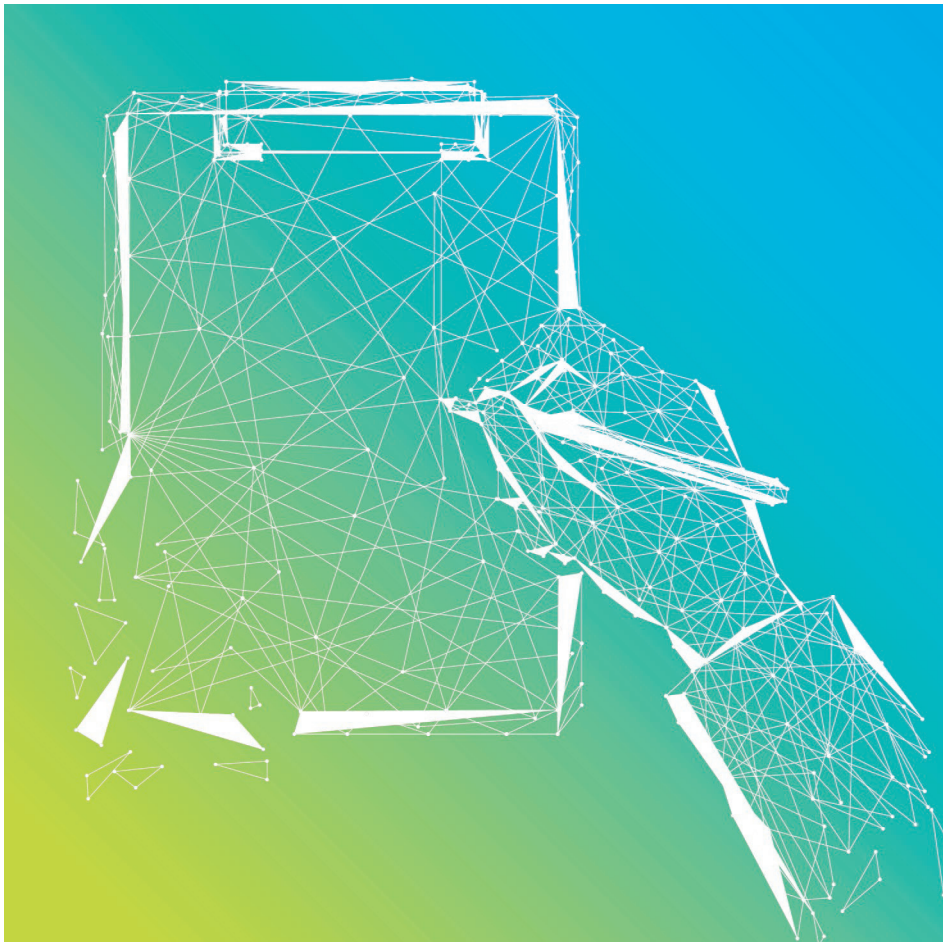
5G ACIA
5G Alliance for Connected Industries and Automation

White Paper

Key 5G Use Cases and Requirements

From the Viewpoint of Operational Technology Providers



5G Alliance for Connected Industries and Automation

5G ACIA

5G Alliance for Connected Industries and Automation

Key 5G Use Cases and Requirements

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

May 2020

Graphics: ZVEI, 3GPP, Pepperl+Fuchs

Contents

1 Introduction

3GPP's 5G specifications include multiple manufacturing and control use cases and requirements. Requirements with regard to 5G services and 5G performance are defined by the 3GPP SA1 working group in corresponding 3GPP Technical Specifications (TS) [2] [3] and are summarized by 5G-ACIA [1]. These are normative in character. 3GPP Technical Reports (TR) [5][6] describe use cases and requirements in more detail and are informative in character.

5G specifications are evolving over multiple releases, starting with Release 15. A substantial set of features supporting the use of 5G in manufacturing is available in Release 16 and expected to continue with Release 17.

The aim of this white paper is to present the industrial use cases and requirements that, from the operational technology (OT) viewpoint, are key for 5G networks.

