limit. This is the required user experienced data rate. The highest data rate for non-deterministic traffic is given as 1 Gbit/s for communication between mechanically coupled train segments.

### 5.2.3 Time synchronicity

Time synchronization is important for many factory and process use cases as well as for the 5G network itself. Time synchronicity requirements are given in TR 22.804 [1] and TS 22.104 [2] section 5.6. Fulfillment of these requirements is the basis for processing and transmitting data in accordance with IEEE 1588v2 (Precision Time Protocol), and for implementing mechanisms to synchronize user-specific time clocks of UEs with a global clock and/or a working clock. To account for the complexity of the real-world factory floor, 5G supports up to 32 working clock domains.

TS 22.104 [2] describes three time synchronicity requirements for factory and process automation. The most stringent requirement is < 1 µs for motion control (up to 300 UEs in a service area of ≤ 100 m x 100 m) and smart grid power distribution/power management unit (PMU) synchronization (up to 100 UEs in a service area of < 20 $km^2$). The latter use case is extremely challenging, and it is probable that 3GPP will have to consider complementary non-3GPP technologies to achieve this degree of wide area synchronization.

## 5.3 Dependability

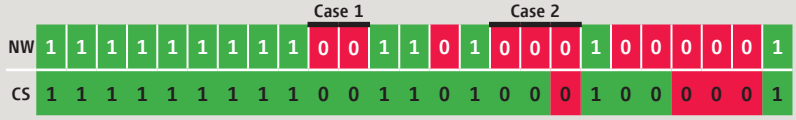
Dependability encompasses availability, reliability, maintainability, safety, integrity, and assurance. These parameters apply to logical connections (rather than physical). They are explained in detail in section 4.3 of TR 22.804 [1]. A brief overview is given here.

### 5.3.1 Communication service availability

Availability is described as the "ability to be in a state to perform as required" [9] or readiness for correct operation. In [7], two detailed definitions are given: network availability and communication service availability. Communication service availability (CSA) is given in the requirement tables and the QoS tables in TS 22.104 [2]. CSA is based on the values for service uptime and downtime. An additional parameter required to calculate CSA is survival time. 3GPP defines CSA as the "percentage value of the amount of time the end-to-end communication service is delivered according to an agreed QoS, divided by the amount of time the system is expected to deliver the end-to-end service according to the specification in a specific area."

A detailed description of this relationship can be found in Annex A in TR 22.804 [1] and Annex C in TS 22.104 [2]. An example for periodic communication is given in Figure 5. Messages must be sent within a given transfer interval. A figure one in a green field indicates the message has been correctly received. A figure zero in a red field indicates that the message has been incorrectly received or lost. The example is for a survival time of two times the transfer interval. This means if two messages in sequence (case 1) are incorrectly received or lost within the network (NW) and the following message is correct, the communication service is still considered available. If three messages (case 2) or more in a sequence are incorrect or lost before receipt of the next correct message, the communication service is considered unavailable. According to 3GPP's definition, the CSA percentage can be calculated over longer periods of time to assess the overall quality of the connection.

**Fig. 5: Comparison of network (NW) and communication service (CS) availability depending on consecutively lost messages**




Source: 5G-ACIA / ZVEI

### 5.3.2 Communication service reliability

Reliability is the "ability to perform as required, without failure, for a given time interval, under given conditions" [9] or, in other words, continuity of correct operation. Communication service reliability (CSR) is the mean time between failures (MTBF), calculated using the cumulative value for time between failures (example values are given in TS 22.104 [2]). It is important to note the differing definitions for reliability in the context of dependable communication and in the context of TS 22.261 [3], which defines reliability as a correctly received packet ratio expressed as a percentage. TS 22.104 [2] section 5 describes the relationship between communication service availability and reliability of [7].

A message consists of several packets. Without taking any corrective measures in case of packet errors, the correctly received message ratio would be lower than or equal to the correctly received packet ratio. Due to correction mechanisms applied (e.g. repetition of packet or forward error correction) the correctly received message ratio can be higher than the correctly received packet ratio.

