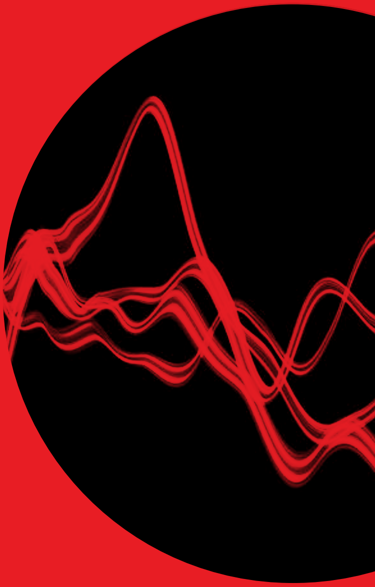
CHARTING THE FUTURE OF INNOVATION | #10·2022

Review

ERICSSON TECHNOLOGY



PROGRAMMABLE 5G FOR THE INDUSTRIAL IoT

ERICSSON

Creating programmable 5G systems for the Industrial IoT

In close collaboration with the operational technology company ABB, we have developed and tested a prototype of a programmable 5G system and successfully integrated it with an ABB automation system. Beyond demonstrating the advantages of using 5G to support industrial automation solutions, the ABB proof of concept highlights the importance of emerging 3GPP standards to address the expectations of industry verticals with regard to system integration.

GERGELY SERES, DIRK SCHULZ, OGNJEN DOBRIJEVIC, ABDULKADIR KARAAĞAÇ, HUBERT PRZYBYSZ, ALA NAZARI, PETER CHEN, MÁRK LÁSZLÓ MIKECZ, ÁRON DÉNES SZABÓ

A steadily growing number of factories, plants, mines and ports around the world are exploring the potential of 5G technology and considering how best to deploy it. This is to be expected, since 5G has been designed with vertical use cases in mind, and industrial automation systems are one of the most promising segments.

■ Private 5G networks [1] are becoming a critical and indispensable tool for enterprises in the operational technology (OT) vertical. The transformation of production environments such as process plants (chemical industry, mining, pharma, food and beverage, and so on) and factories (automotive or electronics manufacturing) driven by Industry 4.0 [2, 3] creates a dynamic environment that necessitates the reconfiguration of the automation system infrastructure and, by extension, the reconfiguration of the supporting 5G network and the continuous monitoring of the wireless connectivity service it provides.

Such flexibility enables the stepwise introduction of industrial applications over a common 5G infrastructure. In most cases today, the reconfiguration and monitoring of private 5G networks is done manually, often with the involvement of the communication service provider

(CSP) or other entity that operates the 5G network. In wired automation networks based on technologies such as Industrial Ethernet or fieldbuses, the automated configuration and monitoring from within the automation system is the state of the art, translating the needs of applications into network configuration without lag, effort and quality problems. To use 5G as a part of the automation infrastructure on scale, that same seamless integration is required.

Therefore, the next step is to establish a live connection between private 5G networks and existing OT/IT systems. A private 5G network is expected to act as an integral part of the OT/IT communication infrastructure, seamlessly integrated with existing wired networks and upcoming technologies such as Time-Sensitive Networking (TSN) from the Institute of Electrical and Electronics Engineers (IEEE). Industry verticals expect to perform this system integration relying on their existing OT/IT skills, without the need to acquire additional competence in cellular wireless communication systems.

While 5G technology is designed to be scalable, flexible and extremely versatile regarding performance, these advantages come with a complex approach to building and operating networks that requires expertise commonly not available in OT companies today. The need to understand cellular technology in detail is therefore a significant roadblock to the adoption of 5G in the industry sector.

To overcome this challenge, private networks need to include user-oriented 5G exposure interfaces that are much simpler to use than any of the current telco-oriented exposure interfaces that assume deep knowledge of the internal workings of cellular systems. Such interfaces must offer the adequate level of abstraction that allows factory or plant operators to execute their regular operational tasks without the need for dedicated support from the service (and network) provider. In short, the ability to execute network automation across the organizational boundaries of CSP and OT enterprises needs to be an integral part of an industrial private 5G network offering.