2 3GPP

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

As its name implies, it was first created to establish such specifications for the third generation (3G) of mobile communication 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 operational technology (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.), higher education, research, and other groups.

The paramount objective of 5G-ACIA is to ensure the best possible applicability of 5G technology and 5G networks for industry, particularly discrete and process manufacturing. 5G-ACIA's mission is to make sure the interests and needs of the industrial domain are adequately considered in 5G standardization and regulation.

5G-ACIA also works to ensure that ongoing 5G developments are understood by and effectively transferred to the industrial domain.

4 Use cases

In order to identify a list of key use cases and requirements, a variety of relevant use cases, mainly drawn from TR 22.804 [5] (see [1]), were discussed, reviewed, and evaluated within 5G-ACIA. This process resulted in the following use case categories:

1. Connectivity for the factory floor
2. Seamless integration of wired and wireless components for motion control
3. Local control-to-control communication
4. Remote control-to-control communication
5. Mobile robots and automated guided vehicles (AGVs)
6. Closed-loop control for process automation
7. Remote monitoring for process automation

Some use cases on this list are described as "local" or "remote". "Local" means that a use case is restricted to a local area and is based on a 5G non-public network [4]. "Remote" denotes use cases that require a combination of (multiple) non-public and/or public 5G networks that allow remote access. For example, a distinction has to be made between communication for local machines (e.g. for machine synchronization) and for remote access (e.g. for monitoring and logging) in the instance of control-to-control communication.

As real-time (RT) requirements are very important for 5G applications, the use cases are organized into three categories:

- Non-RT: Cycle times and latency are not critical; several seconds are regarded as sufficient
- Soft RT: Cycle times and latency are moderately critical, i.e. approximately one second
- Hard RT: Cycle times and latency are highly critical, to within milliseconds or even microseconds

The key use cases can be assigned to the real-time clusters as shown in the following table:

	Use case	Category
1.	Connectivity for the factory floor	Hard RT
2.	Seamless integration of wired and wireless components for motion control	Hard RT
3.	Local control-to-control communication	Hard RT
4.	Remote control-to-control communication	Soft RT
5.	Mobile robots and AGVs	Soft RT
6.	Closed-loop control for process automation	Soft RT
7.	Remote monitoring for process automation	Non-RT

Source: 5G-ACIA

4.1 Connectivity for the factory floor

There are many fixed-position or mobile devices such as drives, robots, machines, sensors, actuators, screen terminals, and other systems that interact on the factory floor and require fast and reliable connectivity. In this context, 5G-based wireless transmission offers new opportunities and greater flexibility. Typical closed-loop control applications will run over the 5G network. On-site service engineers will be able to access the 5G network for monitoring and maintenance.

Safety is a key issue on the factory floor. If safety-relevant components communicate wirelessly, ultra-high reliability is absolutely essential and response time is an extremely important parameter.