### 5.3.3 Dependability and assurance

When measuring dependability, QoS has a key role to play. Four types of value are classified in TS 22.261 [3] for each parameter (e.g. CSA, CSR, lost message ratio): required value, offered value, achieved value, and perceived value. It is important to identify the interface where each value is measured.

- The required value is defined by the communication service user.
- The network operator (communication service provider) defines the offered value.
- The achieved value is obtained by measurements made by the network operator during system operation.
- The perceived values are obtained by measurements made by the service user during system operation.

The achieved value and the perceived value should be the same, as they are measured at the same interface. An example for CSA and mean time between failures is given in Table 3.

**Table 3: Example of the four types of values for communication service availability and MTBF**

| | Required value | Offered value | Achieved value | Perceived value | Unit |
|---|---|---|---|---|---|
| Communication service availability | 95 | 95 | 98.38 | 98.38 | % |
| Mean time between failures | 30 | 30 | 45.25 | 45.25 | days |

Source: 5G-ACIA / ZVEI

## 5.4 Deployment

### 5.4.1 Non-public networks

In contrast to a public land mobile network (PLMN) that offers mobile network services to the general public, a 5G non-public network (NPN, also sometimes informally called a private network) provides 5G mobile network services to a clearly defined user organization or group of organizations. This organization – also called a vertical domain – deploys the 5G non-public network on its premises, such as the factory floor, an industrial plant, or for its installed devices (e.g. within a smart grid).

The user organization administers the non-public network itself; the network can be operated by the user organization itself, or by a contracted service provider.

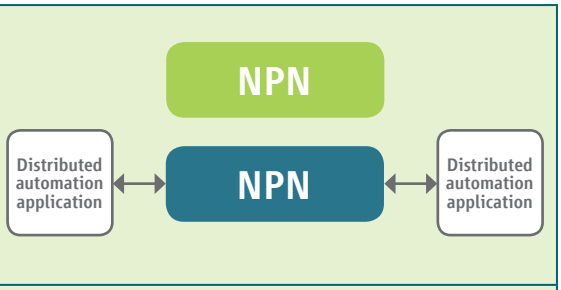
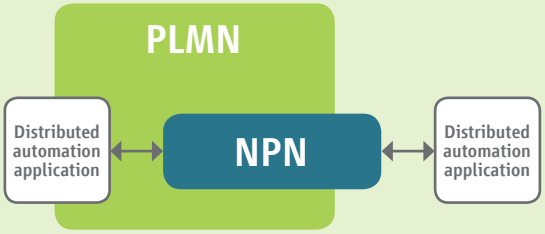
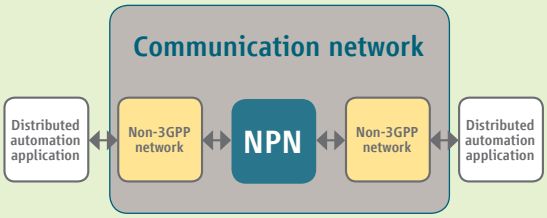
For vertical domains, non-public networks can be desirable for several reasons:

- High QoS requirements: Communication services for automation in industrial networks are associated with high QoS requirements, especially in terms of availability and latency. These cannot be satisfied by the public mobile network. It is very probable that other public-network communication services, such as voice calls, video and internet traffic, with their much lower QoS requirements, would negatively impact the vertical communication services used for automation.
- Dedicated security credentials: Industrial communication networks need security credentials that are different from those used in public networks. The same credentials are often used for both device authorization and communication encryption. For some industrial use cases, the credentials are subject to regulation.
- Isolation from other networks: The industrial communication network needs to be isolated from the public mobile network for reasons of performance, (data) security, privacy, and safety.
- Accountability: A non-public network supports efficient maintenance and operation of industrial communication and responsibility for availability.

A number of industrial use cases (mentioned in section 4) require service continuity across and between the NPN and the PLMN. This might, in certain instances, necessitate roaming between the NPN and PLMN. It is important to note that service continuity when interoperating with public networks requires security credentials for and the agreement of the public network for the corresponding user devices.

