N5GEH

Report v2.0

5G ICT Requirements and Solutions for N5GEH Use Cases

Project Name	N5GEH
Actual Publication Date:	**31.03.2021**
Author(s):	EDD, RWTH, TUD
Security:	Public Document
Version:	v2.0
Total number of pages:	65

Abstract

This document defines potential 5G Information and Communication Technology (ICT) requirements and solutions relevant for large-scale deployment of the energy use cases studied in N5GEH project in the commercial power networks.

It also describes the results of 5G latency performance test series when supporting the energy use cases studied in N5GEH and IEC104 protocol deployment scenarios. These tests were conducted with live 5G networks in a laboratory setting during 2020.

Keyword list

Power grid, VPP, smart buildings, microgrid, 5G, ICT, latency, reliability, edge infrastructure, gateway, protocols, test system, MQTT, IEC 60870-5-104

Disclaimer

All information provided reflects the status of the N5GEH project at the time of writing and may be subject to change.

Executive Summary

In this document, the ICT aspects of the energy use cases studied in N5GEH project are described with a focus on 5th generation cellular communications network technology (5G).

The energy use case studied in the N5GEH project comprise Regional Virtual Power Plant, Grid Protection, Building Monitoring, Closed loop Control within Buildings, District Monitoring, Control in Energy Markets and MV/LV-Grids Monitoring and Control with PMU’s.

5G concepts and features relevant for the energy use cases studied in N5GEH project are described. These 5G concepts and features are related to the energy use cases resulting in the **5G ICT solutions and recommendations** for the energy use cases. The **5G ICT requirements of** large-scale deployments of the use cases in power networks enabled by 5G are defined.

The results of a set of **laboratory tests** conducted with 5G networks as hardware in the loop in power network simulations are described. The communication latency requirements of all use cases were evaluated and then analysed with respect to the capability of 5G networks to support them.

Additionally, a set of use cases in which the IEC104 protocol is commonly used have been identified and described. The 5G ICT latency requirements for the use cases were determined and the ability of 5G networks to support these requirements was tested in the laboratory with live 5G networks. The test results showed that 5G has the capability to support the latency requirements in all IEC104 protocol use cases.

Timescales and preconditions relevant to the commercial scale use of the N5GEH energy use cases as well as possible ICT communication solutions addressing these requirements are elaborated.

Authors

Version1.0

Partner	Name	e-mail
Ericsson GmbH (EDD)		
	Robert Farac	robert.farac@ericsson.com
	Felix Maier	felix.maier@ericsson.com
	Fiona Williams	fiona.williams@ericsson.com
Technische Universität Dresden (TUD)		
	Joachim Seifert	joachim.seifert@tu-dresden.de
	Martin Knorr	martin.knorr@tu-dresden.de
	Sebastian Krahmer	sebastian.krahmer@tu-dresden.de
Rheinisch-Westfälische Technische Hochschule Aachen (RWTH)		
	Igor Sowa	isowa@eonerc.rwth-aachen.de
	Thomas Storek	tstorek@eonerc.rwth-aachen.de
	Marc Baranski	mbaranski@eonerc.rwth-aachen.de
	Sebastian Blechmann	sebastian.blechmann@eonerc.rwth-aachen.de
	Stephan Groß	sgross@eonerc.rwth-aachen.de
	Alexander Kümpel	akuempel@eonerc.rwth-aachen.de

Version 2.0

Partner	Name	e-mail
Ericsson GmbH (EDD)		
	Robert Farac	robert.farac@ericsson.com
	Felix Maier	felix.maier@ericsson.com
	Fiona Williams	fiona.williams@ericsson.com

Document History

Date	Revision	Comment	Authors/Editors	Affiliation
28.07.2020	V1.0	First version of this report.	All authors listed above.	EDD/RWTH/TUD
08.03.2021	V2.0	5G related texts and references updated and extended. Version 1.0 is deprecated and replaced by Version 2.0.	Robert Farac Fiona Williams Felix Maier	EDD

Table of Contents

1. Introduction

The transformation of the energy sector in Germany towards the increased use of sustainable green power generation and management is well underway. At the same time, improvements in the energy management of buildings and of energy in all its forms is increasingly in focus. New techniques based on the regional management of energy with a focus on the regional coordination of local electrical and thermal consumption and the integration of new ICT communications, such as LTE and 5G including the use of Edge Infrastructure to support Cloud-based systems need to be investigated and evaluated. In this context, the N5GEH project has defined the ICT requirements of a set of novel use cases and has evaluated the extent to which 5G technologies could fulfil these requirements and support them with 5G-based solutions.

A set of monitoring and control use cases for buildings and power networks as well as use case for regional VPPs were defined by the project. The requirements of these use cases placed on communication were defined and an evaluation of the performance of 5G in relation to these use cases were undertaken over the lifetime of the project and are described in this report. Timescales and preconditions relevant to the commercial scale use of the N5GEH use cases are described.

Key features of cellular wireless generations and of 5G and solutions based on LTE and 5G are described. Additionally, the Ericsson approach to the provision of Mission Critical Networks relevant to the project use cases is briefly described.

The report then evaluates of how well 5G could fulfil these requirements, based on analysis of test results and laboratory experiments. The test configuration and the test infrastructure, including the components and the lab test limitations are briefly presented. Two types of communications performance evaluations were conducted in the project by Ericsson:

- Evaluation of the 5G latency performance supporting N5GEH use cases, based on the analysis of relevant test results, and
- Evaluation of the 5G latency performance in the use cases in which the IEC104 protocol is used through conducting an extensive series of laboratory experiments.

During 2020, and extra set of tests with live 5G networks was undertaken to investigate the latencies which 5G could achieve for the use cases in which the IEC104 protocol is commonly used.

The ICT 5G solutions and recommendations relevant for all the use cases are described and followed by a summary of the conclusions of the work.

Despite long-lasting restrictions on accessing Ericsson laboratories due to COVID-19, all planned tests were successfully completed.

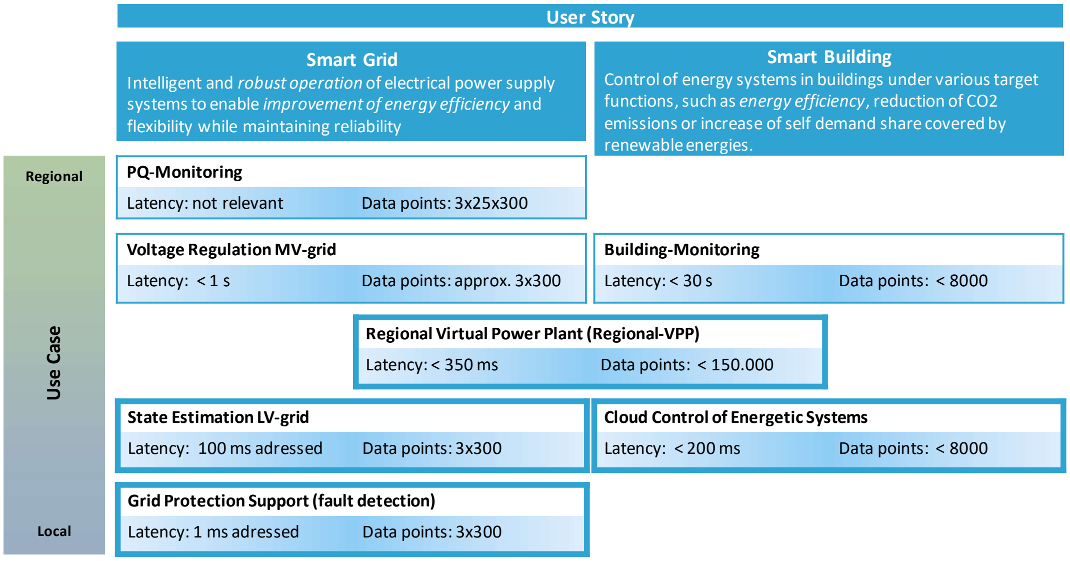
This report complements the contractually required reports of the project.

2. ICT Requirements of the N5GEH Use Cases

This chapter describes ICT requirements derived from the N5GEH use cases. Additionally, it describes timescales and preconditions relevant to the commercial scale deployment of N5GEH use cases based on the best estimates of the project partners, as they described them in project discussions. Their estimates have been summarised in this chapter by the Ericsson authors of this report.

The power generation, transmission, and distribution sector will move from the current hierarchical and centralized architecture, to a decentralized one where multiple and independent regional systems cooperate to control and coordinate their power production. Therefore, the overall goal of the project "National 5G Energy Hub" is the implementation of modern communication technologies in the energy sector with use of radio/ 5G technologies for the control of decentralized devices.

In the first project stage (two years) a cloud based open source communication platform was developed. To show the functionality of such a platform and to test the performance and flexibility selected uses case were determined. These use cases can be assigned to the domains or user stories low voltage distribution grid (smart grid) and smart buildings. Figure 2-1 shows some energy related use cases. With regard to the capabilities of 5G technology on the one hand the use case regional virtual power plant is interesting, because a high number of data points can be addressed with this (massive IoT). On the other hand, the grid protection use case has challenging requirements to the latency.



Smart Grid
Intelligent and *robust operation* of electrical power supply systems to enable *improvement of energy efficiency* and flexibility while maintaining reliability

Smart Building
Control of energy systems in buildings under various target functions, such as *energy efficiency*, reduction of CO2 emissions or increase of self demand share covered by renewable energies.

PQ-Monitoring
Latency: not relevant — Data points: 3x25x300

Voltage Regulation MV-grid
Latency: < 1 s — Data points: approx. 3x300

Building-Monitoring
Latency: < 30 s — Data points: < 8000

Regional Virtual Power Plant (Regional-VPP)
Latency: < 350 ms — Data points: < 150.000

State Estimation LV-grid
Latency: 100 ms adressed — Data points: 3x300

Cloud Control of Energetic Systems
Latency: < 200 ms — Data points: < 8000

Grid Protection Support (fault detection)
Latency: 1 ms adressed — Data points: 3x300

Figure 2-1: N5GEH User Stories and Use Cases

For each energy use case, the following set of the 5G ICT requirements is elaborated: number of endpoints, latency, message sampling rate, message size, data transfer rate, reliability, availability and security.

The **number of endpoints** shows total number of devices (sensors, actuators) or data points (smart buildings use cases) with a connection to the communication network providing data from and to energy network or building management system.

The **latency** describes the transmission time needed for a measurement or control signal to be sent from the sensor in the power grid to the control center via communications network or vice-verse from the control center to the actuator.

The **message sampling rate** describes the number of messages per second per device that are transmitted between the sensor and the control center (or vice versa).

The **message size** indicates size of the message transmitted between the sensor and the control center including overhead for addressing, time stamps, authentication and authorisation, encryption, et al.

The **data transfer rate** describes the data rate per device depending on the message sampling rate and size.

The **reliability** describes the ability of a communication network to guarantee that messages reach their destination complete and uncorrupted and, in the order, they were sent. It is an informal interpretation of the description of the project partners.

The **availability** represents maximal allowed communications system downtime. Availability of communications is described as a percentage of time in which system is available. E.g., a system which is available 99.9999% has a downtime of 3 seconds per month.

The **security** describes the need for the prevention of unauthorized access to telecommunications traffic. It is an informal interpretation of the description of the project partners

2.1 Use Case 1: Regional Virtual Power Plant

2.1.1 Energy system requirements

The main objective of the use case is to improve the balancing of energy generation and energy consumption in a local district by using intelligent regional networks. With this the load of transmission grids also can be reduced. Furthermore, it is possible, by bundling several systems and the ability to respond quickly to take part on the energy market and generate revenue. Generally, the use case contains in addition to the higher-level control tasks, also control tasks of the local energy system. This control can be carried out under several objective functions, such as a reduction of energy costs or an increase in the portion of own consumption of renewable energies. In order to achieve the central objectives described above, the fulfilment of subtasks is required. This includes the prediction of the thermal and electrical load which is significantly involved in the creation of an energy trend band. The energy trend band contains the prediction of the energetic flexibility of the system and thus defines the potential for a positive or negative load shift. Prediction algorithms have been already created and tested in [1] and [2], and will be further developed in the N5GEH project.

Regional virtual Power Plant (RVPP) will apply in:

- Rural area with one- and two-family houses
- Periphery of a city with mixed structure (industry, residential, commerce)
- Buildings allocated to one cell of low voltage grid (approximately 300 buildings)

Measurement devices in buildings will send the data to the gateway for pre-processing (see Figure 2-2). Further smaller amount data will be sent to the backend central cloud. Normally cloud will issue switching commands to the actuators, but gateway can also take over basic control functions independently from the cloud. MQTT protocol [3] will be used for the communications between the devices, the gateway and the central cloud.

Back End (Cloud) will be coupled to DSO or energy service providers that will be able to specify control conditions and receive monitoring information via standardized interfaces (IEC 60870-5-104 and IEC 61850).

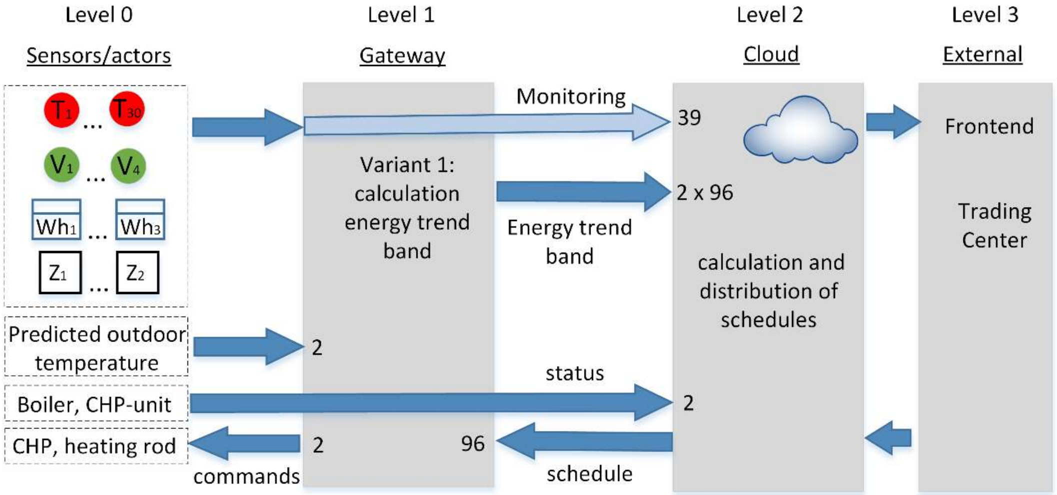


Figure 2-2: RVPP platform levels with related data routes

2.1.2 5G ICT requirements

Bidirectional communication between the aggregation gateway and the devices takes place.

Number of endpoints

Central Element for providing flexibility is the thermal storage[1]. The realization of storage management requires the measurement of the current state of charge of the storage by means of a series of sensors. The number of required data points per building is determined by the type of building, the size of the building and the degree of automation of the building and is approximately 30 for a single-family house with basic configuration.

In cities about 5,000 people are living per km^2. It means 15,000 people per 3 km². 10 datapoints per person lead to 150,000 datapoints. Accordingly, maximum number of datapoints is 150,000 in one district with an area of about 3 km^2 assuming that the communications structure is also used for smart home functionalities and cloud control.

Latency

The highest required latency is 350 ms and is determined by the scenario of a load shedding in the electrical network. For further regulation and control tasks higher latencies are permissible.

Message sampling rate

Sampling rate of the messages sent from the device to the aggregation gateway will be 6 messages per minute. For the energy vector upper limit is 15 min.

Message size

Message size depends on the used protocol. If MQTT is used containing the headers (56 B fix) and payload with 1 measurement value and the time stamp (20 B per value + 20 B for timestamp), the message size would be 96 B.

Data transfer rate

The data transfer rate per data point with the sampling rate of 6 messages per minute and if MQTT protocol is used, would be 9.6 KB/s = 76.8 bps = 0.076 Kbps

Reliability

The reliability is important particularly for load shedding because of a reliable data transfer is needed. But the use case contains no directly safety relevant aspects.

[1] Thermal storage is essential for the concept. But an electrical storage is not a basis component of this. Probably a battery could provide more flexibility but is not considered here.

Availability

The communication availability should be high and is a precondition for qualification to take part on the balance energy market (“Regelenergiemarkt”). The requirements are defined by the transmission grid operators. For instance, the document describing a minimum standard set by the German TSOs for the IT requirements of the reserve providers for the provision of control reserves (page 15, point A12) [4] says that the individual connection between the control systems of the TSO and the reserve provider must have an availability of at least 98.5% (calculated total availability of both redundantly connections is 99.9775%). In this context, 99,9% is an objective in N5GEH project and has to be adapted specifically.

Security

Medium (energy supply must be guaranteed).

High level of privacy is requested (current values could be used to identify the behaviour of single households; storage/transfer of data (e.g. fault report) is most likely forbidden); consider GDPR.

Table 2-1 shows 5G ICT requirements Use Case Regional Virtual Power Plant.

Table 2-1 5G ICT for Use Case Regional Virtual Power Plant

5G ICT Requirements	**Use Case Regional Virtual Power Plant**
Req-RVPP-endPoints	50,000 datapoints per km^2
Req-RVPP-latency	<350 ms (round-trip)
Req-RVPP-sRate	6 messages per minute
Req-RVPP-mSize	96 B (MQTT protocol)
Req-RVPP-dtRate	0.076 Kbps
Req-RVPP-reliability	Important
Req-RVPP-availability	99,9% (downtime per month of 43 minute)
Req-RVPP-security	Important

2.1.3 Timescales and preconditions relevant to the commercial scale use of Use Case Regional Virtual Power Plant

Important precondition for the role out is on the one hand, that energy-political boundary conditions are adapted, and it becomes more financially attractive to use energy locally instead of feed it in transmission grid. That applies for instance for feed-in tariffs in the “Erneuerbare-Energien-Gesetz” or “Kraft-Wärme-Kopplungsgesetz”. On the other hand, also the barriers (costs, data privacy) for connecting small devices into a RVVP-network have to be reduced.

In terms of time scale, it can be stated, that RVVP already introduced and running in a number of projects and that also first smart meter gateways are passed the test of BSI. So far, a timescale has to be seen in a range of less than 5 years.

2.2 Use Case 2: Grid Protection (FLISR)

2.2.1 Energy system requirements

Nowadays in Low Voltage (LV) grids the number of connected decentralized generators respectively battery storages is raising. Thus, a decrease of the gap between maximum operating current and minimum short-circuit current occurs. In addition to this, the Short Circuit Current (SCC) contribution from DGs can lead to so-called "Blinding" or “Sympathetic Tripping”. In the first case, a fault detection via mains fuse is not possible in every situation, because of the penetration with DGs the SCC though mains fuse can be less than minimum tripping current. In the second case, the fault can be mistakenly detected in a wrong feeder, because of DGs contribution to SCC. To avoid such effects, a permanent tracing of current at relevant nodes can be a solution. Therefore, low cost measurement devices, so called Wireless Transducer Interfaces (WTI), have to be developed, which ensure a sampling rate of > 1 kHz and can communicate via radio-based transmission. The current measurement has to be performed for 3-phase simultaneously as well as simultaneously within the observed area of the protection device. To gain advantages in comparison to mains fuses nowadays used, the iteration of transmission, evaluation and control has to be performed within 20 ms (the faster the better). In addition to the latency of the transmission process itself, the grid operator imposes high requirements on the adherence of latency. Based on these needs, a communication architecture has to be defined which fits a compromise of latency, jitter and availability. Furthermore, to ensure a proper protection function during each time step, a concept of redundancy has to be considered as well. In general, the function of data aggregation, evaluation and control can be done by a) a physical protection device located at the LV/MV-transformer, which is connected to the 5G-network; b) a virtual protection device, which runs in the mobile Edge Infrastructure.

Objectives:

- Establishment of a separate reserve protection in the LV and MV level. Advantages: radio-supported, retrofittable, cost-effective, diversity compared to Smart Meter Gateway
- Reliable detection of faults through reserve protection in the LV network
- Evaluation of grid states (e.g., short-term overload) as support for grid protection in the MV grid

User:

- Local energy companies
- Electrical network operators (distribution network / local network)

Functional requirements:

It has to be mentioned that the time synchronicity of the WTIs is essential (time synchronicity of at least 250µs). Therefore, synchronization based on a mobile network time service is necessary.

2.2.2 5G ICT requirements

Bi-directional communication is required to get measured values of current and voltage in the cloud (representing the place of the FLISR service itself) and to apply on/off-commands from the cloud to the actuators.

Additional bi-directional communication is required to get switch status in the control center and to apply open or close control actions from the control centers to the switches.

The following requirements are based on the first part described above.

Number of endpoints

Up to 300 Wireless Transducer Interface (WTI) endpoints within low voltage grid area plus actuators (number of connected Decentralized Generators DGs plus number of feeders).

Latency

The requirement for latency is critical. Lowest latency is targeted (aim: 1 ms). It will work even with higher latency, but then of course the improvement against the legacy protection system will be smaller. End-to-end latency should be less than 30 ms. A low algorithm computational time for the service is more important than a low one-way-latency.