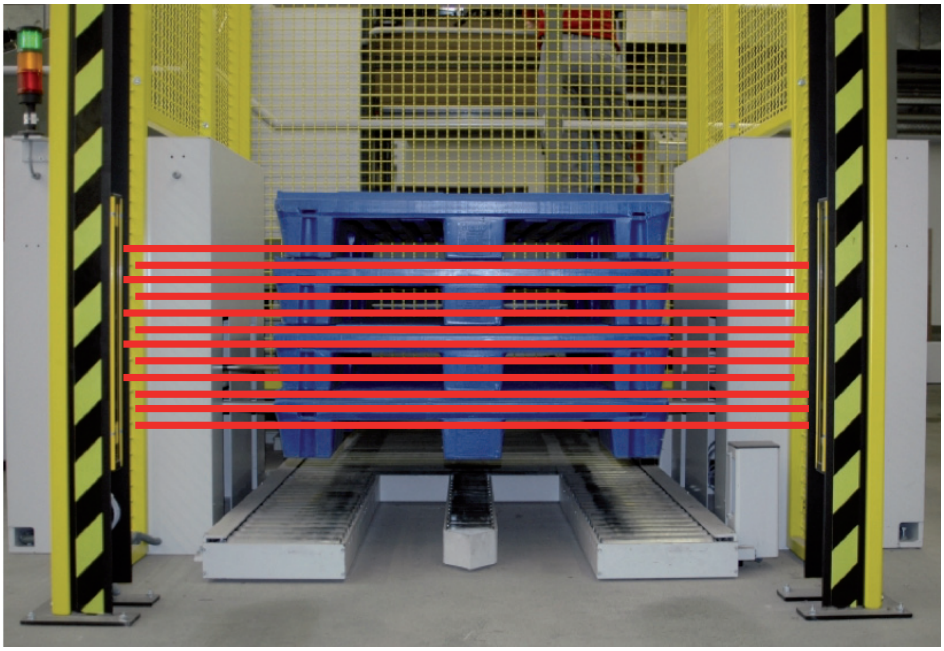
4.1.1 Example: safety light curtain

A light curtain consists of a transmitter and a receiver. The transmitter emits multiple parallel light beams towards the receiver. If one of the beams is interrupted by an object, the light curtain generates a signal. The chosen distance between light beams is determined by the smallest object requiring detection (e.g. a human finger).

Based on the methods described in EN ISO 12100 [8], a risk assessment has to be performed for each individual machine in its specific deployment scenario, not least in order to avoid injuries. This assessment must also consider additional risks and safety issues associated with degraded or lost connectivity.

Typically, a light curtain system will periodically poll safety equipment in order to elicit a response within a specified time, i.e. confirming the safety equipment is operational. The required response time for a light curtain is generally based on the specific industrial use case, e.g. the proximity of the nearest worker to a potential danger, the walking speed of the worker, and the total reaction time (sensors plus controller plus time required to halt the machine) that is needed to place the machine in a safe state.

Fig. 1: Arrangement of light beams for a safety light curtain



Source: Pepperl+Fuchs

Certain safety functions may require a response time of a maximum of 1 ms. This means that the safety mechanism needs to react within 1 ms, i.e. this is the transmission time according to [7].

If the response is delayed or not received, the machine is placed in a safe state, i.e. all drives are stopped and placed in a safe state (e.g. brakes are activated, the machine's power is cut off, etc.) and tools (e.g. a laser beam) are deactivated. Manual intervention, such as acknowledging and canceling a safety message on the operator panel, is required to make the machine operational again. Until this is done, production is halted. The costs for this interruption increase drastically when not just a single machine, but interlinked machines are impacted.

4.1.2 Example: machine layout planning

When planning the installation and layout of one or more machines on a factory floor, safety mechanisms (especially light curtains) play a crucial role with regard to defining space requirements and safety distances. In principle, the slower the reaction of a safety mechanism, the greater the distance needed between the device and the area deemed safe. A direct consequence of longer response times is a need for greater safety distances. Reliable communication with low latencies reduces space requirements.

4.2 Seamless integration of wired and wireless components for motion control

Not all devices in a motion control system, such as sensors, actuators, and drives, will be connected wirelessly. As a result, motion control systems need to integrate wired industrial communication network components with wireless 5G components. This seamless integration has to support the demanding performance requirements of motion control applications such as cycle times and microsecond latency.

4.2.1 Example: body-chassis marriage in automobile manufacturing

The process of joining the chassis and the car body (known colloquially as "marriage") in automobile manufacturing requires communication between the conveyor carrying the chassis and the conveyor carrying the body. The chassis and the body are moved closer to each other to allow them to be bolted together. These movements must be precisely controlled, as any collision will result in damage to valuable car components.

Fig. 2: Body-chassis marriage in automobile manufacturing

Source: Pepperl+Fuchs

4.3 Local control-to-control communication

Control-to-control communication is needed when devices with separate controllers interact to perform a shared task. There is a local aspect to this scenario if the devices are positioned close to one another in a single environment, e.g. they are components of a larger machine or they are multiple machines within a single production building. In these instances, communication is not based on IP, as the distances involved are relatively short.