Three deployment scenario categories for non-public networks have evolved: standalone, hosted, and integrated [16]. Table 4 shows the three categories according to [16].

## Table 4: Deployment scenario categories for non-public networks according to [16]

| | |
|---|---|
| **Standalone:**<br>NPN and PLMN are deployed on separate network infrastructure. |  |
| **Hosted:**<br>NPN is hosted completely or in part on PLMN infrastructure, implemented by means of e.g. software, policies and/or network slicing (private slice). |  |
| **Integrated:**<br>NPN 5G network is integrated into a larger non-3GPP communication network. The NPN 5G network is a subset of the communication infrastructure. The NPN 5G network provides, for instance, wireless links. |  |

Source: 5G-ACIA / ZVEI

Many of the vertical use cases given in TR 22.804 [1] assume the deployment of non-public networks for the above-mentioned reasons. This is also true for the manufacturing use cases described in section 4. Normative 5G service requirements for non-public networks are given in section 6.25 of TS 22.261 [3].

### 5.4.2 Slicing and isolation

Network slicing is one of the key features of 5G. It allows the network operator to provide customized networks for specific services, and to achieve varying degrees of isolation between the various service traffic types and the network functions associated with those services.

For example, within a single network infrastructure, there may be diverse needs in terms of functionality (e.g. priority, charging, policy control, security, and mobility), in performance (e.g. latency, mobility, availability, reliability and data rates), or operational requirements (e.g. monitoring, root cause analysis, etc.).

Moreover, the slices can be configured to serve specific user organizations (e.g. public safety agencies, corporate customers, roamers).

A network slice can deliver the functionality of a full-fledged network, including radio access network and core network functions (potentially from multiple network equipment vendors). One network can support one or several network slices.

Network slicing also opens up new ways of isolating and separating data traffic types, e.g. in a factory. Moreover, slicing can be employed to isolate the various logical networks, as mandated by IEC 62443 [17].

According to 3GPP, each item of 5G user equipment is able to support up to eight slices for multiple logical networks carrying diverse data types e.g. transferring monitoring data to an MES via OPC UA, and at the same time supporting Industrial Ethernet traffic for the control of devices by a PLC.

3GPP TS 22.261 [3] section 6.1 describes some basic service requirements that 5G must fulfill to enable network slicing:

- Network slicing management by the operator, i.e. creating, scaling, modifying, configuring, deleting slices;
- UE management for the network slice,
- Traffic isolation and network resource management within and between network slices,
- Roaming, and
- Cross-network slice coordination.

5G is an enabler of new business models. There is therefore strong interest from verticals, such as the factory and process automation industry, in leveraging network slicing to allow new business relationships between mobile network operators (MNOs) and OTs. 3GPP TR 22.830 [5] addresses these relationships and the corresponding requirements.

TR 22.830 [5] considers a number of potential new business models, and these will be used as the basis for further work. There are four potential business models:

- Model a: the MNO provides the virtual/physical infrastructure and virtual network functions; a third party uses the functionality provided by the MNO,
- Model b: the MNO provides the virtual/physical infrastructure and virtual network functions; a third party manages some virtual network functions via APIs exposed by the MNO,
- Model c: the MNO provides the virtual/physical infrastructure; a third party provides some of the virtual network functions,
- Model d: a third party provides and manages some of the virtual/physical infrastructure and virtual network functions.