Message sampling rate

Signal is sent between the WTI/sensor and the cloud every 1-20 ms depending on the hardware capability.

Message size (per device)

Message size depends on the used protocol. If MQTT is used containing the headers (56 B fix) and payload with 6 measurement values and the time stamp (20 B per value + 20 B for timestamp), the message size would be 196 B.

Data transfer rate

The data transfer rate per device with the sampling rate of 1000 messages per second and if MQTT protocol is used, would be 196 KB/s = 1,568 Kbps

Reliability

The requirement for reliability is critical. Regarding that the proposed wireless grid protection is foreseen as an additional system to the legacy grid protection, the achieved quality can be lower while still gaining an improvement.

Availability

Usually in grid operation a system availability of 99,999 % (equivalent of downtime of < 5.3 min/year) is claimed.

In case of breakdown of base station, a deploy of a redundant system should be foreseen within 100 ms.

Security

High (highly effects the grid operation)

High privacy level – current values could be used to identify the behaviour of single households; storage/transfer of data (e.g. fault report) is most likely forbidden

Table 2-2 shows 5G ICT requirements for Use Case Grid Protection (GP).

Table 2-2 5G ICT requirements for the Use Case Grid Protection (FLISR)

5G ICT Requirements	Use Case Grid Protection (FLISR)
Req-GP-endPoints	300 within LV grid area plus actuators (number of connected DGs plus number of feeders)
Req-GP-latency	1-10 ms (round-trip)
Req-GP-sRate	50-1000 messages per second
Req-GP-mSize	196 B
Req-GP-dtRate	1,568 Kbps
Req-GP-reliability	Critical
Req-GP-availability	99.999% (communications downtime per month of 26 seconds)
Req-GP-security	Critical

2.2.3 Timescales and preconditions relevant to the commercial scale use of Use Case Grid Protection

It can be assumed that the technology will be used more long-term than short-term as a backup solution to existing grid protection systems in the LV grid. Background is the currently not yet existing experiences regarding costs to benefit. Reliability and security will even be more important than a low latency from robust grid operation point of view.

On the other hand, in MV grids a selective measurement and monitoring of currents at the grid connection point (POC) of companies of particular interest to support the existing grid protection will be more likely in the short term.

2.3 Use Case 3.1: Building Monitoring

2.3.1 Energy system requirements

Scope:

Currently, there are lots of different machines from different manufacturers in the field of building energy systems. This results in a big variation on proprietary communication protocols and data formats. In this use case, different sensors are connected via wireless protocols (see Figure 2-3). The data can be channelled through an optional low-priced gateway or can be sent directly to a (edge) cloud platform. In this platform the data is processed and can be monitored by a user. The monitored data usually consist of different quantities like temperature, humidity, pressure, heating and cooling fluids, alarms, weather data or electricity usage. In this use case, a lock-in effect to a few manufacturers is avoided, which is beneficial. Furthermore, the developed algorithms and software components will be open source and the data processing will be decentralized and scalable.

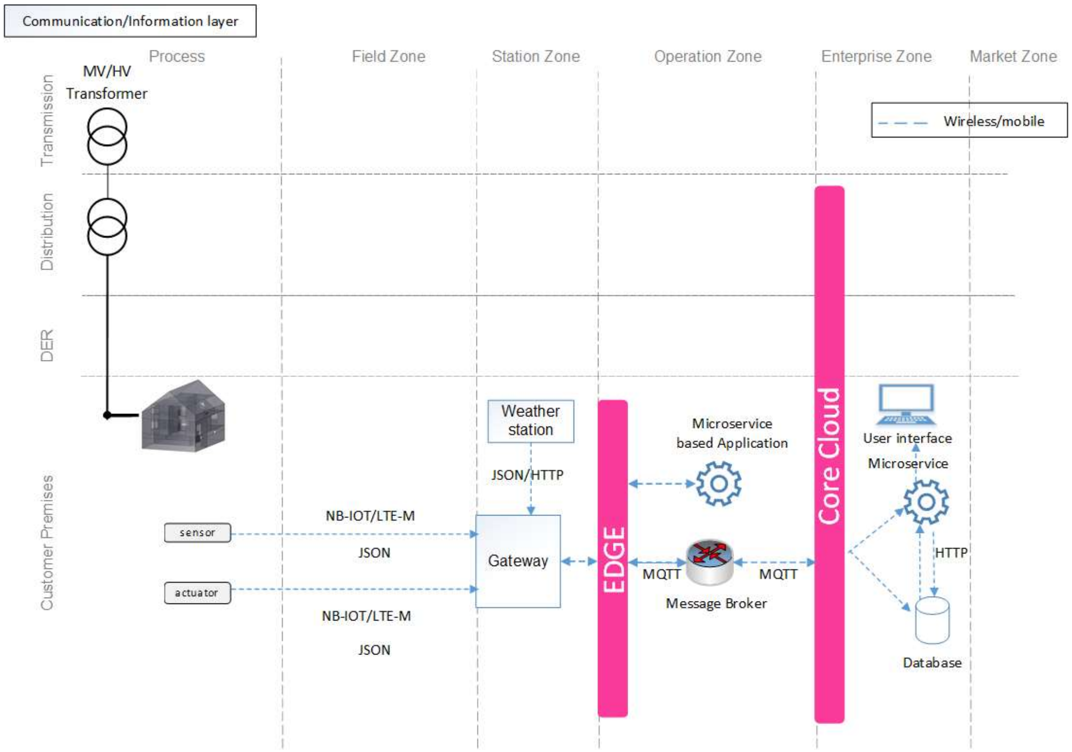


Figure 2-3: Mapping of the Use Case Building Monitoring onto the SGAM-Model

The use of a cloud platform and an optional gateway enables decentralized and scalable computing and avoids a lock-in of systems to devices from specific manufacturers. The gathered data in the cloud can be displayed in real time by authorized users. This visualization of the buildings' performance is supposed to create some awareness of the building energy system with the user. Through cloud computing, electricity, heat and cold demand and production can be calculated and processed locally to a certain point while encryption protocols guarantee GDPR-conform handling.

Modern energy building concepts come with a huge range of different sensors to estimate the building status and user comfort. All the different sensors can be connected either via cable, which is mostly expensive, especially in finished buildings, or wirelessly. The wireless connection can be done through an optional gateway or directly to a (edge) cloud platform. The actual processing of the data is done in the cloud which enables decentralized and thus scalable computation. Latter allows to form virtual local edge clouds which enable local computation of local energy demands. In combination with the feature of a 2-way data exchange, this peaks in the opportunity of local demand side management.

Objectives:

- Data storage takes place in cloud.
- Visualization of current metering data from smart meter and DSO. The stored data are retrieved back from the server.

Functional requirements:

Support for Device Protocols: The sensors and actuators will use MQTT for communication with the cloud platform. The payload is structured in the JSON-LD protocol (JavaScript Object Notation for Linked Data). Data models are used.

Platform Internal Communication: Fiware platform uses IoT agent and Orion context broker. If using Publish/Subscribe broker mechanism, a very frequent subscribe action must be implemented for these processes.

Data Aggregation: In this use case, data are aggregated on Fiware platform. It is connected with time series database. It is used for data visualization and data analysis. The API such as Grafana are connected for visualization.

2.3.2 5G ICT requirements

Communications (message transport) for Building Monitoring use case is uni-directional, i.e. uplink only, from the sensors to the Edge Infrastructure.

Number of endpoints

Number of data points in monitoring of ACS building is approximately 7000. A data point is a single string of data sent by any device, meter or sensor in a building. The best way to understand a data point is to think about it as a “variable” in a mathematical or scientific way. Therefore, one meter does not automatically equal one data point.

For office building up to 10,000 data points (sensor values). For smart home approximately ten sensors (one sensor per room plus energy system).

Latency

Lower radio frequencies are to be used in order that signal can penetrate in a building. This leads to higher latency that is not critical requirement for building monitoring. However, the controlling (see Use Case Closed Loop Control within Buildings below) still has to work where the round-trip latency of 200 ms is required.

Message sampling rate

The sampling rate of the data communicated between the devices (sensors and actuators) and the cloud platform:

- heat-pump: <30 s, except for pressure evaporator <1 s,
- boiler: <30 s,
- photo-voltaic: <30 s,
- battery storage system: <1 s,
- energy/water meter/valves/pump: <30 s, and
- energy meter: <10 ms.

Message size (per datapoint)

Message size depends on the used protocol. If MQTT is used containing the headers (56 B fix) and payload with 1 measurement value and the time stamp (20 B per value + 20 B for timestamp), the message size would be 96 B.

Data transfer rate

The data transfer rate per data point with the sampling rate of 100 messages per second and if MQTT protocol is used, would be 9.6 KB/s = 76.8 Kbps

The data transfer rate per data point with the sampling rate of 1 message per second and if MQTT protocol is used, would be 96 B/s = 768 bps = 0.7 Kbps

The data transfer rate per data point with the sampling rate of 2 messages per minute and if MQTT protocol is used, would be 3.2 B/s = 25.6 bps = 0.03 Kbps

Reliability

No specific requirements are foreseen related to communications reliability.

Availability

No specific requirements are foreseen related to communications availability. Generally, availability of the communications should not be critical issue in the Building Monitoring use case.

Security

Communications have to be secured by the actual standards like Transport Layer Security (TLS) 1.2 and higher. The management platform has to be secured. No direct access to the components, especially not the database, has to be allowed. Software has to be up to date. Devices should also be protected against physical attacks. E.g. gateways locked in rooms with restricted access and devices not hanging openly.

Since personal data are mostly handled with, GDPR needs to be respected.

Table 2-3 shows 5G ICT requirements for the Use Case Building Monitoring.

Table 2-3 5G ICT requirements for the Use Case Building Monitoring

5G ICT Requirements	Use Case Building Monitoring
Req-SB-endPoints	<8,000 datapoints (office building); 10 devices (smart home)
Req-SB-latency	100 ms (uplink, from sensor to the cloud platform)
Req-SB-sRate [messages per second]	100 (energy meter) 1 (battery storage system) 2 messages/minute (heat-pump, boiler, photo-voltaic, energy/water/meter/valves/pump)
Req-SB-mSize	96 B (MQTT protocol)
Req-SB-dtRate	76.8 Kbps (energy meter) 0.7K bps battery storage system) 0.03 Kbps (heat-pump, boiler, photo-voltaic, energy/water/meter/valves/pump)
Req-SB-reliability	Important but not critical
Req-SB-availability	99,9% (communications downtime per month of 43 minutes)
Req-SB-security	Important both physical and cyber security

2.3.3 Timescales and preconditions relevant to the commercial scale use of Use Case Buildings Monitoring

The case can be implemented with the current technology. Devices and cloud solutions are already available in the market. However, the implementation in live networks can be expected in 3-5 years.

2.4 Use Case 3.2: Closed Loop Control within Buildings

2.4.1 Energy system requirements

Scope:

In building energy systems, a huge number of actuators need to be controlled to achieve certain set points (e.g., temperature or volume flow). 5G and LTE technologies allow the direct internet access of sensors and actuators, such that the system can be controlled by a cloud service. The advantage of a cloud-based control using 5G or LTE radio technology is the reduction of local hardware and installation costs as, e.g., wiring. Additionally, it provides possibility for high computational power if needed and an easy-to-maintain software/program and hardware, e.g., software updates over the air. This use-case aims to demonstrate a closed-loop control in which the data transfer is realised with 4/5G whereas the controller runs remotely as a service on a cloud platform.

Objectives:

- Simple connection of sensors and actuators: connection via 5G, low latency and sampling rate around 1 s needed for sensors and/or event based using sensor depending thresholds.
- Advanced control: Use of advanced and maintainable control strategies on a cloud platform.
- Cost reduction: No cables necessary, no installation of cables (working time), cheap hardware (no plc needed)

Narrative of the Use Case:

In building energy systems, a huge number of actuators need to be controlled to archive certain set points (e.g., temperature or volume flow). Therefore, sensors and actuators have to be connected to a plc and a control program/algorithm needs to be implemented (see Figure 2-4). This leads to the following major issues:

- Due to the high number of different bus systems and protocols, which may be open or proprietary, many gateways and specialised hardware and software is needed at the moment. Hence, the integration of different bus systems could also be time consuming and could require high expert knowledge due to the lack of interoperability. Using 4/5G based IoT sensors and actuators, the installation of the building automation system can be simplified.
- Control algorithms are implemented on local hardware. This hardware can be expensive and the provided computational power is rarely fully used. Additionally, some vendors still do not use normed languages (e.g. IEC 61131). Hence, in order to maintain or improve the software a specialised and mostly expensive programmer to come to the site in person. The use of the 5G technology could solve these problems: the hardware costs decreases, and the maintainability increases by using cloud services.

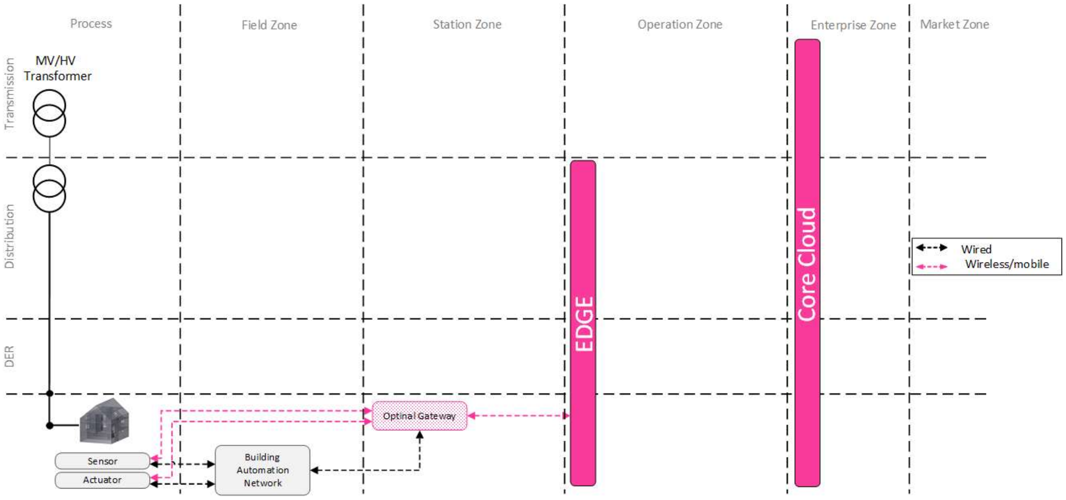


Figure 2-4: Mapping of the Use Case Closed Loop Control within Buildings onto the SGAM-Model

Functional requirements:

Support for Device Protocols: The actuators and sensors will use MQTT for communication with the cloud platform.

Platform Internal Communication: The control algorithms need to receive the sensor data and send the calculated control signal to the actuators. The control algorithm could communicate with the platform via http requests and posts. Unauthorized access must be prohibited.

Service Interface to Smart Energy Platform Users: An automated integration of the devices is required. Additionally, a service for debugging would be helpful (e.g. list which service receives which kind of data, in order to localize errors).

Data Aggregation: The data don't need to be aggregated for the first implementation.

2.4.2 5G ICT requirements

Communications (message transport) for Closed Loop Control use case is bidirectional, between the sensors/actuators and the Edge Infrastructure.

Number of endpoints

For office building up to 10,000 data points (sensor and actuator values). For smart home approximately 3-4 sensors (one sensor per room plus energy system) and 2-3 actuators (one actuator per room). Even more in industry buildings and airports.

Latency

200 ms the transmission of data for lighting; others depending on physical properties.

Message sampling rate

Sampling rate around 1 s needed for sensors and/or event based using sensor depending thresholds.

Message size

Message size depends on the used protocol. If MQTT is used containing the headers (56 B fix) and payload with 1 measurement value and the time stamp (20 B per value + 20 B for timestamp), the message size would be 96 B.

Data transfer rate

The data transfer rate per data point with the sampling rate of 1 message per second and if MQTT protocol is used, would be 96 B/s = 768 bps = 0.7 Kbps

Reliability

The higher the reliability the better. Reliability is very important and the higher the better. However, in practice, there are a lot of faults in current automation systems, but the systems are generally working. Furthermore, the components could have a fall-back mode if the connection is lost.

Availability

The higher the reliability the better. Availability is very important and the higher the better. However, in practice, there are a lot of faults in current automation systems, but the systems are generally working. Furthermore, the components could have a fall-back mode if the connection is lost.

Security

Secure system against hacking of the system is requested, to have more trustful system compliant to the standards. Costs, availability and security are three main factors for the system purchase. Security is critical, since the components of the building could be damaged in an attack.

Table 2-4 shows ICT communications requirements for the Use Case Closed Loop Control within Buildings.

Table 2-4 5G ICT requirements for the Use Case Closed Loop Control within Buildings

ICT Communications Requirements	**Use Case Closed Loop Control within Buildings**
Req-CLC-endPoints	<10,000 datapoints (office building); 5-7 devices (smart home)

Req-CLC-latency	200 ms (round-trip)
Req-CLC-sRate	1 message per second per device
Req-CLC-mSize	96 B (MQTT protocol)
Req-CLC-dtRate	0.7 Kbps
Req-CLC-reliability	Important but not critical
Req-CLC-availability	99,9% (communications downtime per month of 43 minutes) – normal operations 99.999% (communications downtime per month of 26 seconds) – critical operations (e.g. fire alerts)
Req-CLC-security	Critical

2.4.3 Timescales and preconditions relevant to the commercial scale use of Use Case Closed Loop Control within Buildings

The case can be implemented with the current technology. Devices and cloud solutions are already available in the market. However, the implementation in live networks can be expected in 3-5 years.

Obstacle for faster acceptation of the solution could be undefined responsibility for faults when occur.

2.5 Use Case 4: District Monitoring and Control in Energy Market

Scope:

Nowadays, grid operators balance load fluctuation in the electrical grid on HV level exclusively. Therefore, the grid operators need to have enough flexible available to react to any possible load variation. This flexibility is mostly provided by old conventional power plants fired by fossil energy sources. In context of the "Energiewende", we are reducing the number of conventional power plants and consequently the amount of flexibility in the grid. Additionally, the amount of large wind parks is increasing, which causes new fluctuation in the grid. Summarizing, we can say that one the one hand side we are reducing conventional flexibility sources and on the other hand we are introducing further sources of fluctuation generation in our power mix.

Demand side management (DSM) offers the opportunity to utilize flexibility available at the demand side of the energy system. Such sources of flexibility can be electrical vehicle, battery systems, smart buildings, etc. Aggregating all these flexibility sources on district level, a control system could operate the district towards a fix power consumption.

By allowing the grid operators to define a set-point for the consumed power of the district, fluctuations in the HV grid can be avoided, which leads to less expensive grid interventions.

Functional requirements:

Estimation data rate: ~1.5 MB per flexibility source and direction per cycle. With 100 sources and 15 min cycle length the data exchange sums up to 14.4 GB per day.

Latency: With 1000 iterations and an average latency of 150 ms (LTE) the time for one optimization estimates to 150 sec = 2.5 min exclusively for communication, not considering other communication issues and computational time. The number of iterations increases with the numbers of flexibility sources and smaller cycle times. With the 10 ms standard 5G latency, iterations can be performed much more frequently than using higher latency LTE communications.

2.5.1 5G ICT requirements

Communications (message transport) for the use case is bidirectional, between the measurement devices and the control center.

Number of endpoints

One district in this use case is a mid-size city. One district will be controlled by one electricity provider. 500,000 to 1,000,000 devices typically smart gateways will be connected to the control center. The control center will be 100's kilometres away from the district.

Smart gateway installed in a house will send the measurements to the control center that will reply with the control signal back to the smart gateway.

Latency

Measurements collected from end devices are used for 15 minutes energy forecast. Accordingly, communications latency of collected measurements can be one minute, i.e., it is not critical.

Message sampling rate

Measurements and control signals need to be sent in one-minute intervals.

Message size

DLMS/COSEM communication protocol will be used for transmission of measurements and control signals. MQTT is not foreseen to be used in this use case. Message size containing the headers (12 B fix) and payload with 1 measurement value and the time stamp (6 B per value + 6 B for timestamp), the message size would be 24 B [5].

Data transfer rate

The data transfer rate per measurement device with the sampling rate of 1 message per minute and if DLMS/COSEM protocol is used, would be 0.4 B/s = 3.2 bps = 0.003 Kbps.

Reliability

Reliable communication is not needed for monitoring and control. However, added value services (e.g. emergency call, smart mobility) will be used that request very high reliability of the communications.

Availability

Communications should be always available for added value services traffic transmission. Availability can be expressed with five nines (99.999%) meaning communications downtime of 26 s per month.

Security

The traffic has to be secured especially for added value services. End-to-end encryption occurring on application layer is expected.

Communication channels will be encrypted end-to-end. The encryption will be done on application layer. Therefore, very high security is requested.

Table 2-5 shows 5G ICT requirements for the Use Case District Monitoring and Control in Energy Market.