4.3.1 Example: shuttles in a packaging machine

With many state-of-the-art packaging machines, one or more track-based shuttles convey materials inside a single machine or between multiple machines. These shuttles have local on-board controllers that can communicate their position or other control data via 5G.

As shuttle controllers interact with other devices, such as robots or machines that require the exact position of the shuttles in real time, failed or delayed transmission of the corresponding data could lead to the cessation of machine operation and therefore downtime.

4.3.2 Example: collaborative component handling

Collaborative handling of large components is an established use case in, for instance, the aviation and shipping industries. This form of handling is performed by several (two to four) remotely controlled driverless vehicles, which move along their own dedicated tracks and whose relative positions are locally controlled to minimize the force applied to the component being conveyed.

4.4 Remote control-to-control communication

Remote control-to-control communication is required for devices that normally interact autonomously with their local controller and only need remote communication occasionally (e.g. when there are changes to tasks) or for servicing/maintenance.

4.4.1 Example: remotely controlled PCB assembly lines

Printed circuit board assembly lines typically operate entirely autonomously, but can be remotely controlled to implement product changes or to capture in-process data. Communication is required between the multiple controllers for the various components/devices on the assembly line and the central control unit.

4.5 Mobile robots and AGVs

Mobile robots and autonomous guided vehicles (AGVs) add greater flexibility to industrial environments, and are being deployed ever more frequently. Wireless communication is essential for any mobile device, as wired data transmission is not an option.

4.5.1 Example: mobile robots

Common use cases for mobile robots include material handling (picking/put-away) in warehouses and at production plants. Picking robots retrieve items from various storage positions and convey them to a predetermined destination, such as a packing station or container. At production plants, mobile robots are used to retrieve products and to move them from one production step to the next.

4.5.2 Example: AGVs in a chemical plant

Extremely large AGVs are often deployed in chemical plants. They are typically remotely controlled by an operator in a control room. The operator observes images captured by cameras mounted on the AGV. The camera signals are transmitted wirelessly. The operator immediately stops the AGV if they recognize an obstacle in the AGV's path or any other malfunction. Any failure of or delay in the transmission of camera signals can potentially lead to serious accidents or, at the very least, unnecessary interruptions to the operation of the AGV.

4.6 Closed-loop control for process automation

The various interacting components within a control loop, such as sensors, actuators and control units, require fast and reliable communication. In process automation, these components are generally located in environments of greater size (area) than in discrete manufacturing.

4.6.1 Example: controlled conditions in a chemical reactor

The growing need for production efficiency and product quality calls for the precise control of manufacturing processes. Pumps, valves, heaters, coolers, stirrers and other components are monitored continuously by sensors measuring flowrates, temperature, and pressure in order to keep conditions in the reactor within tight thresholds. Long-term dependability of all components, including availability, reliability, security and confidentiality of communications, are crucial for this use case.

4.7 Remote monitoring for process automation

Remote monitoring for process automation requires communication for observation, diagnosis or monitoring, and may entail the use of public networks. Certain sub-processes (process steps) may require their own dedicated non-public networks. As a result, the overall process can only be effectively monitored by capturing information on all these individual non-public networks.

4.7.1 Example: an oil/gas field

In the oil and gas industry, items of equipment are distributed over a significant geographical area, e.g. an oil field. Data on the efficiency and operational status of wells, assets and devices are captured by corresponding sensors for remote monitoring. Availability, reliability, and communication security are important aspects for the entire communication chain. In addition, consideration must be given to battery operation in some cases due to a lack of on-site power supply.

5 Key industrial requirements

In light of the above use cases, the following technical requirements have been identified. They have been assessed from a technical point of view:

1. Reliability and availability
2. Security
3. Transmission time (latency)
4. Diagnostics
5. Network isolation

5.1 Reliability and availability

Reliability is dependent on multiple parameters, including non-susceptibility to radio interference and guaranteed connectivity in terms of both time and area (i.e. coverage). In the context of wireless communication, guaranteed connectivity is closely linked to the packet loss rate. Communication service reliability (CSR) has been defined in 3GPP TS 22.104 [2] and IEC 61907 [9] as the ability of the communication service to perform as required for a given time interval under given conditions.