To facilitate these models, 5G supports the following [3]:

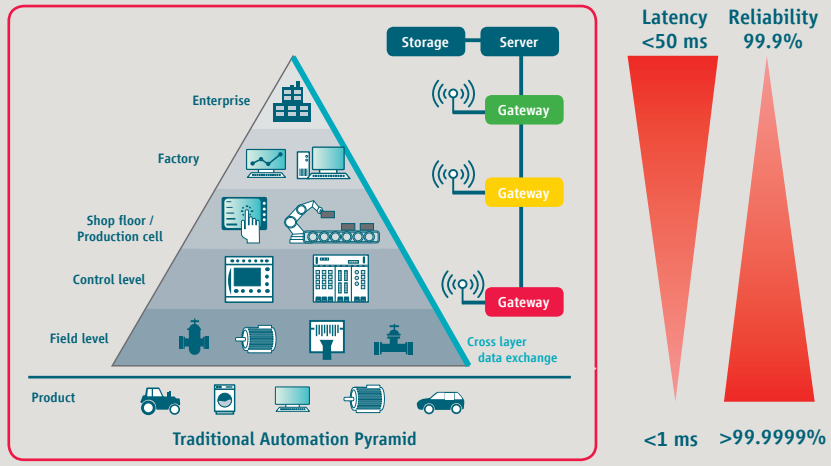
- Hosting of private slices by an MNO for a defined user organization, e.g. an OT
- Network openness (APIs) to expose network capabilities to and enable management by the user organization within its slice(s)
- Enhanced security, including authentication and authorization, for non-public networks and private slices hosted by MNOs.

## 5.5 Interworking

### 5.5.1 Seamless integration

For most communication on the factory floor and enterprise level (see Figure 6), 5G can be employed as soon as the 5G spectrum and products are available. In current factories, all time-critical devices (e.g. controllers and field devices) have wired connections. Wireless is mainly used for non-critical services. 5G networks for wireless automation on the factory floor will support a wide variety of sensors, devices, machines, robots, actuators, and terminals. These may be directly connected to public or non-public networks and/or be connected via gateway(s).

**Fig. 6: Latency and reliability demands on TCP/IP and Ethernet traffic**



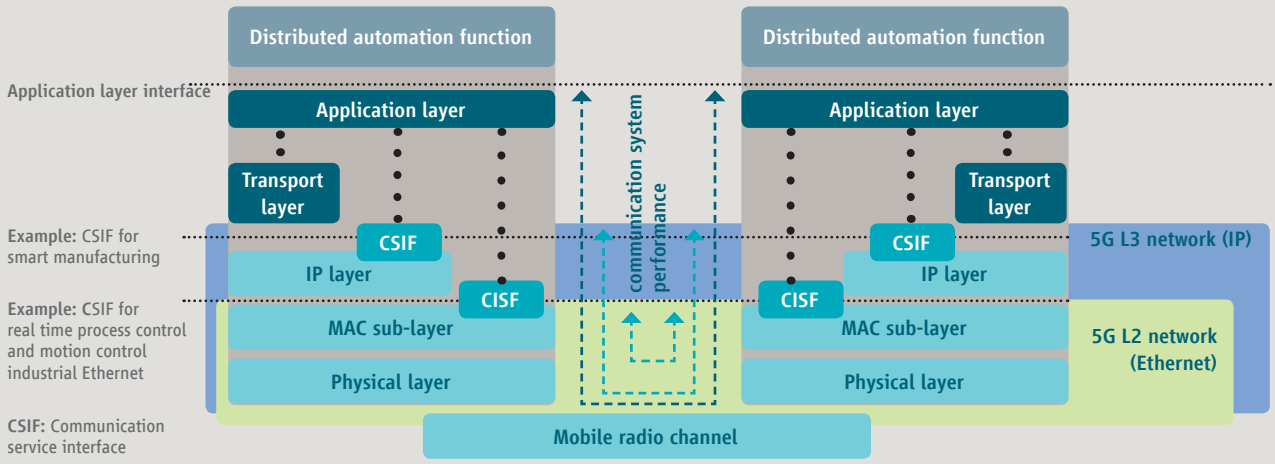

Source: 5G-ACIA / ZVEI

A number of Industrial Ethernet technologies (see IEC 61158-1 [13], IEC 61784-2 [14]) are used in industrial automation for real-time communication between controllers and machines. Compared to standard Ethernet communication, these technologies have very specialized requirements:

- Layer-2 switching (MAC, Ethertype, VLAN)
- Short cycle times, support for multiple parallel cycles
- Short data frames (e.g. encapsulated into Ethernet frames)
- High synchronization requirements
- Transfer of functional safety protocols (see IEC 61784-3 [15])
- Machine cloning in order to use the same machine type in a cell or on a line.