Table 2-5 5G ICT requirements for the Use Case District Monitoring and Control in Energy Market

5G ICT Requirements	Use Case District Monitoring and Control in Energy Market
Req-DCE-endPoints	500K – 1M devices per district in size of 100's km^2
Req-DCE-latency	1 minute (round-trip)
Req-DCE-sRate	1 message per minute
Req-DCE-mSize	24 B (DLMS/COSEM protocol)

Req-DCE-dtRate	0.003 Kbps
Req-DCE-reliability	Critical
Req-DCE-availability	99.999% (communications downtime per month of 26 seconds)
Req-DCE-security	Critical

2.5.2 Timescales and preconditions relevant to the commercial scale use of the Use Case District Monitoring and Control in Energy Market

This service is not available in commercial networks at the moment. Roll-out of the monitoring service is starting this year (2020) since rollout of smart meters started this year. Added value services are being developed and discussed currently. Control services deployment is foreseen to start during the period of three to five years.

2.6 Use Case 5: MV/LV-Grids Monitoring and Control with PMU

2.6.1 Energy system requirements

Scope:

In the distribution system (medium and low voltage power system), the monitoring based on Phasor Measurement Units (PMUs) would give opportunity to improve the quality of grid algorithms responsible for control and management. The usage of mobile 5G technology with higher bandwidth, lower latency and the Edge Infrastructure significantly contribute together with utilization of the PMUs to the increase of performance in monitoring and control. Combining PMUs and 5G with in monitoring and control in distribution network might bring multiple benefits such as grid control robustness or monetary benefits to system operators. Besides, the advantages of wireless connection and computing in the cloud are further possible improvements in grid monitoring and control.

Objective:

- Development of the grid monitoring based on the low-cost PMU hardware and implementation of the algorithms utilizing the hardware with the features of increased reporting rate and lower latency between the measurement and the final output of the monitoring and control algorithms (e.g., state estimation algorithm as well as subsequent algorithms, e.g., based on optimal power flow).
- Development of control and management of the islanded microgrid through the monitoring based on PMUs and potential of running services in the Edge Infrastructure under blackout conditions of the bulk power system

Narrative of the Use Case:

The PMUs are implemented together with simulated environment of distribution network and microgrid. Besides the real hardware of PMU, several devices, sensors and actuators are implemented in the simulated environment. The measurements are sent to the cloud platform and the algorithms of monitoring and control are executed in the cloud (see Figure 2-5). The platform can operate in the edge cloud or in the core cloud. In particular scenarios, it is required to run the services (control algorithms) in the edge cloud. Algorithms should realize appropriate control depending on the dynamics in the grid. The control values are sent from the cloud to the devices - in this way, the control loop is closed.

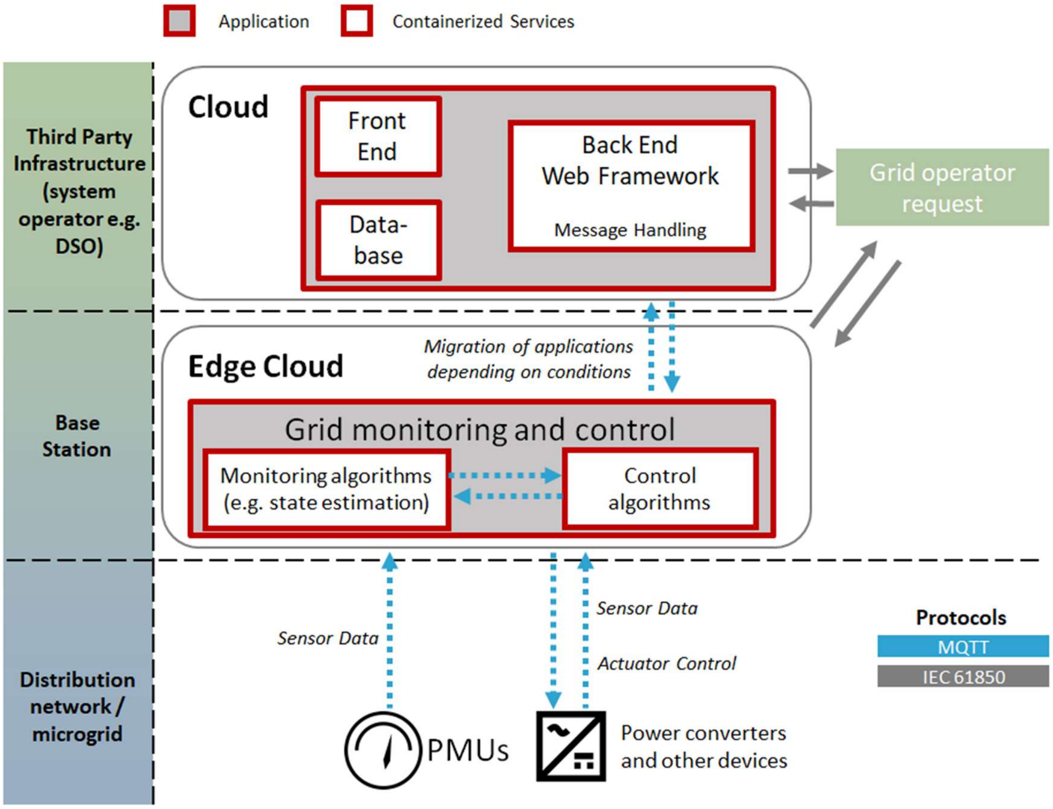

Application
Containerized Services
Third Party Infrastructure (system operator e.g. DSO)
Base Station
Distribution network / microgrid
Cloud
Front End
Data-base
Back End Web Framework
Message Handling
Grid operator request
Edge Cloud
Migration of applications depending on conditions
Grid monitoring and control
Monitoring algorithms (e.g. state estimation)
Control algorithms
Sensor Data
Sensor Data
Actuator Control
Protocols
MQTT
IEC 61850
PMUs
Power converters and other devices

Figure 2-5: Diagram of the Use Case MV/LV-Grids Monitoring and Control with PMU

Functional requirements:

Support for device protocol: The PMUs will use MQTT for communication with the cloud platform. The payload is structured in the IEC61850 SV protocol and Ultra-Light protocol of FIWARE.

Service interface to smart energy platform users: the external access to the services in the platform could be provided via REST protocol, e.g., for system operator, microgrid operator, etc.

Data aggregation: The data used for the monitoring and control are not aggregated. Ultra-light data protocol is supposed to minimize the size of the payload. It is still not an aggregation though, but it is much lighter than JSON. Therefore, in the first implementation (every 100 ms phasors and other measurements) aggregation is not necessary and not considered.

Data analysis: Data analysis is performed in the platform, serving for monitoring, or monitoring and control of distribution network and microgrid. Secondary microgrid controller will be implemented and will be responsible for analysis of the data and derivation of the control values. There are no specific requirements on the type of the databases. It should be easily accessible by the algorithms.

2.6.2 5G ICT requirements

Communication is bidirectional. The measurements are provided from the measurement devices to the control point(s), and control signal are sent back to actuators in the grid.

Number of endpoints

Assuming that a residential district has 200 houses, all equipped with inverters, and having 200 buses with PMUs plus about 100 additional measurement points, would result in about 500 measurement points (devices) in area of a district. It can also be assumed that the area is supplied from one substation and could be covered with one radio base station. Typical area size in suburb is about 3 km^2.

Latency

In the normal conditions what is usual case, round-trip latency is not critical. 100’s ms of latency can be tolerated. However, in grids with high density of renewable energy sources, or in volatile weather conditions, or number of faults happening in the network, low latency needs to be maintained in the grid. Keeping low latency is applicable for distribution grid but especially important is for microgrids. In such cases round-trip latency should be in a range of 30-50 ms.

In case of distributed grid geographically dislocated control points need to communicate to each other that increases total close loop latency. In a case of microgrid, the service logic would typically be run in one central point.

Message sampling rate

The data from both PMU and inverter should have the same sampling rates. They have to be synchronized in the cloud anyway and delivered to the controller. Initial sampling rate (for both) was 8Hz, i.e., every 125 ms and the target is 50 Hz, i.e., every 20 ms.

Message size

The sampling values of the data communicated between the physical implementation (PMU, RTDS) and the cloud platform:

- PMU: 30 values
    - 3xI measurements (id, magnitude, angle, frequency, RoCoF) + 3xV phasors (respective content)
- Inverter: 4 values

Message size (PMU) depends on the used protocol. If MQTT is used containing the headers (56 B fix) and payload with maximum 30 measurement values and the time stamp (20 B per value + 20 B for timestamp), the message size would be 676 B.

Message size (inverter) if MQTT is used containing the headers (56 B fix) and payload with maximum 4 measurement values and the time stamp (20 B per value + 20 B for timestamp), would be 156 B.

Data transfer rate

The data transfer rate for PMU device with the sampling rate of 50 messages per second and if MQTT protocol is used, would be 33.8 KB/s = 270.4 Kbps

The data transfer rate for inverter with the sampling rate of 50 messages per second and if MQTT protocol is used, would be 7.8 KB/s = 62.4 Kbps

Reliability

Usually high reliability is not crucial when grid is stable. However, in critical conditions the highest reliability would be necessary in order to keep the grid stable. Critical conditions are fault on lines, sudden change of load, unplanned disconnection, change in the production because of the weather change. Especially sensitive to changes are small microgrids. E.g., one component is out, or bigger load is introduced. In these cases, very high reliability is necessary.

Usually, higher reliability, low latency and high reporting rate is not necessary.

Availability

Unavailability might cause instabilities in the network. One of the scenario assumes the migration of the control services between the cloud in case of the black-out and thus unavailability of the core cloud, but availability of the edge cloud, which is able to operate independently, and still provide the communication for the devices in it coverage.

High availability (five nines) is generally fine, but in case of systems in moderate conditions and slow dynamics, availability can be much lower, because the components can handle control themselves. Therefore, it has to be tailored to the network and its expected conditions.

Security

Power grid is critical infrastructure and it should be very secure because manipulations could lead to the critical situations even to black outs. Even in the stable conditions, if system is manipulated the system can go unstable especially small microgrids where manipulation of only one point could have much bigger impact than in a bigger grid. Security is even more critical for microgrid.

Table 2-6 shows ICT 5G requirements for the Use Case MV/LV-Grids Monitoring and Control with PMU.

Table 2-6 5G ICT requirements for the Use Case MV/LV-Grids Monitoring and Control with PMU

5G ICT Requirements	Use Case MV/LV-Grids Monitoring and Control with PMU
Req-GMC-endPoints	100’s in rural till 1000’s in urban areas per km^2
Req-GMC-latency	30-50 ms (round-trip)
Req-GMC-sRate	50 messages per second
Req-GMC-mSize	PMU: 676 B, inverter: 156 B (MQTT protocol)
Req-GMC-dtRate	PMU: 270.4 Kbps, inverter: 62.4 Kbps
Req-GMC-reliability	The highest reliability in critical conditions
Req-GMC-availability	99.999% (downtime per month of 26 seconds)
Req-GMC-security	Critical

2.6.3 Timescales and preconditions relevant to the commercial scale use of the Use Case MV/LV-Grids Monitoring and Control with PMU

The service is currently not deployed. Basic preconditions for the large service deployment in commercial networks are as follows:

- Availability of measurement devices in the grid (such as PMUs and smart meters) with higher reporting rate
- Modern communication infrastructure
- Digitalization of the DSO or a party, which manages a prospective microgrid
- Regulations towards grid islanding and control of private grid side inverters

Implementation of different preconditions can lead to the different timescales of the deployment of the service in the commercial networks. Fulfilling certain preconditions like regulations and digitalisation could take longer time (5 years). Availability of measurement devices (PMUs, smart meters) depends on investment, policy of the country as well as country regulations.

2.7 Summary of 5G ICT requirements for N5GEH Use Cases

Table 2-7 shows Energy Use Cases and their 5G ICT requirements. Boundary values are shown in the table.

Energy Use Case / ICT Requirement	Regional VPP	Grid Protection	Building Monitoring	Closed Loop Control within Buildings	District Monitoring and Control in Energy Market	Grid Monitoring / Control with PMU
Number of Endpoints	50K/km^2	300/LV area	8K/building	8K/building	10K/km^2	1K/km^2
Latency [ms] [1]	350	<10	100 [2]	200	6,000	<10
Sampling Rate [messages per second] [3]	0.1	1000	100	1	1/60	50

Message Size [KB]	<1	<1	<1	<1	<1	<1
Data Transfer Rate [Kbps] 4)	0.1	1,568	76	0.7	0.003	270
Reliability 5)	Important	Critical	Important	Important	Critical	Critical
Availability	99.9%	99.999%	99.9%	99.999%	99.999%	99.999%
Security 5)	Important	Critical	Important	Critical	Critical	Critical
Note 1: The lowest required round-trip latency is indicated. *Note 2: Uplink latency (from the sensor to the cloud platform)* *Note 3: The highest required sampling rate per device is indicated.* *Note 4: The highest required data transfer rate per device is indicated.* *Note 5: Informal interpretation by Ericsson of the description of the other project partners.*						

Table 2-7: Summary of 5G ICT requirements for Energy Use Cases

3. 5G ICT concepts and features

This chapter describes 5G features that can be used to optimise the 5G system performance when used to support the N5GEH use cases. The intention of the chapter is to provide to the reader theoretical 5G technology background relevant in this context.

Additionally, information is provided on the Ericsson approach to implementing 5G and on the Ericsson approach to Mission Critical Networks.

3.1 Evolution of mobile networks and introduction to 5G

Compared with previous generations of wireless communications technology (Figure 3-1), including LTE, the rationale for 5G development is to expand the broadband capability of mobile networks, and to provide specific capabilities not only for consumers but also for various industries and society at large, hence unleashing the potential of the Internet of Things (IoT). The overall aim of 5G is to provide ubiquitous connectivity for any kind of device and any kind of application that may benefit from being connected.

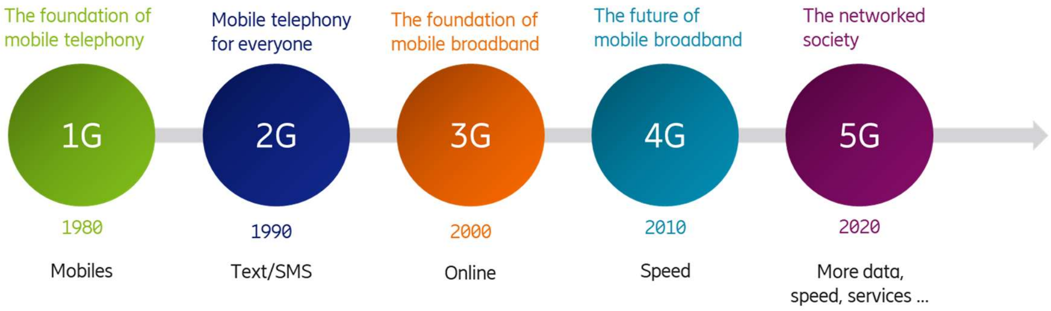

The foundation of mobile telephony
Mobile telephony for everyone
The foundation of mobile broadband
The future of mobile broadband
The networked society
1G
2G
3G
4G
5G
1980
1990
2000
2010
2020
Mobiles
Text/SMS
Online
Speed
More data, speed, services ...

Figure 3-1: Wireless access generations

3.2 Basic 5G functionality

In order to enable connectivity for a very wide range of applications with new characteristics and requirements, the capabilities of 5G wireless access must extend far beyond those of previous generations of mobile communication. These capabilities will include massive system capacity, very high data rates everywhere, very low latency, ultra-high reliability and availability, very low device cost and energy consumption, and energy-efficient networks [6].

5G should support **data rates** exceeding 10 Gbps in specific scenarios such as indoor and dense outdoor environments. **Very low latency** will be driven by the need to support new applications. Some envisioned 5G use cases, such as traffic safety and control of critical infrastructures and industry processes, require much lower latency compared with what is possible with the mobile-communication systems of today. To support such latency-critical applications, 5G should allow for an application end-to-end latency of 1 ms or less. In addition to very low latency, 5G should also enable connectivity with **ultra-high reliability** and ultra-high availability. For example, some industrial applications might need to guarantee successful packet delivery within 1 ms with a probability as high as 99.9999 percent. To enable the vision of billions of wirelessly connected sensors, actuators and similar devices, a further step has to be taken in terms of **device cost and energy consumption**. It should be possible for 5G devices to be available at very low cost and with a battery life of several years without recharging. **Energy efficiency on the network side** has recently emerged as an additional Key Performance Indicator (KPI).

In order to support increased traffic capacity and to enable the transmission bandwidths needed to support very high data rates. 5G will extend the range of frequencies used for mobile communication (Figure 3-2). This includes **new spectrum** below 6GHz, as well as spectrum in higher frequency bands. Frequency spectrum relevant for 5G wireless access therefore ranges from below 1GHz up to 100GHz. The specification of 5G will include the development of a new flexible air interface, New Radio (NR), which will be directed to extreme mobile broadband deployments.

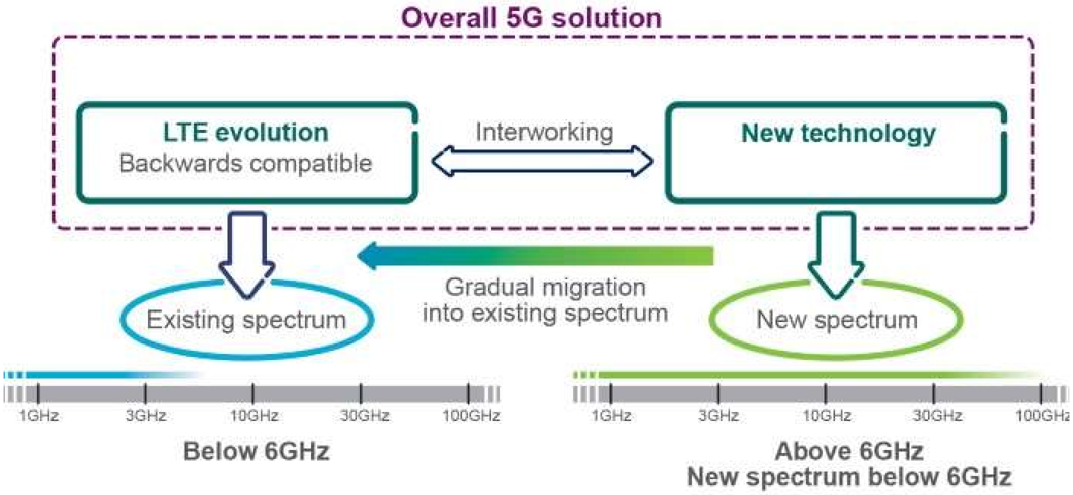


Figure 3-2: 5G Frequency Spectrum for LTE Evolution and New Radio

Note: Reprinted from “5G Radio Access,” 2016, Ericsson white paper, p. 2. Copyright 2016 by Ericsson AB.

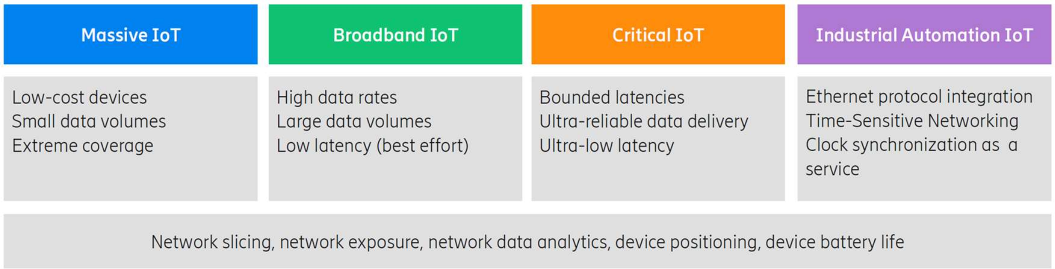
It is important to understand that high frequencies, especially those above 10GHz, can only serve as a complement to lower frequency bands, and will mainly provide additional system capacity and very wide transmission bandwidths for extreme data rates in dense deployments. Spectrum allocations at lower bands will remain the backbone for mobile-communication networks in the 5G era, providing ubiquitous wide-area connectivity.

3.3 Cellular IoT use cases

Cellular Internet of Things (IoT) has the capability to address both the relatively simpler requirements of the Massive IoT market as well as the highly specific, sensitive demands of complex environments and applications [7]. The number of Cellular IoT connections enabled by Narrowband IoT (NB-IoT) and Long Term Evolution for Machines (LTE-M) continues to grow. The number of devices connected by Massive IoT and other emerging cellular technologies is forecast to reach 4.1 billion by 2024.