Typical industrial systems need to be operated consistently and continuously – not only to achieve high efficiency and productivity, but also to guarantee high-availability, safe and uninterrupted production processes and automation. Interruption of communication – even for a very brief period – may lead to application failure/downtime for a significant period, and cause increased administrative overhead and heightened effort and expenditure for recovery.

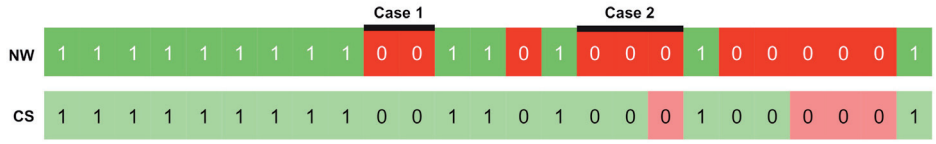
A key requirement is therefore availability of the communication service, which in turn depends on reliability of communication. Communication service availability (CSA) has been defined as the amount of time the end-to-end communication service is provided in line with the agreed quality of service (QoS), expressed as a percentage [2][3]. The reliability of the deployed communication systems is therefore a central requirement for applications in industrial environments.

Wireless communication solutions for closed-loop control applications have high requirements in terms of reliability. The corresponding use cases require highly reliable wireless communication with a maximum packet loss ratio (PLR) in the order of $5 \cdot 10^{-7}$ and, furthermore, no consecutive packet loss (see [2]).

5.1.1 Survival time and consecutive packet loss

Survival time is "the time that an application consuming a communication service may continue without an anticipated message" [2]. It can be considered a "safety net", providing protection against brief sporadic message losses. In periodic-deterministic communication, survival time can be also expressed as tolerable consecutive message loss. A simple example of periodic-deterministic communication is given in Figure 3. Messages are sent periodically in a given transfer interval. Correctly received messages are labeled "1" in Figure 3. Incorrectly received or lost messages are labeled "0". The example gives a survival time of two times the transfer interval. If one or two consecutive messages (case 1) are incorrectly received or lost in the network (marked red in Figure 3) and the following message is correct, the communication service is still considered to be available; it is within a period of tolerated consecutive message loss. If three consecutive messages (case 2) or more are incorrectly received or lost before the next correct message is received, the number of tolerable lost consecutive messages is exceeded, and the communication service is unavailable (marked light red in Figure 3), which results in the failure of the application.

Fig. 3: Comparison of network (NW) and communication service (CS) failures depending on the survival time



Source: 5G-ACIA

5.1.2 Recovery and application availability

After each failure, the communication service and the corresponding application have to recover. For example, with a robot application, the robot has to be moved to a safe restarting position – which can last up to several minutes.

When determining availability, recovery times have to be aggregated for all failures. As a result, a single extended period of communication service downtime has less impact on application availability than multiple shorter communication service downtime periods.

The availability of the application, however, is of paramount interest to the user of a machine or a plant. Communication service availability and reliability are key factors for this performance attribute.

5.2 Security

Security is essential in today's industrial domains in order to guarantee reliable operation and confidentiality, and to prevent interruption of service and data corruption. Aspects such as privacy, safety, and integrity depend to a great degree on secure systems and secure communication. Identities of communication participants need to be authenticated and trustworthiness in general must be guaranteed.

The following four aspects need to be addressed if security in general is to be ensured: ecosystem, communication, identities, and trustworthiness of all the participants.