Today, there are also fieldbuses using various means of communication in addition to Ethernet-based industrial standards, for example Profibus (DB/PA) [13] and Foundation fieldbus H1 in the process industries. Gateways and converters will be used to interface digital signals to support successful incorporation of 5G technology into industrial networks. 5G will allow the IT and OT networks to be integrated.

## Fig. 7: Integration of 5G networks on L3 (IP) and L2 (Ethernet)




Source: 5G-ACIA / ZVEI

The IEEE Time Sensitive Networking (TSN) Task Group is developing a TSN standard with the goal of enabling the delivery of deterministic services via IEEE 802 networks. TSN provides many of the services needed in factory automation use cases, e.g., time synchronization, as well as ultra-reliability through redundancy. The aim of TSN is to support both real-time and non-real-time traffic multiplexed on Ethernet. 5G will therefore support TSN functionality. Furthermore, 5G acts as a TSN bridge, supporting seamless interworking with Industrial Ethernet and TSN-based industrial networks.

It is important to address mobility when integrating TSN and 5G wireless networks. Mobility is key to flexibility in the manufacturing process, i.e. making it possible to add certain manufacturing resources on-demand, for example by relocating a machine to the corresponding production line. This means that machines that are synchronized with divergent working clock domains may need to interact.

5G will support seamless integration into the existing (primarily wired) infrastructure. For example, 5G can be combined with wired technologies on the same machine or production line.

To support seamless integration, the 5G system will support highly deterministic cyclic data communication and guarantee bounded delays [11]. In addition, it supports seamless handover between two base stations without any observable impact on the use case, in particular with regard to safety.

There are many use cases that depend on Layer 2 Ethernet-based communication [4]. Sensors and actuators use non-IP transport services (e.g. Ethernet) to transmit control signals in legacy LANs at industrial factories. For this scenario, the 5G-LAN service supports communications between UEs via Ethernet-based protocols (i.e. non-IP packets), while ensuring the defined QoS (e.g. reliability, latency, and data rate).

### 5.5.2 Service continuity between non-public and public 5G networks

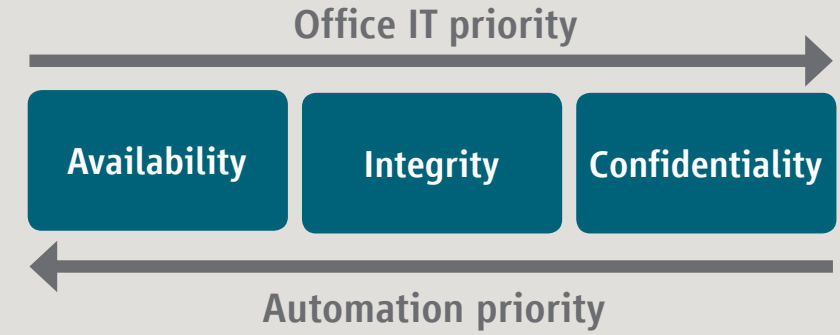
As mentioned above, 5G systems can be operated as non-public networks to allow deployment of networks within a factory or plant isolated from public mobile operator networks. Flexible interfaces allow service continuity, seamless interoperability and seamless handovers between non-public and 5G public mobile operator networks [3]. Several use cases for service continuity are described in TR 22.830 [5].

## 5.6 Security

Most security concepts and solutions were developed for office IT systems and applications. Security for automation systems in vertical domains is associated with different priorities, and with different management and operational characteristics and requirements. The following presents a bird's-eye view of the salient differences between office IT systems and automation systems.

The three key attributes of security are confidentiality, integrity, and availability (with availability meaning access to the system in question). While office IT typically prioritizes confidentiality over integrity, and integrity over availability, the complete opposite is true for automation in many vertical domains (see Figure 8).