Identifying 5G exposure requirements for industry verticals

With broad participation from the OT/IT and telecommunication industries, including Ericsson and ABB, the 5G Alliance for Connected Industries and Automation (5G-ACIA) collected and documented the requirements on 5G exposure capabilities for the process automation, production IT, logistics and warehousing industry verticals and published them in a white paper [4].
Figure 1 visualizes the concept of 5G exposure interfaces of a 5G private network, as presented in 5G-ACIA's white paper [4]. These interfaces enable Industrial Internet of Things (IIoT) applications to program the 5G network in a variety of ways, such as establishing connections of device-to-device and device-to-enterprise-network types with customized quality of service (QoS).

The 5G-ACIA concept builds on nine key exposure requirements in the area of device management:

1. Device connectivity management
2. Device connectivity monitoring
3. Device group communication management
4. Device provisioning and onboarding
5. Device identity management
6. Device location information
7. Security
8. Time-sensitive networking (TSN) integration
9. Time-sensitive communications.

Private 5G networks and the Industrial Internet of Things

A private 5G network is a deployment of the 5G system for private use. A private 5G network can be either standalone or deployed with the support of a public 5G network. In either case, a standardized exposure service offering is necessary to allow enterprises to customize 5G connectivity to fit the specific communication needs of industrial applications.

The **Industrial Internet of Things** (IIoT) is a subset of IoT applications tailored for advanced industrial automation.

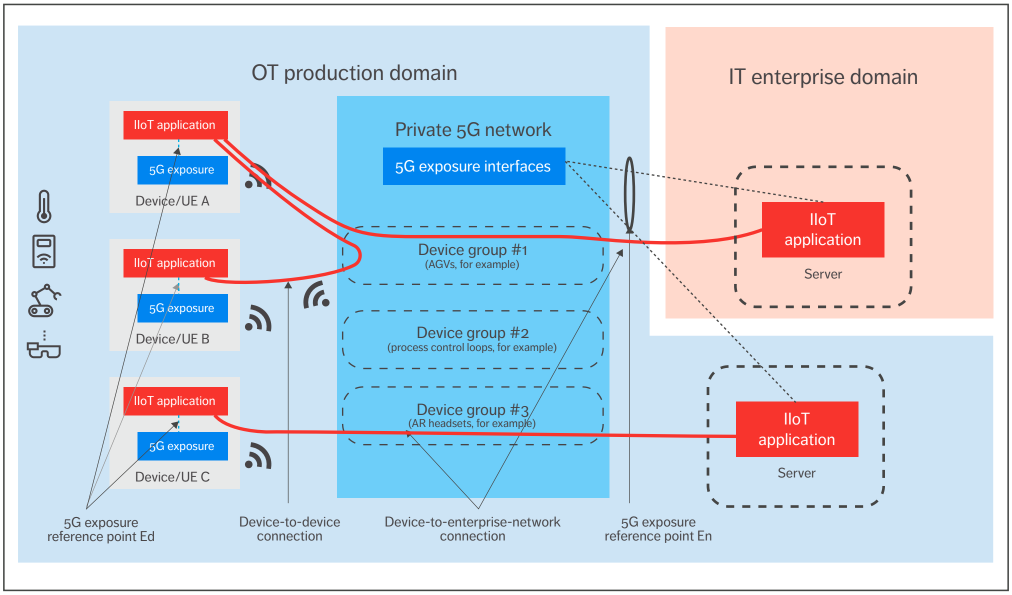


Figure 1 The 5G-ACIA concept of 5G exposure interfaces

To test the concept, we addressed the majority of these requirements in the joint ABB-Ericsson proof of concept.

Device connectivity management

IIoT applications are often time-critical, requiring low bounded latency and reliable communication. Through the 5G exposure interfaces, applications must be able to set up one or more connections per device with customized QoS, including guaranteed and minimum bitrate, latency and packet transmission reliability. These IP or Ethernet connections must support device-to-device or device-to-enterprise-network configurations. The exposure interfaces must hide the underlying realization aspects of the 5G network, such as QoS flows, resilient connections with low interruption time in case of node/link failure or disjoint user plane paths.