Cellular IoT itself is a rapidly growing ecosystem based on 3rd Generation Partnership Project (3GPP) global standards, supported by an increasing number of mobile network providers as well as device, chipset, module and network infrastructure vendors. It offers better performance than other Low Power Wide Area (LPWA) network technologies in terms of unmatched global coverage, Quality of Service, scalability, security and the flexibility to handle the different requirements for a comprehensive range of use cases. (Zaidi et al., 2019, p. 2)

The wireless connectivity across various industries can be grouped into four distinct sets of requirements. To address these requirements, Ericsson has defined four IoT connectivity segments: Massive IoT, Broadband IoT, Critical IoT and Industrial Automation IoT, as illustrated in Figure 3-3. Each IoT connectivity segment addresses multiple use cases in multiple industries. (Zaidi et al., 2020, p. 2)



Massive IoT	Broadband IoT	Critical IoT	Industrial Automation IoT
Low-cost devices Small data volumes Extreme coverage	High data rates Large data volumes Low latency (best effort)	Bounded latencies Ultra-reliable data delivery Ultra-low latency	Ethernet protocol integration Time-Sensitive Networking Clock synchronization as a service

Network slicing, network exposure, network data analytics, device positioning, device battery life

Figure 3-3: One 5G network with four multi-purpose IoT connectivity segments

Note: Adapted from “Cellular IoT in the 5G era,” 2020, Ericsson white paper, p. 3.

The **Massive IoT** segment supports very low-cost devices with long battery life, deployed in massive numbers and supporting use cases that demand very low data usage in the networks – use cases such as fleet management or logistics, asset management or smart metering. This segment is already deployed in today’s Long-Term Evolution (LTE) commercial networks and is continuing to grow in terms of ecosystem and numbers of connections.

3GPP standardized three new technologies for massive Machine Type Communications (MTC) in Release 13: Extended Coverage GSM IoT (EC-GSM-IoT), LTE-M and NB-IoT. LTE-M extends LTE with new features for improved battery life, extended coverage and support for low-complexity device category series, named Category M (CAT-M) (Zaidi et al., 2019, p. 4). NB-IoT is a standalone radio access technology based on LTE that enables extreme coverage and extended battery lives for ultra-low complexity devices. (Zaidi et al, 2019, p. 4)

LTE-M and NB-IoT should target complimentary use cases. LTE-M is better suited for applications that require voice connections, lower latency, higher throughput and better positioning. Typical LTE-M use cases include sensors, trackers, wearables, customer support buttons and alarm panels, and all with support for voice and data connections. On the other hand, NB-IoT is the technology of choice for very low throughput applications that are tolerant of delay but require very good coverage, such as simple utility meters and sensors deployed in challenging radio conditions. (Zaidi et al., 2019, p. 4)

The **Broadband IoT** segment uses the capabilities of Mobile BroadBand (MBB) to achieve higher throughput, low latency and larger data volumes than Massive IoT can support and together with some additional functionality can support IoT use cases for drones or unmanned aerial vehicles, augmented reality/virtual reality, automotive, utilities, based on 4G and 5G NR radio access technologies.

The **Critical IoT** enables extremely low latencies and ultra-high reliability at a variety of data rates. This segment addresses extreme connectivity requirements of many advanced wide area and local area applications in intelligent transportation systems, smart utilities, remote healthcare, smart manufacturing and fully immersive augmented reality/virtual reality (Zaidi et al., 2019, p. 4). Powered by the most innovative capabilities of 5G NR, Critical IoT is expected to enable many new use cases within the IoT arena. (Zaidi et al., 2019, p. 4)

For the most complex segment, the **Industrial Automation** segment, some very challenging use cases specific to the industrial campus and manufacturing environments can be supported – use cases such as collaborative robotics which would require functionality such as industrial protocols in addition to time sensitive networks and very precise positioning.

3.4 Device availability

Figure 3-4 shows the approximate timing of 5G device availability [8]. Early Fixed Wireless Access (FWA) devices have been developed to meet market needs in the USA and Australia for example. The first 3GPP-compliant 5G smartphones and tablets are likely to be launched in 2019. To date, the IoT business has primarily been driven by the affordability of devices. Costs of 3GPP-compliant devices have come down significantly recently, and as they approach 5–10 euros, we are starting to see the cellular-delivered IoT market becoming better established. The market for industrial IoT, or critical machine to machine communications, services is at an earlier stage, but will likely be a significant

> market in the longer term. We foresee 3GPP systems becoming the IoT technologies of choice for operators and industry in the longer term. (Ericsson, 2018, p. 5)

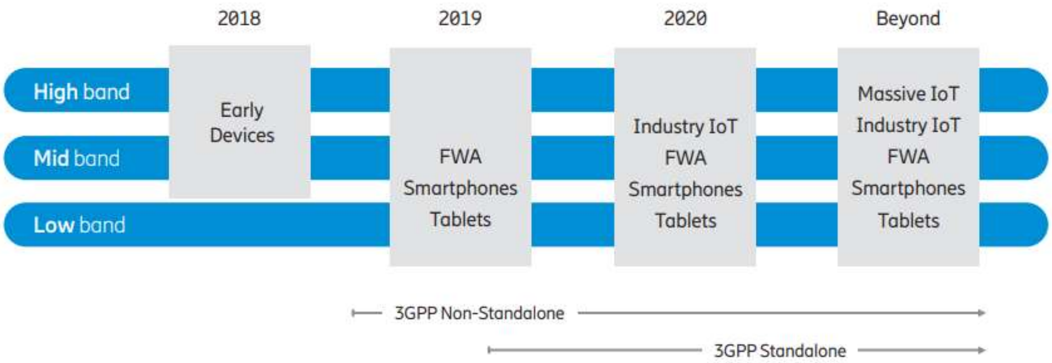


Figure 3-4: 5G device availability

Note: Reprinted from “5G deployment considerations,” 2018, Ericsson white paper, p. 5. Copyright 2018 by Ericsson AB. Reprinted with permission of the authors.

3.5 The global spectrum picture

Figure 3-5 gives a general indication of spectrum availability across all mobile network generations over time [8]. The spectrum available to 5G will vary from market to market, according to whether it is already in use and the timing of auctions and licensing processes (Ericsson, 2018, p. 5).

More spectrum will be needed for 5G, because its benefits are fully achieved in new millimeter wave frequencies, with extremely wide bands. Here, the ultra-high peak rates and low latency are most likely to be used to add new levels of capacity and throughput for enhanced mobile broadband, especially as a way of offloading congested LTE networks (and for new special use cases) (Ericsson, 2018, p. 6). But there is also broad interest in deploying 5G technology in new mid bands (3.5–6GHz) and existing, legacy mid bands (1.8–2.6GHz) as a way of achieving national 5G coverage as rapidly as possible (Ericsson, 2018, p. 6).

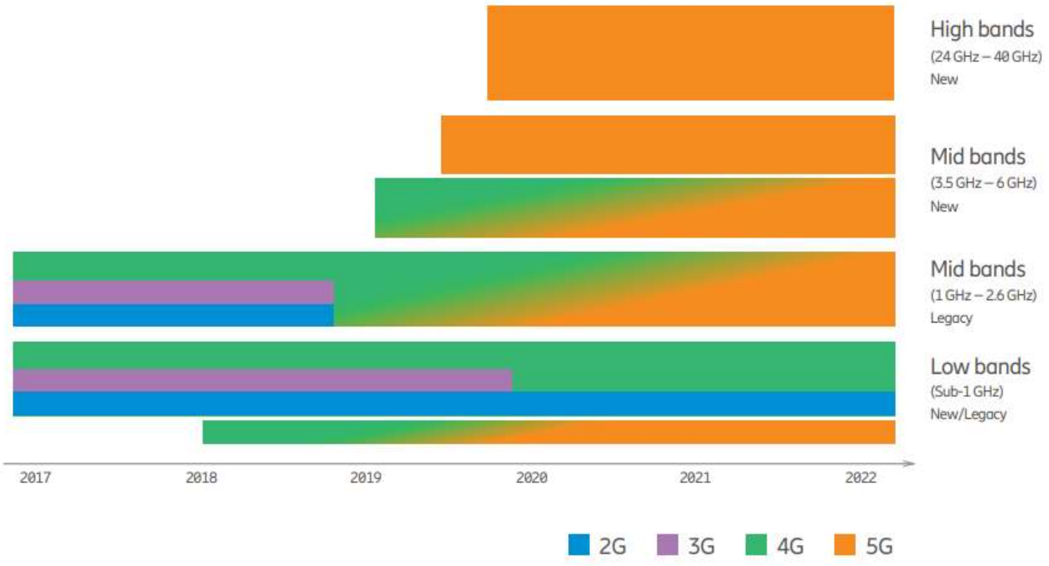


Figure 3-5: Spectrum allocation over time

Note: Reprinted from “5G deployment considerations,” 2018, Ericsson white paper, p. 6. Copyright 2018 by Ericsson AB. Reprinted with permission of the authors.

> Each spectrum band has different physical properties, meaning there are trade-offs between capacity, coverage and latency, as well as reliability and spectral efficiency, as

illustrated in Figure 3-6. If the network is optimized for one metric, there may be degradation of another metric.

Low-band spectrum has historically been used in 2G, 3G and LTE networks for voice and mobile broadband services, as well as broadcast TV. The available bandwidth is typically between 10MHz and 30MHz. This makes this spectrum most suitable for wide-area and outside-in coverage from macro base stations. For a typical 5G mobile broadband use case, capacity and latency are similar to LTE on the same band.

Legacy mid-band spectrum is currently used for 2G, 3G and 4G LTE services. New mid-band spectrum has typically been allocated in 3.5GHz spectrum bands. In these bands, especially in the new higher spectrum, we are likely to see larger bandwidths (50–100MHz). This will enable high-capacity, lower latency networks which can be used for new 5G use cases, with better wide-area and indoor coverage than higher-band spectrum. (Ericsson, 2018, p. 8)

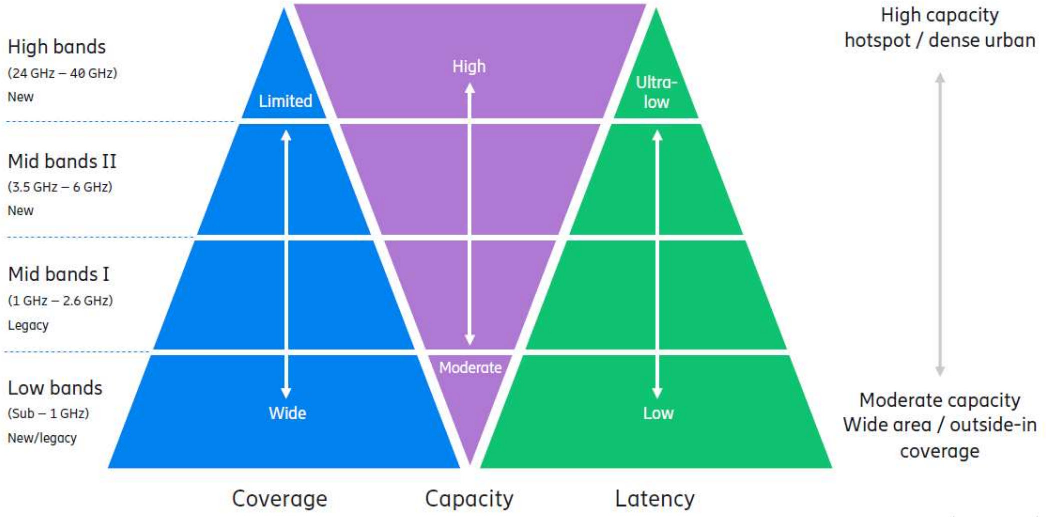


Figure 3-6: Spectrum trade-off

Note: Reprinted from “5G deployment considerations,” 2018, Ericsson white paper, p. 8. Copyright 2018 by Ericsson AB. Reprinted with permission of the authors.

High-band spectrum provides the quantum leap in performance promised by 5G. These new spectrum bands are typically in the 24–40GHz range, with bandwidths in 100MHz (or larger) blocks. Such large bandwidth enables ultra-high spectrum capacity networks (5–10 times higher than today), with latency as low as 1 ms. However, these higher frequencies come with a coverage limitation compared with lower bands. (Ericsson, 2018, p. 9)

5G spectrum harmonization challenge for local industrial networks

Harmonizing the use of spectrum bands across geographies is essential to achieving mass-market conditions which in turn enables cost-efficient and competitive industrial devices. Many countries have already begun to assign spectrum for 5G wide-area cellular networks, and quick regulatory actions and decisions have proven to be highly positive for all ecosystem parties, benefiting service providers and device makers with the ability to make technology investments as well as consumers with the possibility for earlier enjoyment of new generations of technology. Some countries have also begun to consider licensed spectrum as part of industrial digitalization and industrial applications. Germany, for example, allocated local licensed spectrum in 3700–3800 MHz band range to industries for their applications already in 2019, while Japan similarly announced the allocation of the 28 GHz band. Other countries, like France and Italy, are looking primarily at allocating spectrum to Communication Service Providers (CSPs), who then need to ensure the availability of spectrum for industries. The approaches taken differ widely between regulators, and the allocated bands are in many cases shared with incumbents.

Regarding the locally licensed spectrum considered by administrations, these diverse allocations pose challenges to building a device ecosystem for industrial applications.

> Device chipsets need to be supported not only by an ecosystem of traditional mobile broadband (MBB) devices but also by an ecosystem that includes industrial devices of varying complexity on different spectrum bands. These ecosystems, however, are still under formation [9]. (Norin et al., 2020, p. 7-8)

3.6 Network Slicing

The technique of Network Slicing allows for the definition of multiple logical networks (or slices) on top of the same physical infrastructure. Resources can be dedicated exclusively to a single slice or shared between different slices. A network slice is built to address a desired behaviour from the network. Such behaviour can be associated with security, data-flow isolation, quality of service, reliability, independent charging and so on. A network slice may support one or many services and can be used to create a virtual operator network and may provide customized service characteristics. Network slicing can be used for several purposes: a complete private network, a copy of a public network to test a new service, or a dedicated network for a specific service.

For instance, when setting up a private network in the form of a network slice that can be an end-to-end virtually isolated part of the public network, the network exposes a set of capabilities in terms of bandwidth, latency, availability and so on. Thereafter, a newly created slice can be locally managed by the slice owner who will perceive the network slice as his or her own network complete with transport nodes, processing and storage. The resources allocated to a slice can be a mix of centrally located and distributed resources. The slice owner can initiate applications from his or her management center, and applications will simply execute and store data, either centrally, in a distributed management system or a combination of both.

3.7 Ultra-Reliable and Low Latency Communication

5G NR and 5G core have been standardized for Ultra-Reliable and Low Latency Communication (URLLC) from day one (Rel-15) with further evolution in Rel-16 and Rel-17 [7]. With URLLC capabilities, 5G NR can achieve latencies down to 1 ms and reliability up to 99.9999%. Latency within the core network is typically below 1 ms. The transport network can be a major contributor to the end-to-end latency. Transport network latency varies widely between regions, depending on distances and the transport solutions used. A general trend is that transport latency is being optimized by higher availability of fiber and fewer router hops. As an example, the round-trip time between 2 cities in a European country (city distance 1,300 km) is today just 16 ms (theoretical minimum optical fiber latency is 13 ms), which is less than half of the latency of 5 years ago.

Stand-alone 5G is ideal for fulfilling the challenging Critical IoT requirements. 5G core is better than 5G evolved packet core in terms of ultra-reliability mechanisms, advanced service differentiation, flexible edge computing, network data analytics, advanced Quality of Service (QoS), Ethernet connectivity, and end-to-end network slicing capabilities which can be important for critical use cases. Provided that LTE is also not enhanced for Critical IoT, Non-Stand-Alone (NSA) 5G does not offer full potential for URLLC from both radio access and core network perspectives. However, in wide area coverage, 5G deployments would be initially NSA and could leverage NR user plane capabilities for URLLC to enable less demanding Critical IoT use cases. Over time, NSA 5G deployments will transition to SA 5G, achieving the full potential of Critical IoT in wide areas.

3.8 Edge Computing

As shown in Figure 3-7, Ericsson defines the **Distributed Cloud** [10] as a cloud execution environment that is geographically distributed across multiple sites, including the required connectivity in between, managed as one entity and perceived as such by applications. The key characteristic of our distributed cloud is abstraction of cloud infrastructure resources, where the complexity of resource allocation is hidden to a user or application. Our distributed cloud solution is based on Software Defined Networking (SDN), Network Functions Virtualization (NFV) and 3GPP edge computing technologies to enable multi-access and multi-cloud capabilities and unlock networks to provide an open platform for application innovations.

Ericsson Distributed Cloud solution enables edge computing, which many applications require. It defines **Edge Computing** as the ability to provide execution resources (specifically compute and storage) with adequate connectivity at close proximity to the data sources.

The distributed cloud relies on efficient **management and orchestration** capabilities that enable automated application deployment in heterogeneous clouds supplied by multiple actors. Figure 3-7 illustrates how the service and resource orchestration spans across distributed and technologically heterogeneous clouds. It enables service creation and instantiation in cloud environments provided by multiple partners and suppliers. When deploying an application or a Virtual Network Function (VNF), the placement decisions can be based on multiple criteria, where latency, geolocation, throughput and cost are a few examples. These criteria can be defined either by an application developer and/or a distributed cloud infrastructure provider, serving as input to the placement algorithm.

Each of the layers in the distributed cloud stack will expose its capabilities. The cloud infrastructure layer and the connectivity layer will expose their respective capabilities through the **Appplication Programming Interface(s)** (API(s)), which will then be used by application developers of the industries making use of the mobile connectivity. By setting developer needs in focus, the exposed API(s) will be abstracted so that they are easy to use.

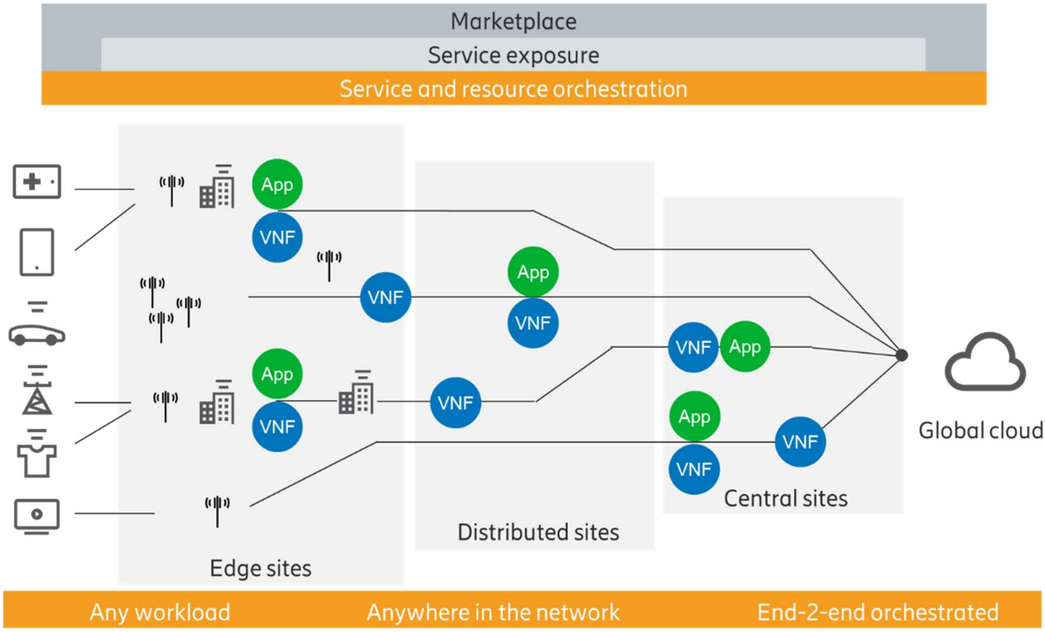


Figure 3-7: Distributed Cloud architecture

Note: Diagram adapted from “Distributed cloud, Automotive and Industry 4.0,” 2018, Ericsson Technology Review, p. 7. Copyright 2018 by Ericsson AB.

3.8.1 Edge Computing concepts

Edge Computing places high-performance compute, storage and network resources as close as possible to end users and devices [11]. Doing so lowers the cost of data transport, decreases latency, and increases locality. Edge Computing will take a big portion of today’s centralized data centers and cloud and put it in everybody’s backyard. (State of the Edge 2018, 2018, p. 9)

Edge Computing can be split into two layers: Device Edge and Infrastructure Edge layer. **Infrastructure Edge** can be further split into two sublayers: Access Edge and Aggregation Edge sublayer.

Device Edge

The Device Edge refers to edge computing resources on the device side of the last mile network. Some devices will be single function, such as embedded sensors, designed to perform very specific tasks and deliver streams of data to the network. Other edge devices will act as specialized gateways, aggregating and analysing data and providing some control functions. And yet other edge devices will be fully-programmable compute nodes, capable of running complex applications in containers, virtual machines, or on bare metal. The Device Edge will be the basis of many useful applications which require the lowest possible latency, as device edge resources are as close as it is possible to be to the end user.