**Fig. 8: Differences in security priorities between office IT and automation**




Source: 5G-ACIA / ZVEI

In other words, availability is the main concern for automation security, followed by integrity; confidentiality generally has the lowest priority. The real-time behaviour of automation systems can also be critical (especially for control use cases).

Automation systems not only put the emphasis on availability – this availability has to be guaranteed for component lifetimes (as much as 20 years or more) that are typically five to seven times those of components within office IT environments.

Another significant difference is the security "culture". Security patches are released and distributed in relatively long cycles in automation, in particular due to regulatory constraints. Additionally, in many industrial environments patches can only be installed during scheduled maintenance windows. Anti-virus programs are relatively rare in automation, as the virus signatures would have to be updated regularly, causing downtime. Instead, whitelisting can be employed to ensure only authorized, unmodified applications can be executed. While security testing and auditing is the norm for critical IT infrastructure such as service centers, security practices are still evolving for automation in vertical domains. A reason for this lag is that the reliable operation of the automation system must not be endangered by penetration tests.

Security standards are already well established for office IT systems, but are still under development for automation systems. However, the industrial security standard IEC 62443 [17][18] is increasingly being adopted for automation systems.

While confidentiality is generally of high importance in office environments, it is typically a low to medium priority for physically access-restricted automation systems, such as production cells in a factory. However, the confidentiality of business-relevant knowledge needs to be protected, e.g. engineering data or the parameters of a chemical production process. Integrity is essential and, as already mentioned above, so are availability and reliability. Non-repudiation may also be a high priority where the correct operation of production systems is vital, including audit-proof logs, e.g. in the pharmaceutical industry, while it is typically of medium importance for office IT.

In order to ensure the necessary security, 3GPP has taken into account relevant non-3GPP specifications, e.g. from ISO and IEC. The main security requirements are given in sections 6 and 8 in [1]. These describe the means of assuring data received have not been tampered with and were transmitted by the sender, i.e. integrity has been maintained, and the sender cannot deny having transmitted the data (non-repudiation). In addition, sections 6 in [4][5] describe special deployment scenarios, such as private networks or network slices either hosted by a traditional mobile operator, or hosted by an OT company on their own infrastructure.

## 5.7 Positioning

Highly accurate positioning is essential for factory and process automation. It is becoming increasingly important to track mobile devices and mobile assets in order to improve processes and increase flexibility in industrial environments. However, positioning requirements in these environments vary considerably.

In some instances, accuracy to within a few centimeters is needed, in others to within several meters. In some cases, maximum permissible latency can be measured in milliseconds. In others, it is sufficient to receive a few position updates each day. In general, automation and control systems typically need sub-meter accuracy. For tracking, routing and guiding, accuracy above a meter is sufficient. For certain use cases, such as AGVs and HGVs, precise positioning is crucial.

The positioning requirements from about 60 use cases (mobile control panels, autonomous driving systems, modular assembly areas, augmented reality and storage of goods) were considered in 3GPP ([1][6][20]) and were grouped into seven service levels, suitable for all positioning use cases between 20 cm and 10 m accuracy. Some of these use cases are shown in Table 5. The grouping can be found in [3], and includes horizontal and vertical accuracy, availability, latency, mobility and coverage.

## Table 5: Examples of industrial use cases with positioning performance requirements with reference to service levels (extracted from TS 22.104 [2])

| Scenario | Horizontal accuracy | Availability | Heading | Latency for position estimation of UE | UE Mobility | Corresponding Positioning Service Level in TS 22.261 |
|---|---|---|---|---|---|---|
| Augmented reality in smart factories | < 1 m | 99% | < 0.17 rad | < 15 ms | < 10 km/h | Service Level 4 |
| Mobile control panels with safety functions in smart factories (within factory danger zones) | < 1 m | 99.9% | < 0.54 rad | < 1 s | N/A | Service Level 4 |
| Inbound logistics for manufacturing (for storage of goods) | < 0.2 m | 99% | N/A | < 1 s | < 30 km/h | Service Level 7 |

Source: 5G-ACIA / ZVEI

Table 6 shows positioning service level 4 by way of an example of the seven levels defined by 3GPP.