Device connectivity monitoring

For business continuity reasons, it is essential that a factory or plant operator can monitor the 5G connectivity service continuously through its OT/IT applications. The 5G exposure interfaces must enable the monitoring of connections of a device or a group of devices, allowing the retrieval of current and historical performance metrics either on demand, periodically, or on an event-triggered basis related to connection bitrate, latency and packet loss, for example.

Device group communication management

Industry verticals expect to be able to isolate the traffic of different use cases and traffic types for the purposes of performance and security management. Traffic segmentation is enabled by 5G group communication, where devices in the same group communicate privately with one another and can also access services in enterprise networks. 5G provides group communication with 5G local area network (5GLAN)-type services for both IP virtual network (VN) groups and 5GLAN virtual local area networks (VLANs). The 5G exposure application programming interface (API) must provide the means for applications to manage device groups, including creating groups and adding and removing group members, as well as creating dynamic VLAN assignment for devices when connecting to the network.

Device provisioning and onboarding

Industry verticals want to be able to add devices to the 5G network in a plug-and-play manner. The 5G exposure interfaces must enable the provisioning of device identifiers and credentials into the 5G network both for individual devices and groups of devices. In the onboarding step, the 5G network must provide the means for the device to establish a user plane connection to the IIoT application and have the ability to notify the application about the newly established connection.

Device identity management

IIoT applications use a wealth of identifiers both in the application layer and in the connectivity layer, depending on the applied technology. In 5G networks, the primary unique identifier of 5G user equipment (UE) is the Generic Public Subscription Identifier (GPSI), which means that this ID must be used by the 5G exposure interfaces. Translation between the IIoT device's application layer (OT/IT, for example) identifiers and the GPSI must be done in the application. The static IP address of the device or the device's media access control (MAC) address may also be used as the device identifier in the 5G exposure interfaces.

Device location information

Use cases such as mobile robots, automated guided vehicles, portable assembly tools, mobile control panels and plant asset management require the positioning of IIoT devices with different levels of accuracy. IIoT applications may request the location information of one or a group of devices over the 5G exposure interfaces. Device tracking is achieved by reporting device location triggered by events such as movements.

> “INDUSTRY VERTICALS WANT TO BE ABLE TO ADD DEVICES TO THE 5G NETWORK IN A PLUG-AND-PLAY MANNER”

Security

IEC 62443 standards [5] introduce the concepts of “zones” and “conduits” as a way to segment and isolate the various subsystems in a control system. A zone is defined as a grouping of logical or physical assets that share common security requirements based on factors such as criticality and consequence. A conduit consists of the grouping of cyber assets dedicated exclusively to communications within and also external to a zone and which share the same cybersecurity. Device groups (5GLAN VLANs or IP VN groups) combined with secured slicing and application-level security protect the factory zones achieving IEC 62443 Security Levels SL3 and SL4 [5].

Time-sensitive networking integration

OT verticals consider TSN to be the next-generation technology that will bring about convergence in OT networking. When combined with 5G networks, the fully centralized TSN configuration model of IEEE 802.1Qcc must be used. It postulates that a centralized network configuration (CNC) entity configures all the TSN streams in the 5G network, which acts as a TSN bridge. The 5G exposure interfaces must serve as the TSN application function (AF) and provide port and bridge management information. This enables the CNC to determine the allocation of network resources to the streams and configure them in the 5G network through the 5G exposure interfaces.

Time-sensitive communications

5G-native time-sensitive communications (TSC) refers to a time-sensitive communication service that the 5G network offers to 5G devices natively (that is, without integration into a TSN system). 5G exposure