However, it is already clear that many device edge resources will be connected to the cloud and be managed as extensions of the cloud. They will largely be connected to the Infrastructure Edge (IT resources which are positioned on the network operator or service provider side of the last mile network) over wired and wireless networks and that workloads running on the Device Edge will be coordinated with workloads running on the Infrastructure Edge. In many cases it will be both more reliable and less expensive to run workloads on the Infrastructure Edge rather than entirely on the edge devices. (State of the Edge 2018, 2018, p. 18)

Access Edge

The Access Edge is the part of the Infrastructure Edge closest to the end user and their devices. Edge data centers deployed at or very near to the Access Edge are typically directly connected to a radio or other front-line network infrastructure, and they are used to operate application workloads for complex tasks such as machine vision and automated decision support for large-scale IoT. Edge data centers deployed at the Access Edge, a sublayer within the Infrastructure Edge, may also connect to other edge data centers which are deployed above them in a hierarchical architecture at the Aggregation Edge sublayer. (State of the Edge 2018, 2018, p. 21)

Aggregation Edge

The Aggregation Edge refers to a second sublayer within the Infrastructure Edge which functions as a point of aggregation for multiple edge data centers deployed at the Access Edge sublayer. The purpose of this layer is to provide a reduced number of contact points to and from other entities, such as a centralized cloud data center and the Infrastructure Edge and to facilitate the collaborative processing of data from multiple Access Edge sublayer edge data centers. The Aggregation Edge is typically two network hops from its intended users but is still much closer to them than the centralized cloud data center, and it is thus able to achieve far lower latencies. (State of the Edge 2018, 2018, p. 21)

Cloud interoperation

Figure 3-8 shows edge computing layers and its relation to the central cloud. It is important to notice that the edge computing does not exist by itself. Despite the level of computing power and performance that is achievable between the combination of the Device Edge and Infrastructure Edge, both of these entities benefit immensely from tight, cohesive interoperation with the centralized cloud. (State of the Edge 2018, 2018, p. 23)

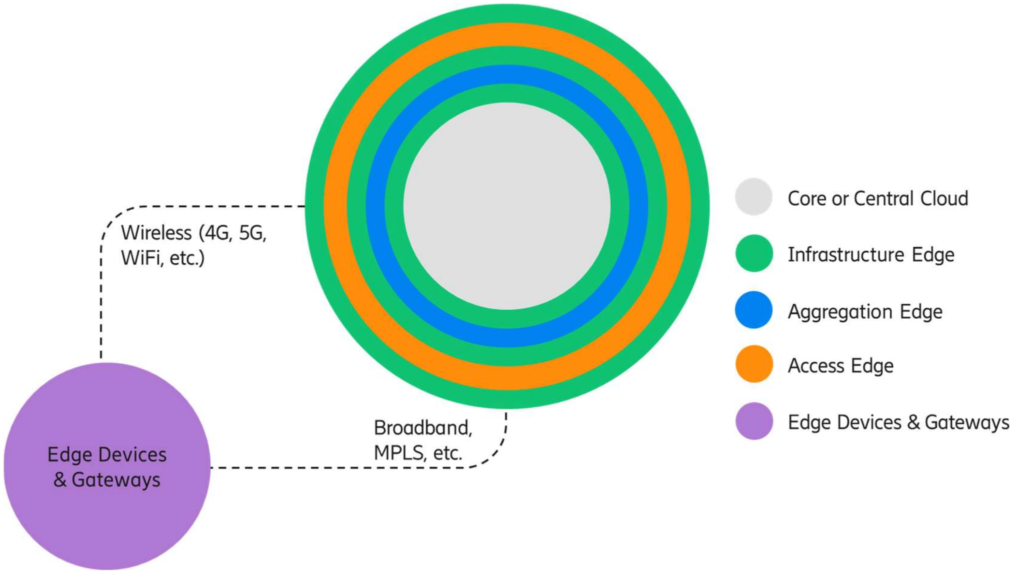


Figure 3-8: Distributed Cloud layers

Note: Adapted from “State of the edge 2018: A Market and Ecosystem Report for Edge Computing,” 2018, p. 23.

As can be seen in

Figure 3-8, both the Device and Infrastructure Edge can be viewed as complementary to, and even as extensions of, the existing centralized cloud (State of the Edge 2018, 2018, p. 23). By connecting these distributed resources together and creating an edge cloud which spans from the current centralized data center, through the Infrastructure Edge and its sublayers through to the Device Edge, the cloud operator will be able to optimally allocate resources and direct Grid Awareness services workloads to the optimal location for them, regardless of whether that is in the Device Edge, Infrastructure Edge or the centralized cloud. For the optimal deployment of the Grid Awareness services, power grid characteristics, e.g., number of nodes, meshed grid, density, area spanned by a DSO, will have to be taken into consideration.

Edge-native applications, as their name suggests, are applications which require the unique characteristics provided by edge computing to function satisfactorily, or in some cases to function at all. These applications will typically rely on the low latency, locality information or reduced cost of data transport that edge computing provides in comparison to the centralized cloud. (State of the Edge 2018, 2018, p. 28)

3.8.2 Cloud Radio Access Network

Cloud Radio Access Network (C-RAN) is a novel mobile network architecture which can address a number of challenges that mobile operators face while trying to support ever-growing end-users’ needs towards 5th generation of mobile networks (5G) [12]. The main idea behind C-RAN is to split the base stations into radio and baseband parts[2], and pool the BaseBand Units (BBUs) from multiple base stations into a centralized and virtualized BBU Pool, while leaving the Remote Radio Heads (RRHs) and antennas at the cell sites. This gives a number of benefits in terms of cost and capacity. (Checko, 2016, p. v)

C-RAN architecture is targeted by mobile network operators, as envisioned by China Mobile Research Institute, IBM, Alcatel-Lucent, Huawei, ZTE, Nokia Siemens Networks, Intel and Texas Instruments. Moreover, C-RAN is seen as a typical realization of mobile network supporting soft and green technologies in fifth generation (5G) mobile networks. (Checko, 2016, p. 8)

Figure 3-9 shows an example of a C-RAN mobile LTE network. The fronthaul part of the network spans from the RRHs sites to the BBU Pool. The backhaul connects the BBU Pool with the mobile core network. At a remote site, RRHs are co-located with the antennas. RRHs are connected to the high-performance processors in the BBU Pool through low latency, high bandwidth optical transport links. (Checko, 2016, p. 12)

[2] Baseband refers to the original frequency range of a transmission signal before it is converted, or modulated, to a different frequency range. For example, an audio signal may have a baseband range from 20 to 20,000 hertz. When it is transmitted on a radio frequency, it is modulated to a much higher, inaudible, frequency range.

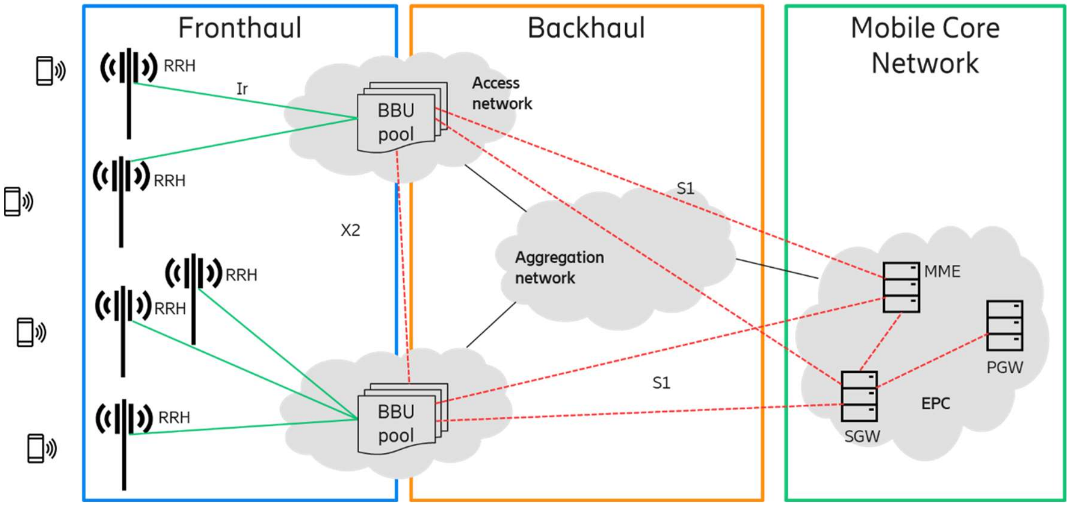


Figure 3-9: C-RAN LTE mobile network

Note: Adapted from “Cloud Radio Access Network architecture. Towards 5G mobile networks,” 2016, Technical University of Denmark, p. 14.

3.9 5G security

Connected devices and mobile applications require wireless network access that is resilient, secure and able to protect individuals’ privacy, and the 5G system is designed with these requirements in mind (Norrman et al., 2021, p. 1) [13]. Figure 3-10 shows five core properties that contribute to the trustworthiness of the 5G system: resilience, communication security, identity management, privacy and security assurance. These properties of the 5G system contribute toward creating a trustworthy communications platform that is an ideal foundation on which to build large-scale, security-sensitive systems, including those used in industrial settings.

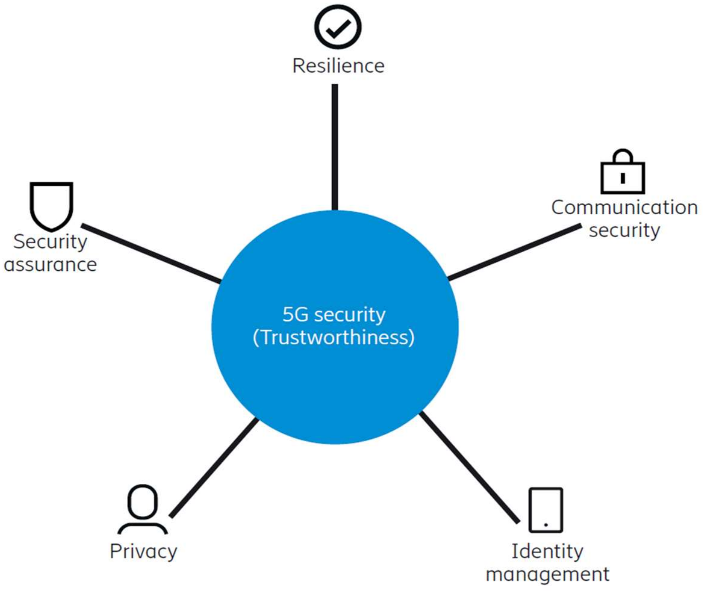


Figure 3-10: Five properties that contribute to the trustworthiness of the 5G system

Note: Diagram reprinted from “5G security – enabling a trustworthy 5G system,” 2021, Ericsson white paper, p. 5. Reprinted with permission of the authors.

Resilience

The 5G system's resilience to cyberattacks and non-malicious incidents comes through a variety of complementary and partially overlapping features. First, the 5G NR access was developed for Ultra-Reliable Low Latency Communications (URLLC). Even greater resilience against failures and attacks can be obtained by deploying a single base station as two split units, called a central unit and a distributed unit. This split also facilitates customizable deployment of security sensitive functions of the 5G NR access, such as user plane encryption, in a secure central location while keeping non-security sensitive functions in less secure distributed locations. Next, the 5G core network architecture itself is designed around resilience concepts. For example, network slicing isolates groups of network functions from other functions. Service Based Architecture principles are another architectural concept that enhances resilience. These principles make use of software and cloud-based technologies that improve on the more static and node-centric designs of previous generation networks. The resilience of the 5G system also stems from the strong mobility support that it shares with previous generation 3GPP networks, which ensures continuous secure connectivity for devices moving from one location to another. In addition to these general features providing resilience, there are more specialized functions introduced to operate a radio access network in extreme situations, such as when it has become separated from its core network. This is called isolated Evolved UMTS (Universal Mobile Telecommunication System) Terrestrial Radio Access Network (E-UTRAN) operation for public safety in LTE/5G and is very useful in disaster areas, for example. Finally, partly due to strong regulations and associated high fines, cellular networks have long adhered to high carrier-grade availability requirements. (Norrman et al., 2021, p. 5-6)

Communication security

The 5G system provides secure communication for devices and for its own infrastructure. In particular, the new Service Based Architecture (SBA) for core network communication takes threats from the interconnect network into account. The 5G system includes protection against eavesdropping and modification attacks. Signalling and user plane traffic is encrypted and can be integrity protected. The strong and well-proven security algorithms from the LTE system are reused. These are encryption algorithms based on SNOW 3G (word-based synchronous stream cipher with name SNOW) [14], Advanced Encryption Standard Counter (AES-CTR) [15], and ZUC (Cryptographic algorithm with name ZUC) [16]; and integrity algorithms based on SNOW 3G, Advanced Encryption Standard Cipher-based Message Authentication Code (AES-CMAC) [17], and ZUC. The main key derivation function is based on the secure Hash-based Message Authentication Code Secure Hashing Algorithm 256-Bits (HMAC-SHA-256) [18]. Mobility in the 5G system also inherits different security features from the LTE system. (Norrman et al., 2021, p. 6-7)

Identity management

At its heart, the 5G system has secure identity management for identifying and authenticating subscribers, roaming or not, ensuring that only the genuine subscribers can access network services. It builds on strong cryptographic primitives and security characteristics that already exist in the LTE system. One of the most valuable new security features in the 5G system is the new authentication framework where mobile operators can flexibly choose authentication credentials, identifier formats and authentication methods for subscribers and IoT devices. Previous mobile network generations required physical Subscriber Identity Module (SIM) cards for credentials, but the 5G system also allows other types of credentials such as certificates, pre-shared keys and token cards. Another valuable new security feature is the ability of a subscriber's operator to determine the presence of the subscriber during an authentication procedure – even when roaming. The 5G system also inherits a mechanism from legacy systems, called Equipment Identity Register (EIR) check, which can be used to prevent stolen devices from using the network services, thereby discouraging device theft. (Norrman et al., 2021, p. 7)

Privacy

Data traffic, including phone calls, internet traffic and text messages, is protected using state-of-the-art encryption. The devices and the network mutually authenticate each other and use integrity-protected signalling. Another privacy enhancement is protection of subscriber identifiers, both long-term and temporary, e.g., subscriber's long-term identifier concealment mechanism that is based on the Elliptic Curve Integrated

Encryption Scheme (ECIES) [19]. In addition, the 5G system enforces a stricter policy for update of temporary identifiers. Further, the 5G system is also able to detect false base stations that are the root cause of International Mobile Subscriber Identity (IMSI) or Temporary Mobile Subscriber Identity (TMSI) catchers. (Norrman et al., 2021, p. 8)

Security assurance

In 3GPP, security assurance is a means to ensure that network equipment meets security requirements and is implemented following secure development and product lifecycle processes. This assurance is especially important for mobile systems, as they form the backbone of the connected society and are even classified as critical infrastructure in some jurisdictions. 3GPP and Global System for Mobile communications Association (GSMA) took the initiative to create a security assurance scheme called the Network Equipment Security Assurance Scheme (NESAS) [20], which is suitable to the telecom equipment lifecycle. NESAS comprises two main components: security requirements and an auditing infrastructure. The security requirements defined on node basis and collected in so-called SeCurity Assurance Specifications (SCAS) are defined jointly by operators and vendors in 3GPP. The auditing infrastructure is governed by the GSMA, the global mobile operator organization, that conduct the audits of vendors' development and testing processes. (Norrman et al., 2021, p. 8)

3.10 5G public and private networks

New 5G deployment architectures options are being investigated considering public and non-public network deployment options for verticals such as manufacturing [21]. In the coming years, 5G will enable many new industrial automation applications using public and non-publicly operated 5G networks. Private networks can be deployed as isolated, standalone networks and in conjunction with a public network. In certain deployments of a private network in conjunction with a public network, private and public networks can share part of a Radio Access Network (RAN). 3GPP specifications include functionality that enables RAN sharing [22].

3.11 Ericsson Mission Critical Network deployment models and the evolution to 5G

Built on the leading 4G and 5G technology, Ericsson's cutting-edge Mission Critical Networks and related applications are designed to complement or replace existing national or regional Land Mobile Radio (LMR) networks, providing comprehensive voice, data and video services [23].

Ericsson Mission Critical Networks offering leverages the entire Ericsson portfolio, spanning areas such as radio, core networking infrastructure, network management, operational and business support systems, expert analytics, security and services. It includes enhanced features and capabilities to ensure mission-critical grade performance in the areas outlined in the figure below:

- Network availability: High availability required to safeguard lives, property and business operations.
- Multi-network operation: Delivering the required networking infrastructure and level of control, whilst optimizing overall investment cost.
- Coverage and capacity: Extending network coverage and capacity for mission-critical users; beyond what is typically available for commercial users.
- Security and hardening: Providing multi-layer security, and addressing operational and regulatory requirements.
- QoS, priority and pre-emption: Control of application priority to guarantee latency and capacity requirements.

3.11.1 Mission Critical Network deployment models and the evolution to 5G

The evolution from legacy LMR to 3GPP networks allows a wider range of network deployment models to be used, and more cost-effective solutions to be delivered. These range from isolated networks to commercial mobile networks with specialist embedded mission critical capabilities. Figure 3-11 shows some of the models currently in use.

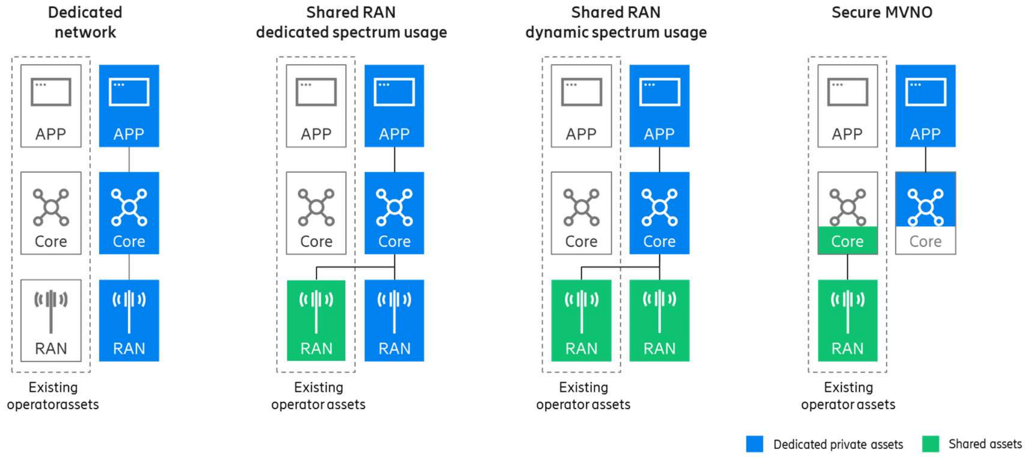


Figure 3-11 Nationwide mission critical 4G networks, leveraging CSP existing RAN coverage

Note: Reprinted from “Enabling intelligent operations with Mission Critical Networks,” 2021, Ericsson white paper, p. 7. Copyright 2021 by Ericsson AB. Reprinted with permission of the authors.

Dedicated networks

A service provider can establish a dedicated critical communications network that is run on separate infrastructure from its commercial network, although both networks can share physical sites and transmission facilities.

Shared RAN – dedicated spectrum usage

By enabling RAN sharing, the service provider can complement the use of its of commercial network with dedicated apps as well as core and RAN infrastructure. This was the initial model for the French Ministry of Interior.

Shared RAN – dynamic spectrum usage

Critical communication users and consumers benefit from shared access to the commercial network’s RAN as well as dedicated RAN, though critical communication users have priority. AT&T took this approach with FirstNet in the US. The public safety operator Erillisverkot in Finland uses shared RAN in a mobile operator core network (MOCN) configuration with a dedicated core.

Secure mobile virtual network operator (S-MVNO)

This model relies on the shared use of the commercial network RAN along with routing capabilities in the core. But this is complemented with a dedicated core (complete or upper part only) and applications to partition sensitive user and network data. Now operational, the UK’s Emergency Services Network is an example of this type of model.

3.11.2 The Journey to mission critical 5G

Many of the 3GPP mission critical network enablers are already standardized for 5G, but some will be standardized in Release 17. Meanwhile, the standardization of integrating mission critical push to-X services with the network is being planned for Release 18. At present, the LTE path of a non-standalone 5G network can be used to support the mission critical services, and the 5G New Radio (5G NR) path can be used for data offload (see Figure 3-12).

From 2022, NR deployments are likely to be more widespread, and more mission critical 5G devices will be generally available. NR-supported use cases will become a reality. These include real-time drone control using ultra-reliable low latency communication (URLLC), or multiple real-time bodycam streaming during major incidents – taking advantage of the high throughput enabled by NR. Mission critical push-to-talk will continue to be supported on the LTE path of the network since critical networking

> capabilities, such as broadcast and device-to-device communications, will not yet be available on 5G NR.
>
> As we approach 2024-2025, there will be the possibility for a mission critical network to evolve to a full standalone 5G network using just NR as the radio interface, if so desired, running all mission critical services on mission critical 5G devices. (Ericsson, 2021, p. 6-8)

Note that if mission critical push-to-talk service is not applicable for the considered energy use cases, then a full standalone 5G network deployment would be possible earlier.