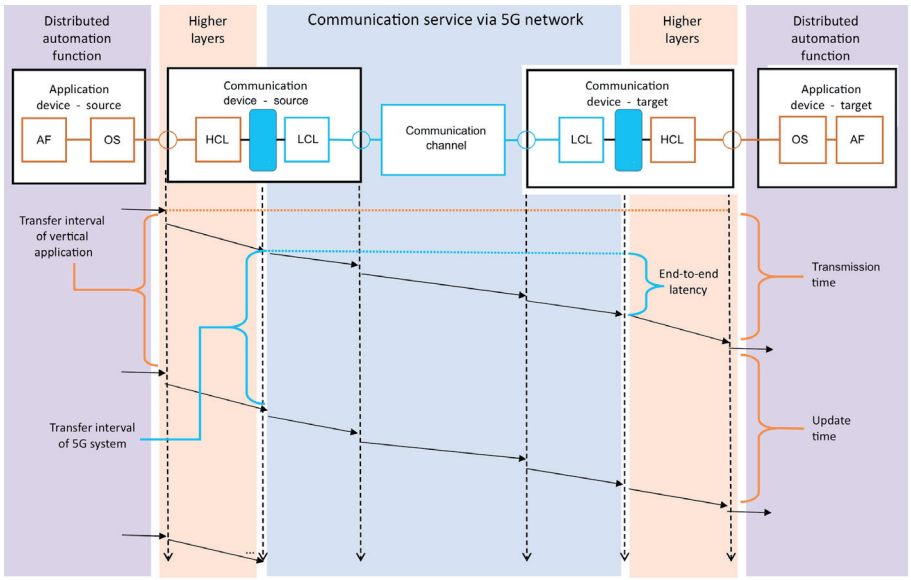
Credentials are a key aspect of security in industrial 5G networks, especially in stand-alone non-public networks. There are already various security architectures, infrastructures for credentials, and security rules implemented in industrial communication networks. Furthermore, security credentials need to be manageable for a very large number of devices.

5.3 Transmission time (latency)

Latency is an essential parameter when defining dependable communication services. Transmission time or latency is the time taken to transfer a given piece of information from a source to a destination, measured at the communication service interfaces (CSIFs), from the moment it is transmitted by the source to the moment it is successfully received at the destination (TR 22.804 [5], see Figure 4).

The (measured) transmission time varies. It is possible to account for this variation by means of the modal value (the value that occurs most frequently) and a possible spread value, for instance, the 95th percentile (the maximum value for 95% of all transmission times) [5].

Fig. 4: Relationship between application device and communication device (3GPP TS 22.104 [2]).



Source: 3GPP TS 22.104 [2]

AF = Application function (source and target)
OS = Operating system (source and target)

HCL = Higher communication layer
LCL = Lower communication layer

In control applications, transmissions of data and control commands often have to be completed within a given time period. This time period determines the maximum permissible end-to-end latency.

5.4 Diagnostics

Diagnostics entails continuously capturing and providing information of the type and volume required to characterize and evaluate the quality of 5G communication services. This includes data on the physical connection, logical links and sub-networks. Access to these data enables root-cause analysis and ensures a rapid response in the event of failure, and the identification of poor connections or other weaknesses or constraints in the network.

The 5G network has to provide interfaces that allow the industrial user to perform diagnostics on and monitoring of the QoS of the 5G communication service.

5.5 Network isolation

For automation applications, it is imperative that service quality can always be guaranteed. Therefore, it is important to ensure the 5G network can be completely controlled and managed by the industrial user, independent of other networks that may interfere with the network employed for automation.

Further reasons for isolating a network are data security and privacy. The industrial user wants to be sure that their data cannot be accessed from outside the network.

Non-public 5G networks of this type are a necessity for deploying 5G in factories with control applications. These non-public networks can be stand-alone 5G networks or integrated with, but separate from, public 5G networks (private network slices).

Furthermore, a dedicated spectrum, e.g. a licensed spectrum, is a great advantage for network isolation from potential sources of interference in order to guarantee high QoS, reliability and determinism for control applications.

5.6 Fundamental requirements

Many of the use cases described in section 4 assume a certain type of manufacturing environment. This includes certain general requirements, such as machine safety and time synchronization that are assumed by OT companies but not commonly discussed or considered with regard to 5G networks.

5.6.1 Machine safety

Safety is essential for any machine and is governed by legislation in many countries. The factory operator is responsible for machine safety, and any OT company simply assumes it is provided. In future applications, communication between safety components and the machine control system may be implemented by means of 5G. Machine safety is therefore an important context for 5G communication. For this reason, this section considers safety standards, integrity levels and the "black channel" principle.