## Table 6: Example of positioning service level 4 (extracted from TS 22.261 [3])

| Positioning service level | Absolute (A) or relative (R) Positioning | Accuracy (95 % confidence level) | | Availability | Latency | Coverage, environment of use and UE velocity | | |
|---|---|---|---|---|---|---|---|---|
| | | Horizontal Accuracy | Vertical Accuracy | | | 5G positioning service area | 5G enhanced positioning service area | |
| | | | | | | | Outdoor and tunnels | Indoor |
| 4 | A | 1 m | 2 m | 99.9 % | 15 ms | N/A | N/A | up to 30 km/h |

Source: 5G-ACIA / ZVEI

All mentioned above, such as positioning service area, enhanced positioning service area, positioning service availability and positioning service latency, are defined [3]. Note that 3GPP has also defined additional performance requirements for positioning for specific use cases. These are:

- Time-to-first-fix
- Velocity vector determination
- Energy efficiency
- Heading determination

However, a positioning service level with an accuracy of at least 10 cm, as described in the 5G-ACIA White Paper on 5G for Connected Industries and Automation [10] has not been defined yet.

## 5.8 Resource and energy efficiency

3GPP first addressed resource efficiency (comprising spectrum, battery (power) and protocol efficiency) for 5G systems in 2017 with the release of the technical specification 3GPP TS 22.261 [3]. Similarly, the industrial specification IEC 62657-1, Wireless Communication Requirements and Spectrum Considerations [8], defines the need for spectrum and energy efficiency for wireless communication in industrial automation environments at a high level.

3GPP (see section 6 in [3]) specifies resource efficiency, efficient user plane and efficient content delivery as prerequisites for various KPIs defined for 5G. Resource efficiency is achieved by optimizing and minimizing signaling overhead, particularly for small packet data transmissions. Other techniques for minimizing resource utilization include in-network caching and operating servers closer to the network edge.

Resource efficiency is always a trade-off between reliability, security and efficiency. For example, in the case of dynamic resource provisioning for industrial automation, the wireless communication system seeks to maximize reliability by making use of additional bandwidth, therefore impairing network efficiency. The 5G system minimizes security signaling overhead without compromising the security of the 3GPP system. For example, 5G supports an efficient, secure mechanism for transmitting identical data (e.g. an update for multiple sensors) to multiple UEs without sacrificing efficiency or battery life.

## 5.9 Operation and maintenance

The Telecom Management group of 3GPP is responsible for specifying the 3GPP network functional management architecture and related interfaces / APIs. For an overview of operation and maintenance in 3GPP, refer to [19].

From a network perspective, the group addresses the radio access network (RAN) and the core network (CN) for all 3GPP technologies (2G, 3G, LTE, 5G). Moreover, it considers functionality in the following areas:

- Fault management
- Configuration management, including provisioning and lifecycle management
- Accounting, including online and offline charging
- Performance management, including the definition of key performance indicators (KPIs)
- Security management

SON (self-organizing network) functions as extensions to 5G networks are currently being studied by 3GPP.

All above-mentioned management functions, including the SON functions specified by 3GPP, are invisible for any type of service/application. This means that the current specifications are also applicable to the manufacturing industry. Specific performance measurements and KPIs for these industries are expected to be specified in the future.

# 6 References


[1] 3GPP TR 22.804, Study on Communication for Automation in Vertical Domains

[2] 3GPP TS 22.104, Service requirements for cyber-physical control applications in vertical domain

[3] 3GPP TS 22.261, Service requirements for the 5G system

[4] 3GPP TR 22.821, Feasibility Study on 5G LAN Support

[5] 3GPP TR 22.830, Feasibility Study on Business Role Models for Network Slicing

[6] 3GPP TR 22.889, Study on Future Railway Mobile Communication System

[7] IEC 61907, Communication Network Dependability Engineering, 2009.