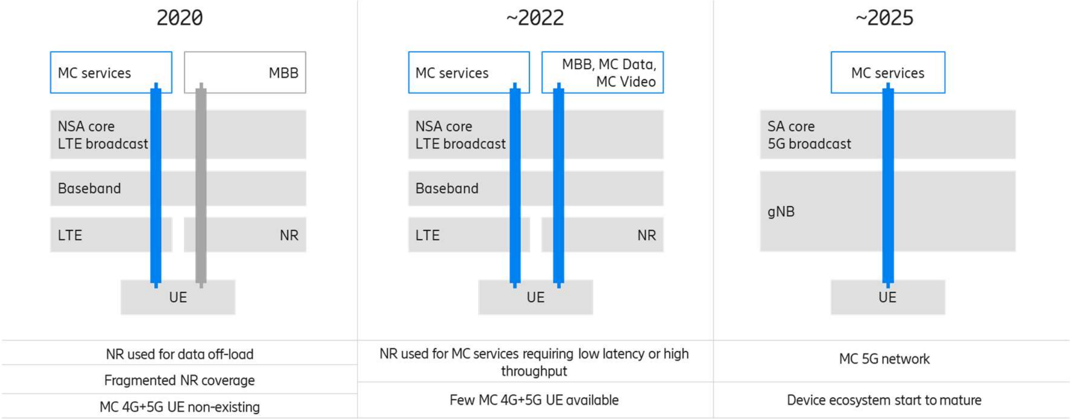


Figure 3-12 The Journey to mission critical 5G

Note: Reprinted from "Enabling intelligent operations with Mission Critical Networks," 2021, Ericsson white paper, p. 8. Copyright 2021 by Ericsson AB. Reprinted with permission of the authors.

3.12 The Ericsson approach to Network Slicing

Ericsson has developed a complete network slicing portfolio from business support systems (BSS), operations support systems (OSS) to end-to-end networks functions (Figure 3-13 below). Multiple end-to-end slices can be deployed with the purple, yellow, green and orange slices, orchestrated across radio access network (RAN), transport and core nodes. On the left-hand side, a simplified view of RAN slicing architecture is shown, and in the center, transport network supporting the same slices. On the right, shared or dedicated virtualised mobile network nodes are shown as cloud-native applications. Network slice policies are mapped across all node with the help of common unique Slice ID. This is called Single - Network Slice Selection Assistance Information, or S-NSSAI for short.

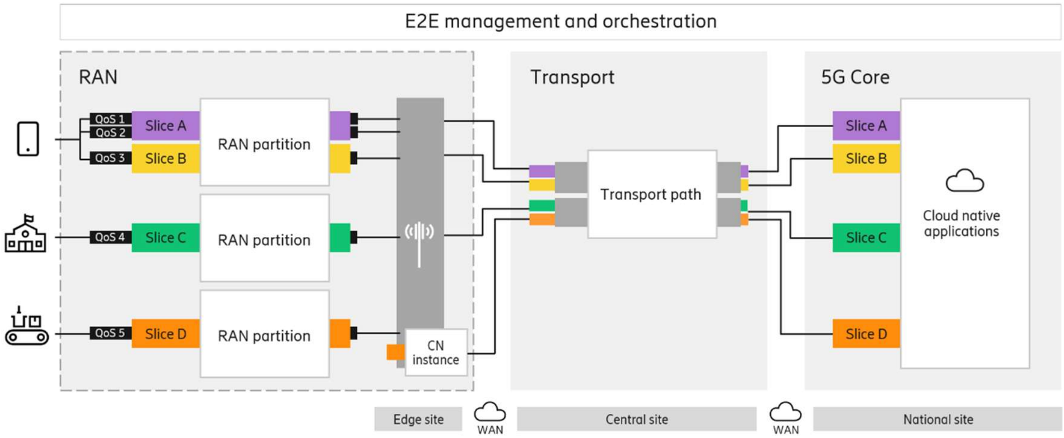


Figure 3-13: 5G Network Slicing

Note: Diagram reprinted from "5G RAN Slicing - Commercial presentation" 2021, p. 8. Reprinted with permission of the authors.

3.13 The Ericsson two-phased approach to 5G deployment

> As 5G will need to coexist and interwork with LTE for many years to come, we are likely to see the vast majority of these deployments as Non-Stand-Alone (NSA) initially, as a way of reducing time to market and ensuring good coverage and mobility [8]. The 5G stand-alone (SA) mode, which requires a new (service-based) core network architecture (known as 5G Core, or 5GC), will enable deployments of 5G as an overlay to, or independent, of LTE coverage.
>
> To achieve nationwide coverage as fast as possible, we're also likely to see 5G deployed in low/mid bands, which will also be suitable for massive IoT use cases in the future. SA 5G in high bands is more likely to be used mainly for data offload in high-traffic areas, as separate networks in factories or campuses, and for critical IoT in data-intensive applications. (Ericsson, 2018, p. 9)

Ericsson favours a two-phase approach to deploying 5G as shown in Figure 3-14. 3GPP standardized options shown in the figure are followed. In the phase 1 (left half of the figure), enhanced MBB and low latency IoT use cases are supported. This is referred to as 5G NSA mode. In the phase 2 (right half of the figure), 5G network operates in SA mode, with both control and user planes carried over 5G NR access.

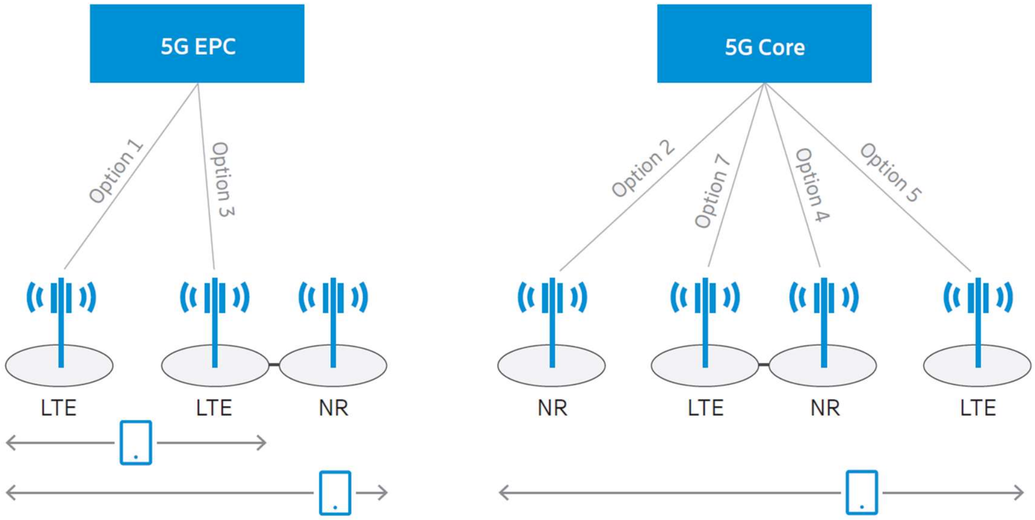


Figure 3-14: LTE-NR connectivity options towards Evolved Packet Core and 5G Core

Note: Reprinted from “5G deployment considerations,” 2018, Ericsson white paper, p. 11. Copyright 2018 by Ericsson AB. Reprinted with permission of the authors.

3.14 Conclusions

5G networks have many currently available and forthcoming features suitable for supporting the N5GEH use cases. In particular, network slicing, distributed cloud and URLLC features will enable lower latencies and higher levels of communications resilience in coming years as they become more widely available on the market. Mission Critical Networks increasingly offer 5G-based solutions tailored to the needs of critical infrastructure owners, such an energy system operators.

4. 5G ICT Solutions for N5GEH Use Cases

This chapter describes 5G and mobile communications components of the solutions for all N5GEH use cases.

4.1 Use Case 1: Regional Virtual Power Plant

The following 5G ICT solutions and recommendations are proposed for this use cases (they are described in further details in Chapter 4.6):

- Providing communications links to new endpoints in the energy system
- Use of public 5G and LTE networks without network slicing
- Public networks can be utilised. However, it should be kept in mind that security of communications is important factor assuring data privacy (user behaviour patterns could be identified through analysis of the sensors information).
- Mobile networks for massive IoT communications
- Good signal penetration is needed to reach the end device often placed in basements especially in residential areas.
- Use of non-public LTE or 5G campus networks
- Non-public also sometimes called private networks are applicable for the usage in office and industry buildings for secured communications and hardly reachable devices.
- Mission critical LTE and 5G networks offer configurations specifically tailored to the needs of mission critical use cases and operations such as those of this use case
- Using Distributed Edge Cloud features to increase reliability and provide local hosting of algorithms
- Use of communications friendly protocols to maximise the reliability of the communications
- Classical power protocol will be preferred by some companies and can be expected to use in the future. In research framework MQTT is mostly used. In the future ICT oriented lightweight protocols like MQTT would be more efficient.

Note that 5G networks can be utilised in RVPP Use Case if available but it is not mandatory because the use case requirements can be met with existing LTE networks except when reliability and security are of upmost importance. In such exceptional cases, 5G network slicing can be utilised.

4.2 Use Case 2: Grid Protection (FLISR)

Generally advanced LTE and critical IoT networks can be utilised in this use case having in mind lower quality of the service as it can partly fulfil stringent latency requirement. Also, usage of public LTE or 5G networks is not recommended except reliable communications is guaranteed, e.g., by using network slicing.

The following 5G ICT solutions and recommendations are proposed for this use cases (they are described in further details in Chapter 4.6):

- Providing communications links to new endpoints in the energy system
- Mobile networks for massive IoT communications
- Mission critical LTE and 5G networks offer configurations specifically tailored to the needs of mission critical use cases and operations such as those of this use case
- Use of end-to-end latency services
- Using Distributed Edge Cloud features to increase reliability and provide local hosting of algorithms
- Network Slicing for energy provider control of QoS and security features

- Use of communications friendly protocols to maximise the reliability of the communications

4.3 Use Case 3: Smart Buildings Monitoring and Closed Loop Control

Utility applications are beginning to be deployed today with LTE technology. The LTE standard contains specific techniques to enable low-bandwidth, very low power devices to coexist in the same network as high-performance smartphones. 5G builds on these LTE capabilities, enabling even higher scalability of device density.

Indoor 5G network will complement outdoor 5G network architectures [24]. Indoor 5G network architectures will begin with migration of existing low bands (sub-1 GHz) to New Radio (NR) bands. These will primarily be outdoor high-power macro radios. Specific improvements in 5G standards will improve cell-edge performance over LTE, which will help outdoor-in coverage to extend. This enables deployments of massive number of devices with LTE technology today, with a path to even higher scalability after 5G migration. Low-band outside-in LTE or 5G network deployments for massive number of devices will be complemented as needed by low-band indoor in extreme cases.

As indoor networks have evolved over several generations of wireless standards, a number of deployment architectures have been developed – distributed antenna systems, uncoordinated small cells and distributed radio systems. Among these architectures the distributed radio architecture is the most optimal for the building use cases because it provides the following advantages:

- Enables easy selective deployment in limited areas
- Flexible capacity assignment between bands
- Ability to share common radio access network capacity with outside low band coverage

Most recently, the Distributed Radio architecture was introduced. Distribute radios ensure high radio frequency signal dominance throughout a venue due to placing many low-power transmitters close to the users. Distributed radio systems can often use low-cost IT-grade cabling for both signalling and power and have low unit cost.

The following 5G ICT solutions and recommendations are proposed for this use cases (they are described in further details in Chapter 4.6):

- Providing communications links to new endpoints in the energy system
- Wireless connections with the devices especially would be cost efficient especially in the existing buildings that usually are not built to support advanced building efficiency.
- Use of public 5G and LTE networks without network slicing
- Public networks can be utilised in building monitoring use case, not for control use case. However, it should be kept in mind that security of communications in the monitoring use case is important assuring data privacy (user behaviour patterns could be identified through analysis of the sensors information).
- Mobile networks for massive IoT communications
- Mission critical LTE and 5G networks offer configurations specifically tailored to the needs of mission critical use cases and operations such as those of this use case
- Good signal penetration needed to reach because of a lot of components are placed in basements especially in residential areas
- Use of non-public LTE or 5G campus networks
- Applicable for the usage in office and industry buildings for secured communications and hardly reachable devices.
- Using Distributed Edge Cloud features to increase reliability and provide local hosting of algorithms
- Edge Infrastructure can be utilised in several reasons mentioning a few of them: enabling decentralised and scalable computing and avoids a lock-in of systems to devices from specific manufacturers, the gathered data in the cloud can be displayed in real time by authorized users, processing of data can be done locally.

- Network Slicing for energy provider control of QoS and security features
- Reliable and secured communications channels are needed for critical operations like fire alerts that has higher priority as normal daily operations.
- Use of communications friendly protocols to maximise the reliability of the communications
- Classical power protocol will be preferred by some companies and can be expected to use in the future. In research framework MQTT is mostly used. In the future ICT oriented lightweight protocols like MQTT would be more efficient.

4.4 Use Case 4: District Monitoring and Control in Energy Market

The following 5G ICT solutions and recommendations are proposed for this use cases (they are described in further details in Chapter 4.6):

- Providing communications links to new endpoints in the energy system
- Cost efficient deployment of smart gateways will be beneficial.
- Mobile networks for massive IoT communications
- Mobile networks characterised by wide area coverage and good signal penetration abilities can be utilised to ensure reliable connections to the smart gateway that will be often located in hardly reachable locations (basement).
- Use of non-public LTE or 5G campus networks
- Non-public campus networks are applicable for the usage in office and industry buildings for secured communications and hardly reachable devices
- Mission critical LTE and 5G networks offer configurations specifically tailored to the needs of mission critical use cases and operations such as those of this use case
- Using Distributed Edge Cloud features to reduce the latency requirements and provide local hosting of algorithms
- Edge Infrastructure can be utilised in several reasons mentioning a few of them: enabling decentralised and scalable computing and avoids a lock-in of systems to devices from specific manufacturers, the gathered data in the cloud can be displayed in real time by authorized users, processing of data can be done locally.
- Network Slicing for energy provider control of QoS and security features
- Added value services requests highly reliable and secured communications.

4.5 Use Case 5: MV/LV-Grids Monitoring and Control with PMU

Advanced LTE and critical IoT networks can be utilised in this Use Case having in mind lower quality of the service as it can partly fulfil stringent latency requirement. Also, usage of public LTE or 5G networks is not recommended except reliable communications is guaranteed, e.g., by using network slicing.

The 5G ICT solutions and recommendations for Use Case GP are listed below and described in detail in Chapter 3:

- Providing communications links to new endpoints in the energy system
- Mobile networks for massive IoT communications
- Mobile networks characterised by wide area coverage and good signal penetration abilities can be utilised to ensure reliable connections to the devices like PMUs deployed in the grid and devices in buildings that will be often located in hardly reachable locations (basement).
- Use of non-public LTE or 5G campus networks
- Non-public campus networks are applicable for the usage in office and industry buildings for secured communications and management of high number devices installed in the building and communications with hardly reachable devices.

- Mission critical LTE and 5G networks offer configurations specifically tailored to the needs of mission critical use cases and operations such as those of this use case
- Use of end-to-end latency services
- Low latency is critical especially in grids with high density of renewable energy sources, or in volatile weather conditions, or number of faults happening in the network.
- Using Distributed Edge Cloud features to increase reliability and provide local hosting of algorithms
- In critical conditions (fault on lines, sudden change of load, unplanned disconnection, change in the production because of the weather change) the highest reliability would be necessary in order to keep the grid stable.
- Network Slicing for energy provider control of QoS and security features
- Use of communications friendly protocols to maximise the reliability of the communications

4.6 Summary of 5G ICT Solutions for N5GEH Use Cases

This section describes the 5G ICT solutions relevant for the Energy Use Cases elaborated in this document. Relationships between the 5G ICT solutions and the Energy Use Cases are indicated in Table 4-1.

Energy Use Cases 5G ICT Solutions	Regional VPP	Grid Protection	Smart Buildings Monitoring and Control	District Monitoring and Control in Energy Market	Grid Monitoring and Control with PMU
Providing communications links to new endpoints in the energy system	✓	✓	✓	✓	✓
Use of public 5G and LTE networks without network slicing	✓	N/A	✓	N/A	N/A
Mobile networks for massive IoT communications	✓	✓	✓	✓	✓
Use of non-public LTE or 5G campus networks	✓	N/A	✓	✓	✓
Mission Critical Network solutions	✓	✓	✓	✓	✓
Use of low end-to-end latency services	✓	✓	✓	✓	✓
Using Distributed Edge Cloud features to reduce the latency requirements and provide local hosting of algorithms	✓	✓	✓	✓	✓
Network Slicing for energy provider control of QoS and security features	✓	✓	✓	✓	✓
Use of communications friendly protocols to maximise the reliability of the communications	✓	✓	✓	N/A	✓

Table 4-1: Relationship between 5G ICT solutions and Energy Use Cases

In further text, 5G ICT solutions listed in Table 4-1 are described in detail.

4.6.1 LTE and 5G Network solutions offering support for N5GEH use cases

Providing communications links to new endpoints in the energy system

Wireless communications systems, such as 5G, will offer cost-effective and easy to deploy solutions to supply communications over shorter distances to connect individual new assets which are part of the frequency management scenario to fixed networks. In a mobile wireless network, it is normal to have a fibre optic cable connecting each base station and antenna to the backbone of the 5G and general communications transmission system. This means that only the distance between the sending device (communications module or gateway) at the new asset (e.g., a wind turbine) and the nearest 5G base station antenna is actually communications over the air. Once the signal reaches the base station, it is transmitted further within the 5G and other communications networks to the intended receiver over fixed communications links.

Use of public 5G and LTE networks without network slicing

National or regional wide area 5G and LTE networks, either publicly or privately owned, can support many of the use cases studied in N5GEH. Their use needs investigation on a case by case basis on the individual use cases.

Mobile networks for massive IoT communications

If the use case does not pose critical communication requirements, other network technologies can be used in addition to 5G for comprehensive communication in the Internet of Things, for example: EC-GSM-IoT, LTE-M and NB-IoT. LTE and 3G cellular networks can also be considered if the use case requirements are met in these cases.

Use of non-public LTE or 5G campus networks

A non-public (sometimes also called private) geographically restricted campus network could be deployed by a DSO or Transmission System Operator (TSO) to provide part or all of the communications links required to use the scenarios defined above. Non-public networks offer the advantage that the owner has complete control of the priorities, security, configuration and access to the network. Public networks can be used to complement the use of non-public wireless networks, for example, enabling single remote locations to be reached by public networks.

Non-public 5G-based campus network solutions provide cost-effective indoor and limited outdoor communications for use in industrial environments and could contribute to communications solutions for this use case if the devices to be connected are located indoors. The solution acts as an indoor repeater enabling LTE and 5G communications to be used indoors in situations where the 4 or 5G signal is too weak to be used without a repeater. This enables a single type of communications network with a single definition of its security and other characteristics to be used for a complete solution giving economy of scale to the operation and maintenance of the communications.

Mission Critical Network solutions

Increasingly, LTE and 5G systems are provided in configurations described as Mission Critical Networks. These configurations are designed to support the requirements of mission critical networks, such an energy networks, with specific features such as enhanced network availability, extended network coverage and capacity, security hardening and multi-network operation options, and adaptations of the networks to conform to the regulatory requirements on infrastructure operators.

4.6.2 Network features particularly relevant to the N5GEH use cases

Use of low end-to-end latency services

5G and in particular stand-alone 5G using NR radio and the 5G core offers services with low latency in the single digit millisecond range.

Latencies of under 20 ms can be achieved by LTE advanced wireless networks. The configuration of the network in the exact locations would have to be investigated to check that the network in question could provide these latencies for each individual link.

The new 5G Ultra-Reliable Low Latency Communications service (URLLC) will be available in 5G products in coming years offering further reductions in latency and increased reliability in comparison to the 5G solutions available today.

Using Distributed Edge Cloud features to reduce the latency requirements and provide local hosting of algorithms

In order to reduce the requirements on latency over the wireless link, so that an LTE or slower wireless link could be used, and also potentially, to enable hosting of the frequency calculation algorithm close to the assets, 5G Distributed Edge Cloud could be included in the architecture of appropriate communications solutions.

Network Slicing for energy provider control of QoS and security features

Additionally, if the energy provider wants to ensure the quality of service of the communication and the security of the communications on an end to end basis, they could use Network Slicing features of 5G networks to set their own priorities for communications resources reserved for their slice and to use whatever communications security mechanisms they consider appropriate. The 5G networks used could be privately owned by energy providers or could be public 5G networks, or any combination of the two.

Use of communications friendly protocols to maximise the reliability of the communications

The packets to be transmitted are of small size, of the order of magnitude of several hundred kilobits of information. The protocols used by the energy systems should preferably be chosen so that they optimise the efficiency of the use of the wireless communications channel. Examples of commonly used energy protocols which make efficient use of wireless communications channels include Message Queuing Telemetry Transport (MQTT) and Advanced Message Queuing Protocol (AMQP) [25] and other Transport Control Protocol (TCP) based protocols. The use of the Sampled Value protocol is not appropriate as this protocol does not confirm the arrival of packets. Other energy protocols, such as 61850 Generic Object Oriented Substation Events (GOOSE) can generate communications problems as it produces bursts of traffic which can suddenly overload wireless channels and cause delays in transmission.