The safety-relevant standards are categorized as Type A, B and C by ISO. Type A are the basic standards that apply to all types of machines. Type B and Type C are for specific types of machine. These standards describe safety aspects and requirements for the functional safety of tools, controls, and software. The standards allow classification of machines according to performance levels A (lowest) to E (highest), safety integrity levels SIL 1 to SIL 4, etc. The standards describe various ways of achieving these levels, for example via redundancy, diversity, latency, reliability, etc. ISO 13849 [10] is one example of a Type B safety standard (a standard for a specific type of machinery), which can be applied to machinery use cases.

5G communication can be regarded as a "black channel", as can almost all communication technologies in industrial automation. 5G components (at least the aspects specified by 3GPP) do not have to implement functional safety standards, but they must be capable of supporting functional/machine safety in production systems.

Functional safety protocols continuously poll the "black channel" to check its availability and initiate corresponding safety actions, where necessary. For example, if the "black channel" communication service is not available, the machine will be placed into a safe state. This typically means that operation will be halted. Hypothetically, a "black channel" communication service with a high packet loss rate and an availability of just 10% would still offer functional safety. However, the machine would be in a safe state, i.e. non-operational, most of the time – which is clearly not acceptable.

This demonstrates that availability is a key requirement for a 5G communication service deployed to safeguard machine safety.

Machine safety is an important aspect to be considered for 5G communication in an industrial environment.

5.6.2 Time synchronization

Communication in manufacturing requires low latency, deterministic behavior, and reliability. This requires a shared understanding of time between communicating devices. Time synchronization is therefore an important capability, already widely deployed in existing industrial communication networks.

Many production processes are simply not possible without highly accurate time synchronization.

Time synchronization between the sync master and any sync device is required in the range of ±1 µs [11].

5.6.3 Integration with existing industrial communication networks

Industrial 5G networks need to integrate with the existing installed base of industrial communication networks.

6 References

[1] 5G-ACIA White Paper "5G for Connected Industries and Automation", 2nd Edition, 2019 https://www.5g-acia.org/publications/5g-for-connected-industries-and-automation-white-paper/

[2] 3GPP Technical Specification 22.104. "Service requirements for cyber-physical control applications in vertical domains" https://www.3gpp.org/ftp/Specs/archive/22_series/22.104/

[3] 3GPP Technical Specification 22.261. "Service requirements for the 5G system" https://www.3gpp.org/ftp/Specs/archive/22_series/22.261/

[4] 5G-ACIA White Paper "5G Non-Public Networks for Industrial Scenarios", 2019 https://www.5g-acia.org/publications/5g-non-public-networks-for-industrial-scenarios-white-paper/

[5] 3GPP Technical Report 22.804. "Study on Communication for Automation in Vertical Domains" https://www.3gpp.org/ftp/Specs/archive/22_series/22.804/

[6] 3GPP Technical Report 22.832. "Study on enhancements for cyber-physical control applications in vertical domains" https://www.3gpp.org/ftp/Specs/archive/22_series/22.832/

[7] BZKI, Aspects of Dependability Assessment in ZDKI, Technical Group 1 "Applications, Requirements and Validation", 2017

[8] ISO 12100:2010. "Safety of machinery - General principles for design – Risk assessment and risk reduction"

[9] IEC 61907. "Communication network dependability engineering"

[10] ISO 13849-1:2015. "Safety of machinery – Safety related parts of control systems – Part 1: General principles for design"

[11] IEC 65C/987/CD. "Time-sensitive networking profile for industrial automation", Committee Draft (CD), Sep 2019

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
AGV	Automated guided vehicle
CS	Communication service
CSA	Communication service availability
CSIF	Communication service interface
CSR	Communication service reliability
ICT	Information and communication technologies
IP	Internet protocol
OT	Operational technology
PLR	Packet loss ratio
QoS	Quality of service
RT	Real-time
SIL	Safety integrity level
TS	Technical specification
TR	Technical report

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 6302-209
Fax: +49 69 6302-319
Email: info@5g-acia.org
www.5g-acia.org

Source of front-cover image: Variante B