[8] IEC 62657-1, Industrial Communication Networks – Wireless Communication Networks – Part 1: Wireless Communication Requirements and Spectrum Considerations.

[9] IEC 60050, International Electrotechnical Vocabulary, Electropedia: The World's Online Electrotechnical Vocabulary, http://www.electropedia.org/

[10] 5G-ACIA, White Paper, 5G for Connected Industries and Automation, ZVEI, November 2018

[11] H. Cao, S. Gangakhedkar, A. R. Ali, K. Ganesan, M. Gharba and J. Eichinger, Use cases, requirements and challenges of 5G communication for industrial automation, IEEE ICC 2018 Workshop - The 11th International Workshop on Evolutional Technologies & Ecosystems for 5G Phase II (WDN-5G), Kansas City, MO, USA, 2018

[12] 5G for the Factory of the Future: Wireless Communication in an Industrial Environment, Florian Voigtlaender, Ali Ramadan, Josef Eichinger, Juergen Grotepass, Karthikeyan Ganesan, Federico Diez Canseco, Dirk Pensky, Alois Knoll

[13] IEC 61158-1:2014, Industrial Communication Networks - Fieldbus Specifications - Part 1: Overview and Guidance for the IEC 61158 and IEC 61784 series

[14] IEC 61784-2:2014: Industrial Communication Networks - Profiles - Part 2: Additional Fieldbus Profiles For Real-Time Networks Based on ISO/IEC 8802-3

[15] IEC 61784-3:2016: Industrial Communication Networks - Profiles - Part 3: Functional Safety Fieldbuses - General Rules and Profile Definitions

[16] 3GPP S1-183394, Description of Deployment Options for Non-Public Networks (NPN), 3GPP TSG-SA WG1 meeting #84, Spokane, WA, USA, November 2018

[17] IEC 62443-1-1, Industrial Communication Networks – Network and System Security, Edition 1.0, July 2009, ISBN 978-2-88910-710-0

[18] Orientierungsleitfaden für Hersteller zur IEC 62443, ZVEI

[19] Management, orchestration and charging in the new era https://doi.org/10.13052/jicts2245-800X.6110

[20] 3GPP  TR 3GPP TR 22.872,  Study on positioning use cases


Note: 3GPP TRs and TSs can be obtained free of charge from: http://www.3gpp.org/specifications/specifications

# 7 Abbreviations

For the purposes of this paper, the following abbreviations apply.

| | |
|---|---|
| 3GPP | 3rd Generation Partnership Project |
| 5G | 5th generation |
| 5G-ACIA | 5G Alliance for Connected Industries and Automation |
| 5GC | 5G core network |
| 5G LAN-VN | 5G LAN-virtual network |
| AGV | Automated guided vehicle |
| AR | Augmented reality |
| C2C | Control-to-control |
| CSA | Communication service availability |
| CSIF | Communication service interface |
| E2E | End-to-end |
| HMI | Human-machine interface |
| ICT | Information and communication technologies |
| IEC | International Electrotechnical Commission |
| IEV | International Electrotechnical Vocabulary |
| IoT | Internet of Things |
| IIoT | Industrial IoT |
| KPI | Key performance indicator |
| LAN | Local area network |
| MNO | Mobile network operator |
| NPN | Non-public network |
| OT | Operational technology |
| PLMN | Public land mobile network |
| PVN | Private virtual network |
| RAN | Radio access network |
| TR | Technical report |
| TS | Technical specification |
| TSN | Time-sensitive networking |
| QoS | Quality of service |
| UE | User equipment |
| VNF | Virtual network function |
| WSN | Wireless sensor network |

# 8 5G-ACIA members


5G Alliance for Connected Industries and
Automation (5G-ACIA),
a Working Party of ZVEI
Lyoner Strasse 9
60528 Frankfurt am Main, Germany
Phone: +49 69 6302-424
Fax: +49 69 6302-319
Email: info@5g-acia.org
www.5g-acia.org