- **Use of the communications protocol MQTT to maximise the reliability, the availability and the security of the communications**

  Reliability and availability: When using MQTT between three stages of “quality of service” (QoS) can be chosen. If a sensor needs just to fire away its data and it’s not necessary that the message is received, QoS0 can be used. QoS1 makes sure the message is delivered and received at least once (could be more often). QoS2 makes sure the message is delivered and received exactly once. Latter could be important for control use cases. Of course, then the transmission is slower and the message (header) is bigger. Furthermore, the option “persistence” can be enabled. Then, in case of a temporary loss of connection, the client and broker store the data until the recipients are available again and sends them out.

- **Security**: MQTT sets up on TCP protocol. Hence, encrypted transmission via Transport Layer Security layer (usually TLS 1.2 or higher) can be used to prevent eavesdropping. Additionally, many MQTT broker technologies handle basic authentication and authorization via access-control lists. Authentication makes sure that only clients with correct credentials are able to connect to the broker. Authorization makes sure that only dedicated clients are allowed to access dedicated topics.

  Also, many add-ons are available to pass the authentication and authorization issues to an external instance. Of course, the connection needs to be encrypted since login data are passed with it. The use of external authentication servers enables easier identity and access management.

5. An analysis of the performance of 5G in relation to the ICT requirements of the N5GEH use case and IEC104 scenarios

Two types of investigations were undertaken to examine the 5G communication performance in terms of supporting the N5GEH use cases and the widely used IEC104 protocol. In the first part of the investigation, the performance of 5G communication connections in terms of latency was reviewed using synthetic data with characteristics typical for N5GEH use cases, based on the test results that were carried out as part of the SOGNO project [26]. The synthetic data that was created for use cases within the framework of the SOGNO project by the ACS Institute of RWTH Aachen University has the same characteristics as use cases in N5GEH. Parts of the results of the SOGNO test series were relevant for both projects and the results described here build on those of the SOGNO project.

In the second part of the investigation, a series of tests was carried out that examined the performance of the IEC104 protocol in terms of latency over the 5G communication link. The data streams of this test series were also generated synthetically, in this case using a method specially developed for N5GEH. The measurements in the test series were carried out in both the uplink and downlink directions. The 5G network was optimized by adding the radio parameters "Prescheduling Data Size", the maximum number of HARQ (Hybrid Automatic Repeat reQuest) transmissions, the choice of MCS (Modulation and Coding Scheme) and the number of available PRBs (Physical Resource Blocks) have been adjusted. The test series was carried out in a laboratory infrastructure in the Ericsson laboratory in Aachen using a non-public 5G network. The test series were carried out in the interior of the Ericsson laboratory with low transmission power using test frequencies instead of frequencies from public mobile network operators.

5.1 Laboratory test infrastructure

Ericsson provided a laboratory infrastructure for tests of the performance of a 5G network in transmitting synthetic data streams of messages in the MQTT and IEC104 protocol. The infrastructure included a non-public 5G network running with live over the air transmission in the laboratory.

This test infrastructure is typical of the type of mobile network equipment which would be used to provide 5G services for power network operators. Such network equipment could be owned and operated by public mobile network operators (E.g. Vodafone or T-Mobile). Increasingly, power network operators are purchasing and operating their own non-public mobile network infrastructure to support the operation of their power networks. In many cases, a hybrid mobile communications infrastructure consisting of a combination of public and non-public mobile networks is likely to be used to support power network operations.

5.1.1 5G network configuration implemented for the communications performance tests

A schematic diagram of the laboratory infrastructure is illustrated in Figure 5-1. On the left, the green box represents a PC, where the data streams for the laboratory tests of the N5GEH use cases were generated or received. Attached to the PC was a radio modem, the 5G phone or the industry WNC router. In the first set of the tests with N5GEH use cases, the OPPO phone was used. In the second set of the tests with IEC104 protocol, the industry WNC router was used. The modem transmitted the data streams over the air. The over the air communication between the antennas of the radio modem and the mobile network is illustrated as a blue dotted arrow.

When the data streams were generated by the PC and sent via the radio to the network, we speak of the **uplink (UL) direction**. When the PC received data streams generated by the 5G network, we speak of the **downlink (DL) direction**.

On the right, the green box symbolizes the mobile 5G network. In our tests, it was assumed that the N5GEH services are hosted in the non-public mobile network, in the edge cloud instead of in a power network operator’s central server or remote cloud. The network also included a Network Time Protocol (NTP [27]) server, which is used for time synchronization. The cable link using Ethernet, illustrated as a dotted line, from the NTP server to the PC was only needed for precise latency measurements in the laboratory infrastructure.

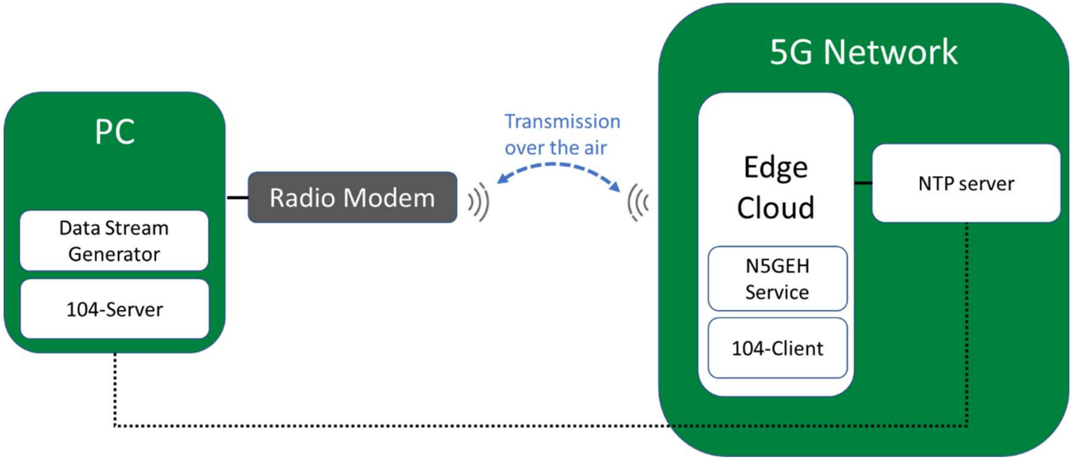


Figure 5-1 Schematic diagram of the laboratory infrastructure

5.1.2 Hardware components of the laboratory test infrastructure

The laboratory test infrastructure comprised of single hardware components (see Figure 5-2), which were linked together such that they form the system illustrated in Figure 5-1.

In the following sections, each of these components will be described in detail.

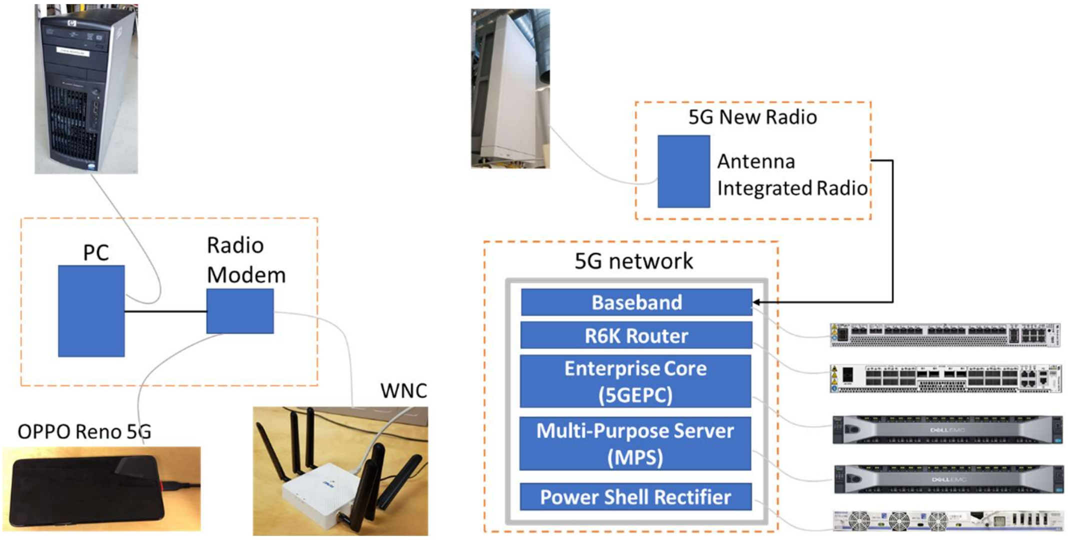


Figure 5-2 Overview of the hardware components of the laboratory test infrastructure

PC

A Linux PC, running on Ubuntu 18.04, was used in the laboratory test infrastructure. It was placed close to the radio network, so that the attached radio device was able to establish a connection to the network. In the tests of unidirectional services, the data streams were generated here. In the tests of downlink for bidirectional services, the data streams were received here.

Non-public 5G network

The non-public 5G network consisted of an antenna and Remote Radio Unit (RRU), Baseband Unit (BBU), R6K router and two Dell servers. The network was located at Ericsson in Herzogenrath. At the time of the tests, the 5G-URLLC (Ultra Reliable and Low Latency Communications) features were not released yet. The latency values using that profile are expected to be lower than the latency results obtained in the set of tests described in this document.

Edge Cloud

The core network was virtualized and running on the Edge Cloud. The user applications of energy services would be also deployed on the Edge Cloud.

5G phone

For the connection to the 5G network, a mobile phone by OPPO, model Reno 5G, was used. It run on an Android-based operating system, ColorOS V6.0. The OPPO phone was connected to the PC via USB.

Industry WNC router

The industrial router by Wistron NeWeb Corporation (WNC) operated with a Linux-based OS and had the model SKM-5x. The WNC router was connected to the PC via Ethernet.

5.1.3 Radio parameters optimized in our 5G test series

In order to get better performance in 5G networks, the radio parameters were adjusted to achieve the optimal radio network performance. The most important radio parameters related to latency, which could be adjusted in the systems available for this set of tests, were:

- The Prescheduling Data Size,
- The maximum number of Hybrid automatic repeat request (HARQ) transmissions,
- The choice of Modulation and Coding Scheme (MCS) used, and
- The number of Physical Resource Blocks (PRB) available.

5.1.4 Measuring latency in the test infrastructure radio networks

In order to measure the latency of the transmitted messages, the network traffic was traced with the Linux tool ‘tcpdump’. The measuring point at the PC was the interface to the radio modem. On the network side, the traffic was traced in the Edge Cloud. The resulting timestamps of the sent and received message were then extracted. In order to compute the latency, the times of the received and the sent message were subtracted.

In each test series, the latencies of 10000 messages were measured. The latency results of the tests described in this report are presented as an arithmetic mean of the results.

5.1.5 Limitations of the radio network test infrastructure

Many issues affecting the performance of large scale commercial 5G-based ICT infrastructure in the field could not be reproduced in the laboratory test environment available for the N5GEH tests.

The 5G-based ICT test infrastructure used for the N5GEH tests reported in this document differs from a commercial 5G-based ICT infrastructure in the field with respect to the following issues:

- **No handover** between base stations was possible in the laboratory and the devices used were stationary. The devices had a fixed distance relationship to the base station in the laboratory. In a full-scale 5G deployment solution scenario, devices would have a range of distances to the nearest base station which will affect the signal strength and performance characteristics of the individual radio links to these devices.
- The **hardware and software performance characteristics** of the equipment and deployed software used in the laboratory can differ from the hardware and software used in a full-scale live infrastructure. E.g., processor, memory and discs performance, software versions, etc of systems used in the field will often be optimised compared to the performance of laboratory prototype equipment, such as that used for these tests.
- There was **less interference** on the radio interface in the test lab and the devices had optical visibility to the antenna. In a real deployment, there will be obstacles in the environment causing many reflected signals, each with a different time delay and phase when they arrive at the receiver.
- In a test environment, a **limited number of traffic types** can be utilised compared to the full range of traffic types in a real-world application.

- **Packet loss** in a real environment is higher than that in a test lab.

Despite these limitations and differences, the results obtained in our laboratory tests are representative of the results which can be achieved in large scale commercial infrastructure using the optimizations tested and reported in this document.

5.1.6 Limitations of devices and systems used in the laboratory tests

In the laboratory test infrastructure, the latest available equipment available was used. During the tests, the following limitations regarding the infrastructure and its components were still encountered.

One limiting factor was the **5G OPPO phone**. It could not handle a burst of messages from multiple data streams or high message frequencies. Minimal message sampling rate was 10 messages/s in the tests of N5GEH use cases where 5G OPPO phone was used. The N5GEH services MV/LV-Grids Monitoring and Control with PMU, District Monitoring and Control in Energy Market and Building Monitoring can generate messages with a sampling rate of 50, 60 and 100 messages per second respectively to be transmitted in the field. However, the 5G OPPO phone device could not support such a high frequency of message transmission. The maximum sampling rate of the generated traffic stream by the OPPO phone in uplink direction was 10 messages per second whereas in downlink direction the maximum sampling rate was 5 messages per second. Hence, these services could therefore not be evaluated to the most detailed level using this equipment. Tests with other services could be run as in a field trial in a live power network.

Another limitation of the phone was **the need to use a VPN tunnel**. Since the OPPO phone is a commercial product, it could not be configured in a way that it forwarded the incoming messages to the PC. Therefore, a VPN tunnel was built between the PC and the 5G network, so that the edge cloud could reach the PC via the phone. Using a VPN tunnel in the 5G setup caused additional traffic to the actual data of the service. That lowered the performance of the radio link and latency was slightly increased.

The transmitted and measured **data stream** traffic was not associated with real data. Instead, synthetic data generators were used to generate data streams with data patterns typical of those which would be produced if live data was being transmitted for the use cases considered in the project. The results of the tests can be treated as if the data stream was measured in a real power grid scenario, even because the same data structure and format as in the field-deployed services have been used.

The last but not least, it has to be mentioned that results of the tests varied slightly because of interferences of radio signals when tests on several 5G laboratory networks were conducted in parallel. E.g. it was not unusual that the latency performance results of a repeated test varied up to 1-2 ms.

5.2 Evaluation of the ability of 5G networks to support the requirements of the N5GEH use cases

In order to evaluate the ability of 5G to support the requirements of the N5GEH use cases in laboratory tests, the N5GEH use cases were not deployed in the laboratory infrastructure. Instead, a stream of synthetic data was defined, which simulated the messages of the N5GEH use cases. The definition of the synthetic data yielded that the N5GEH use cases have the same characteristics as the use cases of the SOGNO project. Therefore, we could build on the results of the test series of the SOGNO project [26] exploiting the synergies between the projects. The data streams were transmitted over a 5G mobile network, and the latencies of each single message of the data stream was measured. The results of the tests can be treated as if the data stream was measured in a real power grid scenario, even because the same data structure and format as in the field-deployed services have been used.

5.2.1 Test methodology

5.2.1.1 Generating data streams typical for energy use cases with synthetic data generator

The simulated traffic of the services was generated by a synthetic data generator.

In order to be more flexible in terms of modifying the traffic patterns of a data stream, a synthetic data generator was created using the Paho Python library [28]. This generator took a single recorded message as input. A data stream of MQTT messages according to the requested traffic pattern was generated sending the same recorded message serially with a specific MQTT topic. With the synthetic data generator, the MQTT broker was installed on the network side. Depending on the communication direction (uplink or downlink), the MQTT publisher and subscriber clients were deployed on opposite sides. The receiver side subscribed to a specific MQTT topic by connecting to the MQTT broker. The sender side published messages to the MQTT broker.

5.2.1.2 Traffic patterns of the data streams

The traffic patterns of the energy use cases were specified in terms of **message size** and **message sampling rate**. The messages were generated and sent in equal intervals.

In some test cases, a higher message sampling rate than the specified in the requirement was used, in order to investigate the possibilities of the radio link to handle higher message frequency. That might become relevant for future power scenarios. With the 5G end-user device available at present for testing, the maximum message sampling rate which could be usefully used in tests was 5 messages per second in the downlink and 10 messages per second in the uplink.

5.2.1.3 Categorizing N5GEH use cases and their communication requirements

The following Table 5-1 categorizes the five N5GEH use cases in terms of their communication direction. Additionally, their latency requirements, as defined in N5GEH project, are stated. For the complete list of the communications requirements per N5GEH use cases, see Chapter 2.7.

Table 5-1: Overview of the N5GEH use cases and their characteristics

N5GEH use case	Communication direction	Message sampling rate [messages per second] 1)	Latency requirement 2)
Regional VPP	Uplink and downlink	0.1	350 ms
Grid Protection	Uplink and downlink	1000	<10 ms
Building Monitoring	Uplink	100	100 ms 3)
Closed Loop Control within Buildings	Uplink and downlink	1	200 ms
District Monitoring and Control in Energy Market	Uplink and downlink	1/60	6,000 ms
MV/LV-Grids Monitoring and Control with PMU	Uplink and downlink	50	<10 ms
Note 1: The highest required message sampling rate per device is indicated. *Note 2: The lowest required round-trip latency is indicated.* *Note 3: Uplink latency is indicated.*			

5.2.2 Evaluation of latencies which 5G networks can achieve supporting N5GEH use cases

Two types of tests were conducted in SOGNO project [26] depending on the communication directions: uplink and downlink. The message size was the same for all test cases, i.e., it was less than 1 KB. MQTT protocol was utilised in the tests. In several test cases required sampling rate was not simulated in the tests because of the limitations of the OPPO device. Because of the device limitation, the maximum sampling rate used in the test in uplink direction was 10 messages per second whereas in downlink was 5 messages per second. For the use cases Regional VPP and Grid Protection, we measured with higher sampling rate than required but we can expect the same results. The average latencies of the tests are shown in Table 5-2.

Because of the limitations of the OPPO phone mentioned before, the use cases Building Monitoring and MV/LV-Grids Monitoring and Control with PMU could not be tested to the most detailed level.

Table 5-2: Evaluation of 5G communications links latencies per N5GEH use cases

N5GEH use case	Communication direction	Message sampling rate [messages per second]	Uplink average latency [ms] [1)]	Downlink average latency [ms] [1)]
Regional VPP	Uplink and downlink	1	5.56	4.01
Grid Protection	Uplink and downlink	10 (UL), 5 (DL)	3.87	3.83
Building Monitoring	Uplink	10	3.87	N/A
Closed Loop Control within Buildings	Uplink and downlink	1	4.75	3.65
District Monitoring and Control in Energy Market	Uplink and downlink	10 (UL), 5 (DL)	3.87	3.83
MV/LV-Grids Monitoring and Control with PMU	Uplink and downlink	10 (UL), 5 (DL)	3.87	3.83
Note 1: Evaluation based on the latency results of the SOGNO test series				

5.2.3 Conclusions

The analysis of relevant test results in the context of the N5GEH use cases shows that 5G can support the latency requirements of N5GEH use cases. In particular, average uplink latencies of 3.87 – 5.56 ms and average downlink latencies of 3.65 – 4.01 ms are observed. The average round-trip latency can be derived when uplink and downlink latencies are added together, resulting in latency values from 7.7 to 9.57 ms. Therefore, it was concluded that even the most challenging requirements, for round-trip latencies of below 10 ms, can be supported by the 5G technology. Furthermore, it is shown that 5G technology is capable of fulfilling even more stringent requirements on latency which may arise in the use cases in future years if they evolve towards near real-time operation. Current trends suggest that the services will evolve towards increasingly frequent analysis of measurements, eventually achieving real-time operation.

5.3 Communications performance tests to support scenarios in which the IEC104 protocol is utilised

This chapter reports on the tests conducted in a laboratory infrastructure to investigate the performance of the wireless 5G technology transmitting messages using the IEC104 protocol. The test cases specified for the experiments represent a range of existing and future energy scenarios in which IEC protocol is utilised.

An implementation of the IEC104 protocol was tested in a live power network in the scope of the SOGNO project [29]. The RTU measurement device was sending messages in the IEC104 protocol via Telekom Romania LTE mobile network to a server, where the FLISR service received and processed the data.

5.3.1 IEC104 protocol scenarios selected for the performance tests

The IEC 60870-5-104 (IEC104) protocol [30] is widely used in the communication systems of power grids. The protocol is based on the Transmission Control Protocol (TCP) and operates on a server/client principle. A measurement device in the grid is usually configured as the 104-server and it needs to be connected to a 104-client, which can be hosted in the network of the DSO. The 104-server and -client can communicate over a fixed or mobile connection.

The most common scenarios where IEC104 protocol is utilised in live power networks as well as future use cases where IEC104 protocol is foreseen to be used are selected in N5GEH project in order to evaluate the IEC104 protocol performance over 5G network communication links.

The following scenarios were identified:

- Standard access to feed-in stations (distributed energy resources)
- Power quality (PQ) monitoring
- Substation monitoring
- Grid protection (the use case studied in N5GEH project)
- Regional VPP
- State estimation

5.3.1.1 IEC104 communications requirements per scenario

N5GEH project specified the communications requirements for each IEC104 scenario. The latency requirements listed in this chapter were evaluated in the 5G network in laboratory tests.

Standard access to feed-in stations scenario

In this scenario, two sub-scenarios were identified:

- (1) 10 measured values are sent as periodic updates in the uplink direction from a measurement device to a substation or from a substation to the next fibre endpoint of the DSO every minute. Required uplink latency is 1 s.
- (3) The control centre or substation sends a command (one data value) to the device of the feed-in station, followed by a confirmation of the device. Required round-trip latency is 1 s.

Power quality monitoring scenario

20 measured values are sent as periodic updates in the uplink direction from a measurement device to a substation or from a substation to the next fibre endpoint of the DSO every second. Required uplink latency is 100 ms. As a difference to the substation monitoring scenario, the number of sending devices (number of uplinks) is much higher.

Substation monitoring (“Umspannwerke”) scenario

In this use case, two sub-scenarios were identified:

- 500 measured values are sent as periodic updates in the uplink direction from a measurement device to a substation or from a substation to the next fibre endpoint of the DSO every second. Required uplink latency is 100 ms.
- The future scenario requires 500 measured values as periodic updates in the uplink direction from a measurement device to a substation or from a substation to the next fibre endpoint of the DSO every 20 ms. Since, one measured value per period in a power network operating with 50 Hz would be sent, the monitoring of the substation could be performed in real-time. Required uplink latency is 100 ms.

Regional VPP scenario

The control centre sends a command (one data value) to the regional VPP backend, followed by a confirmation of the regional VPP backend. Required round-trip latency is 100 ms.

Grid protection scenario

In this use case, three sub-scenarios were identified:

- The control centre sends a command (one data value) to the grid protection backend (may be a cloud service or running on a local machine placed at the substation level), followed by a confirmation of the regional VPP backend. Required round-trip latency is 100 ms.

- A data base update, with 300 data values, is transmitted from the control centre to the substation, followed by a confirmation message. Required round-trip latency is 1 s.
- The future scenario as defined in N5GEH requires 500 measured values are sent with a high message frequency of 20 ms. That enables a better grid protection and a wireless solution is particularly interesting to the grid operator, because the number of connected devices will increase, and it is more cost efficient to connect them wirelessly to the control centre. Required round-trip latency is 20 ms.

State estimation scenario

15 measured values are sent as periodic updates in the uplink direction from a measurement device to the DSO every second. Required uplink latency is 1 s. Number of measurement devices within an observed grid area is 30-50% of the grid nodes.

Summary of communications requirements for IEC104 scenarios

Table 5-3 specifies communications requirements defined in N5GEH project per each IEC104 scenarios evaluated in our laboratory tests.

Table 5-3 Communications requirements for IEC104 scenarios

Scenario	Sub-scenario	Communications flow	Sampling rate [messages/s]	Number of data values per message	Latency [ms] (UL or RT) [1)
Standard access to feed-in stations	Periodic updates	Periodical updates from measurement-device to substation (for fibre access)	1/60	10	1,000 UL
	Interrogations	1. Command from substation/control centre to device 2. Confirmation from device	Event	1	1,000 RT
PQ monitoring	Periodic updates	Periodical updates from measurement-device to substation (for fibre access)	1	20	100 UL
Substations monitoring	Maximum measured values	Periodical updates from MV/LV substation to the next DSO fibre endpoint	1	500	100 UL
	High sampling rate (future scenario)	Periodical updates from MV/LV substation to the next DSO fibre endpoint	50	500	100 UL
Regional VPP	On/off command	1. Command from control centre to regional VPP backend 2. Confirmation from device	Event	1	100 RT
Grid protection	On/off command	1. Update from control centre to substation	Event	1	1,000 RT

		2. Confirmation from substation			
	Topology update	1. Update from control centre to substation 2. Confirmation from substation	Event	300	1,000 RT
	High number connected devices (future scenario)	1. Request from substation or control centre 2. Data message to the control centre	50	500	20 RT
State estimation	Periodic updates	Periodical updates from MV/LV substation to the next DSO fibre endpoint	1/60	15	1,000 UL
Note 1: Either one-way (UL) or round-trip latency (RT)					

5.3.2 Test methodology

5.3.3 Types of communication between 104-server and 104-client

For the tests, two types of communications between the 104-server and 104-client were used: periodic updates and interrogations.

Periodic updates: The 104-server deployed at the PC transmitted the data in equal intervals to the 104-client deployed at the 5G network edge cloud.

Interrogations: The 104-client deployed at the PC sent interrogations to the 104-server deployed at the PC. The message flow of these test cases is illustrated in Figure 5-3: Message flow of the 104-interrogation. The 104-client first sent an interrogation command (Act) to the 104-server. The server confirmed the command with an acknowledgement (ActCon) and consequently sent the requested data (Inrogen) to the server. Three types of latencies were measured here:

- Downlink latency of the Act message
- Uplink latency of the Inrogen message
- Round-trip latency in the 104-client of the time between sending the Act and receiving the ActCon messages

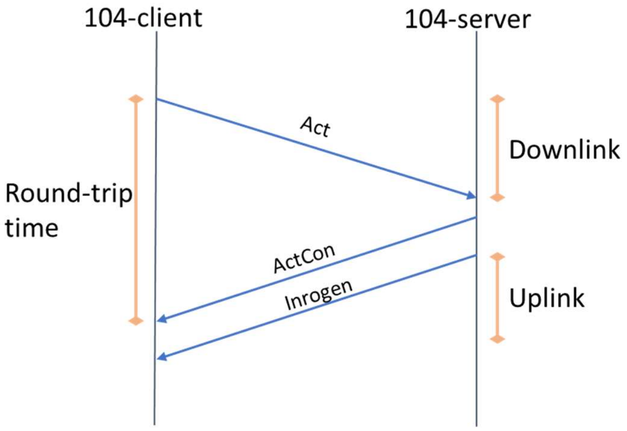


Figure 5-3: Message flow of the 104-interrogation

5.3.3.1 Generating data streams typical for IEC104 scenarios with synthetic data generator for use in laboratory tests

In the tests, the simulated traffic of the services was generated by a synthetic data generator.

In the tests, the data traffic did not originate from a live power network. Instead, the messages were synthetically generated by lib60870-C [31], an open-source implementation of the IEC104 protocol. The data traffic typical of each test case was reproduced using lib60870-C according to the message sampling rate and the number of data values per message.

5.3.3.2 Traffic patterns of the data streams

In cases of event-related communication, we chose to send messages in random periods between 1 and 5 s to simulate infrequent transmissions while ensuring to collect enough samples for evaluation.

The number of data values per message specifies how many measurement points are covered by the 104-server. In the tests, the number of data values were represented by information objects of the IEC104 protocol. A higher number than 60 objects per message of type periodic updates and 127 objects per message of type interrogation is not supported by the protocol, so that the targeted number of data points could not be investigated in some test cases which exceed these numbers (Substation Monitoring and Grid Protection).

5.3.4 Test results

The laboratory tests measured average uplink, downlink and round-trip latencies for each IEC104 scenario. The endpoints of the communications were end-user device and 5G edge cloud. Round-trip latency was always measured from the 5G edge cloud. For some scenarios, it was applicable to measure only uplink average latency. The latency results are specified in Table 5-4.

The following scenarios were not tested in the lab because they have milder communications requirements: Power Quality Monitoring, Regional VPP, Grid Protection On/Off Command and State Estimation. The scenarios that had more stringent requirements were tested, and it can be expected that they fulfil the milder requirements as well.

Table 5-4 5G communications links latencies per IEC scenarios measured in the laboratory

Scenario	Sub-scenario	Communications flow	Uplink average latency [ms]	Downlink average latency [ms]	Round-trip average latency [ms]
Standard access to feed-in stations	Periodic updates	Periodical updates from measurement-device to substation (for fibre access)	6.54	N/A	N/A
	Interrogations	1. Command from substation/control centre to device 2. Confirmation from device	5.61	4.58	10.58
Substations monitoring	Maximum measured values	Periodical updates from MV/LV substation to the next DSO fibre endpoint	6.94	N/A	N/A
	High sampling rate (future scenario)	Periodical updates from MV/LV substation to the next DSO fibre endpoint	7.04	N/A	N/A

Grid protection	Topology update	1. Update from control centre to substation 2. Confirmation from substation	6.10	6.44	12.96
	High number connected devices (future scenario)	1. Request from substation or control centre 2. Data message to the control centre	6.15	7.11	13.64

5.3.5 Conclusions

The average latency in the uplink direction ranged from 6.54 to 7.04 ms and in downlink from 4.58 to 7.11 ms. An average round-trip latency of 10.58 – 13.64 ms was obtained. The latency test results showed that 5G has the basic capability to support the latency requirements for all IEC104 scenarios.

In addition to the existing scenarios, the 5G technology can also cope with the increasingly challenging requirements for future scenarios of the Substations Monitoring and the Grid Protection. Increasing the sampling rate in the tests to 50 messages per second, that is required in all future scenarios, led to only slightly increased average latency compared to the message sampling rate of 1 message per second or lower. It can be highlighted, that 5G has the basic capability to support the most stringent requirement on round-trip latency of 20 ms in the future Grid Protection scenario, as the test measured a latency of 13.64 ms. The trends in grid management suggest that as with other services, Grid Protection will evolve to use lower and lower latencies eventually operating in real-time as part of the general evolution of power grids towards becoming data-driven infrastructures.

5.4 Potential future work

Further improvements in the 5G latency performance supporting the use cases studied in N5GEH and the IEC104 protocol scenarios, could be expected to be measurable in tests which could be undertaken in future projects, to evaluate the impact of the forthcoming 5G Ultra Reliable Low Latency Communication (URLLC) service. Also, the performance of 5G measured with live power network services data could be tested. To investigate a shorter message sending period relevant for the building Monitoring use case, the test equipment could be replaced with newer 5G end user devices and modems, which do not have limitations on message sending frequency.

Besides the latency performance, the communication reliability could be tested in the laboratory using available attenuation tools that could simulate a range of conditions on the radio link. The new feature of the 5G will expose the capabilities of the 5G private networks, like device and network management, to energy applications and services. N5GEH and other energy use cases could be studied in laboratory tests to identify the new benefits that they could have from using of the 5G network capabilities.

Many of the results considering the improvements mentioned above will be further developed in newly started H2020 projects, such as edgeFLEX [32], , which focusses on expanding the role of the Virtual Power Plants (VPP) with new power services supported by 5G and the IoT NGIN project (due to start in October, 2020) which focusses on the use of 5G to support advanced IoT use cases for energy, smart manufacturing and smart agriculture.

The results and experiences gathered in the N5GEH project will be used by Ericsson to address the potential requirements raised by utility customer companies of Ericsson. Where relevant, Ericsson will collaborate with the N5GEH project partners to provide appropriate solutions to customers.

6. Conclusions

This report describes the definition and analysis of the ICT requirements of the energy use cases elaborated in the N5GEH project. Requirements were defined in relation to the configuration of the network and devices, the communications transmission characteristics, the timescales for the full-scale commercial deployment of the use cases and obstacles which need to be overcome to enable their deployment. The analysis of the requirements showed that the use cases place demanding requirements on the performance, reliability, security and latency of the communication networks used to support them.

Evaluation of 5G communications connection performance measured in relevant tests using synthetic data streams typical for the energy use cases in the N5GEH project, shows that a 5G network can support the latency requirements of the N5GEH use cases. It also demonstrates that a 5G network can support the expected evolution of these use cases as they evolve in coming years and place more challenging requirements on the latency of the communication networks. In particular, average latencies of 3.87-5.56 ms in the uplink and 3.65-4.01 ms in the downlink are obtained. Adding together these values of uplink and downlink latency results in average round-trip latencies of 7.52-9.57 ms. For the Grid Protection use case, which is the most time critical use case among the use cases studied in N5GEH with the most challenging requirements, N5GEH specified an expected round-trip latency of less than 10 ms. Note that these average latency values were obtained when optimisations of 5G radio parameters were implemented.

Set of tests was undertaken in the N5GEH project evaluating the 5G communications connection performance using the IEC 60870-5-104 transmission protocol for communication. The most critical existing and future scenarios where IEC104 is used, were selected and tested in the laboratory. The test results showed that 5G does not only meet the requirements of today’s scenarios but also of future more demanding scenarios. In the tests, 5G provided average round-trip latency of 10.58-13.64 ms.

The analysis of the 5G tests results demonstrate that 5G networks offer a range of effective and cost-efficient solutions to the challenging requirements discussed in this report. Specific features of 5G networks, such as its low latency, high availability and reliability, high bandwidth, support of distributed edge infrastructure and of long device battery life all offer relevant support to the use cases of the N5GEH project. Advanced features of 5G increasingly available as products and services, such as the Ultra Reliable Low Latency service (URLLC) and network slicing offer even more possibilities to extend the ICT support 5G can provide. 5G solutions are increasingly offered in the energy sector as so-called Mission Critical Networks. Mission Critical Networks are LTE and 5G networks configured to support the stringent requirements which Critical Infrastructure owners place on the ICT networks they use to support their services.

Further development of the results produced in the 5G studies in the N5GEH project is planned to take place in recently started Horizon 2020 projects in which both RWTH and Ericsson participate.

7. List of Tables

8. List of Figures

9. Bibliography

[1] J. Seifert, P. Schegner, A. Meinzenbach, P. Seidel, J. Haupt, L. Schinke, J. Werner and T. Hess, Regionales Virtuelles Kraftwerk auf Basis der Mini- und Mikro-KWK-Technologie, Berlin: VDE Verlag, ISBN 978–3–8007–3654–6, 2015.

[2] J. Seifert, J. Werner, P. Seidel and E. al, RVK II - Praxiserprobung des Regionales Virtuelles Kraftwerk auf Basis der Mikro-KWK-Technologie, Berlin: VDE Verlag, ISBN 978–3–8007–4630–9, 2018.

[3] ISO/IEC, “PRF 20922, Information technology -- Message Queuing Telemetry Transport (MQTT) v3.1.1”.

[4] “Mindestanforderungen an die Informationstechnik des Reservenanbieters zur Erbringung von Regelreserve, Version 2.1,” December 2019.

[5] S. Feuerhahn, M. Zillgith, C. Wittwer and C. Wietfeld, “Comparison of the Communication Protocols DLMS/COSEM, SML and IEC 61850 for Smart Metering Applications,” 2011.

[6] Ericsson white paper, “5G wireless access: an overview,” 2020. [Online]. Available: https://www.ericsson.com/498a10/assets/local/reports-papers/white-papers/whitepaper-5g-wireless-access.pdf.

[7] Ericsson white paper, “Cellular IoT in the 5G era,” February 2020. [Online]. Available: https://www.ericsson.com/en/reports-and-papers/white-papers/cellular-iot-in-the-5g-era.

[8] Ericsson, “5G deployment considerations,” 2018. [Online]. Available: https://www.ericsson.com/en/reports-and-papers/5g-deployment-considerations.

[9] Ericsson white paper, “5G spectrum for local industrial networks,” 2020. [Online]. Available: https://www.ericsson.com/en/reports-and-papers/white-papers/5g-spectrum-for-local-industrial-networks.

[10] Ericsson Technology Review, “Distributed cloud – a key enabler of automotive and industry 4.0 use cases,” November 2018. [Online]. Available: https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/distributed-cloud.

[11] J. Davis, P. Shih and A. Marcham, “State of the Edge 2018: A Market and Ecosystem Report for Edge Computing,” 2018. [Online]. Available: https://stateoftheedge.com/reports/state-of-the-edge-report-2018/.

[12] A. Checko, “Cloud Radio Access Network architecture. Towards 5G mobile networks,” 2016. [Online]. Available: https://orbit.dtu.dk/en/publications/cloud-radio-access-network-architecture-towards-5g-mobile-network.

[13] Ericsson white paper, “5G security – enabling a trustworthy 5G system,” March 2018. [Online]. Available: https://www.ericsson.com/4965aa/assets/local/reports-papers/white-papers/25032021-5g-security-enabling-a-trustworthy-5g-system.pdf.

[14] ETSI/SAGE, “Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2. Document 1: UEA2 and UIA2 Specification, Version: 2.1,” available at https://www.gsma.com/aboutus/wp-content/uploads/2014/12/uea2uia2d1v21.pdf, March 2009.

[15] IETF RFC5930, “Using Advanced Encryption Standard Counter Mode (AES-CTR) with the Internet Key Exchange version 02 (IKEv2) Protocol,” Hangzhou H3C Tech. Co., Ltd., NSS. Murthy, available at https://tools.ietf.org/html/rfc5930, July 2010.

[16] ETSI/SAGE, “Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3. Document 2: ZUC Specification, Version: 1.6,” available at https://www.gsma.com/security/wp-content/uploads/2019/05/eea3eia3zucv16.pdf, June 2011.

[17] IETF RFC4493, “The AES-CMAC Algorithm,” University of Washington, Samsung Electronics, Nagoya University, available at https://tools.ietf.org/html/rfc4493, June 2006.

[18] IETF RFC2104, “HMAC: Keyed-Hashing for Message Authentication,” IBM, UCSD, available at https://www.rfc-editor.org/rfc/rfc2104.txt, February 1997.

[19] “Elliptic Curve Cryptography Version 2.0 (2009), SECG SEC 1 specification,” available at: http://www.secg.org/sec1-v2.pdf, 2009.

[20] GSMA, “NESAS – Network Equipment Security Assurance Scheme (2018),” [Online]. Available: https://www.gsma.com/aboutus/leadership/committees-and-groups/workinggroups/fraud-security-group/network-equipment-security-assurance-scheme.

[21] 5G-ACIA, “5G Non-Public Networks for Industrial Scenarios,” July 2019. [Online]. Available: https://www.5g-acia.org/fileadmin/5G-ACIA/Publikationen/5G-ACIA_White_Paper_5G_for_Non-Public_Networks_for_Industrial_Scenarios/WP_5G_NPN_2019_01.pdf.

[22] 3GPP, “TS 23.251 v15.1.0 Network sharing, Architecture and functional description,” 2018.

[23] Ericsson broschure, “Enabling intelligent operations with Mission Critical Networks,” 2021. [Online]. Available: https://www.ericsson.com/494930/assets/local/networks/offerings/mission-critical/ericsson-mission-critical-networks.pdf.

[24] C. Wallace, “Bringing 5G networks indoor,” 2019.

[25] ISO/IEC, “ISO/IEC 19464:2014, Information technology -- Advanced Message Queuing Protocol (AMQP) v1.0 specification,” 2014.

[26] “SOGNO D4.6: Description of the integration and testing of the solution including the 5G based advanced communication,” 2020. [Online]. Available: https://www.sogno-energy.eu/global/images/cms/Deliverables/774613_deliverable_D4.6.pdf.

[27] “Network Time Protocol,” [Online]. Available: http://www.ntp.org/.

[28] “Paho Python Client,” [Online]. Available: https://www.hivemq.com/blog/mqtt-client-library-paho-python/.

[29] “D5.2, Report on the outcome of the SOGNO field trials and laboratory tests,” EU Project SOGNO, 2020.

[30] IEC, “IEC/TR 61850-90-5; Communication networks and systems for power utility automation – Part 90-5: Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118,” 2012.

[31] “Official repository of lib60870-C,” [Online]. Available: https://github.com/mz-automation/lib60870.

[32] “edgeFLEX Project,” [Online]. Available: https://www.edgeflex-h2020.eu/.

10. List of Abbreviations

3GPP	3rd Generation Partnership Project
5G	Fifth generation cellular network technology
AMQP	Advanced Message Queuing Protocol
API	Application Programming Interface
BBU	BaseBand Unit
C-RAN	Cloud Radio Access Network
DLMS/COSEM	Device Language Message Specification and COmpanion Specification for Energy Metering
DSO	Distribution System Operator
FLISR	Fault Location, Isolation and Service Restoration
GSMA	Global System for Mobile communications Association
GP	Grid Protection
ICT	Information and Communication Technology
IEC	International Electro-technical Commission
IoT	Internet of Things
JSON	JavaScript Object Notation
KPI	Key Performance Indicator
LTE	Long Term Evolution
LTE-M	Long Term Evolution for Machines
LV	Low Voltage
MQTT	Message Queuing Telemetry Transport
MV	Medium Voltage
NB-IoT	NarrowBand Internet of Things
NSA	Non-Stand-Alone
NR	New Radio
PMU	Power Measurement Unit
PQ	Power Quality
RAN	Radio Access Network
RBS	Radio Base Station
SA	Stand-Alone
SCC	Short Circuit Current
SGAM	Smart Grid Architecture Model
TCP	Transport Control Protocol
TLS	Transport Layer Security
TSO	Transmission System Operator
VPN	Virtual Private Network
WTI	Wireless Transducer Interface