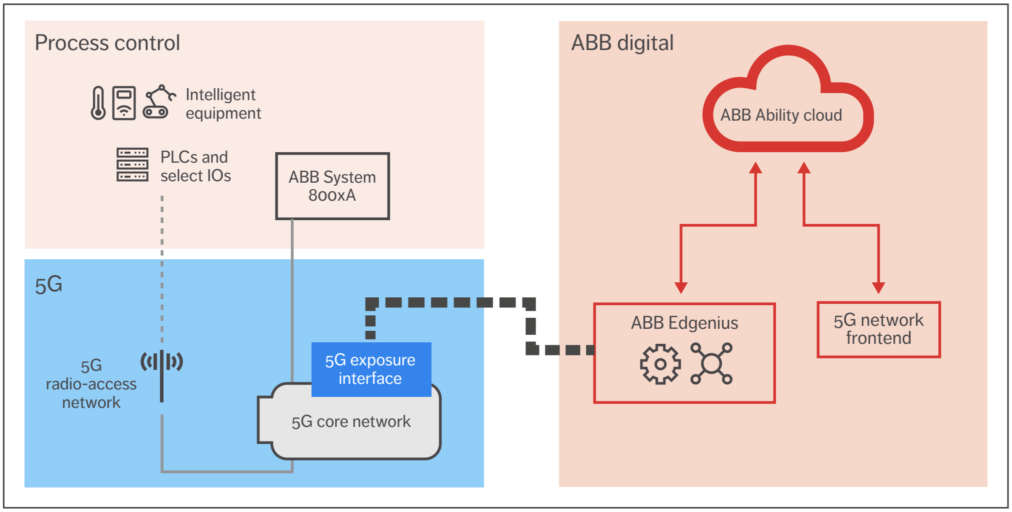


Figure 2 Overview of the demonstrator that integrates an ABB Ability automation system with Ericsson's prototype 5G exposure interfaces

interfaces acting as TSC CNC enable applications such as Centralized User Configuration to discover the availability of resources for a TSC stream and request the creation of a TSC stream with QoS.

Validating the 5G-ACIA exposure concept in partnership with ABB

The proof of concept at ABB integrates Ericsson's pre-standard, prototype 5G exposure interfaces implementation with ABB's cloud-based digital ecosystem (ABB Ability [6] and ABB Ability Edgenius [7]) to achieve 5G network programming by an automation system and thereby validate the exposure capabilities in practice.

The proof of concept offers a plant operator an easy-to-use environment for managing and monitoring the 5G connectivity of networked industrial devices. It also makes it possible to tailor the behavior of the 5G network to the communication requirements of industrial applications and obtain knowledge regarding the status and performance of 5G connections and virtual networks. By means of these capabilities, network-aware applications can interact with an externally operated network infrastructure without the need to know or understand the details of the underlying network technologies.

As illustrated in *Figure 2*, the 5G network frontend allows the control of 5G connectivity for ABB core control devices and intelligent equipment from a web application using the Ability cloud platform and an on-site Edgenius edge module. The Edgenius module interacts with the 5G network's programmable interfaces that expose the management capabilities of the 5G network, thereby offering a unified way of centrally controlling 5G performance (using ABB Ability, in this case).

The 5G network frontend web application provides the means to seamlessly provision and onboard 5G devices, monitor their connectivity performance and create device groups with different QoS attributes on top of the shared 5G infrastructure. Therefore, the developed tool also creates a convenient and scalable solution for configuring and monitoring the 5G network to facilitate the execution of everyday tasks by OT users, from automation engineers to plant operators.

By bringing 5G device management and monitoring data “closer” to the application operation and engineering data, this proof of concept allows the management of several 5G device groups from the tool, mainly based on ABB’s digital solutions. This approach would also make it possible to utilize existing tools in ABB’s digital portfolio to achieve easier and faster development of both simple and advanced network management solutions for the industrial wireless domain.

As a result of the collaboration with Ericsson, ABB also investigated the feasibility of using the exposure capabilities for flexible 5G network programming. This involved allowing different ABB automation solutions to make use of 5G technology, while at the same time shielding these solutions from 5G network implementation details and complexities. The results show how an OT organization (automation vendor or plant operator) could use one logical cloud instance to manage all 5G networks centrally as they grow, or as new ones are added.

The proof of concept at ABB clearly demonstrates that it is possible to run network automation across the boundaries between OT automation systems and private 5G networks, which is a prerequisite for using 5G as a part of automation solutions.

The critical role of 3GPP in enabling the IIOT

Both ABB and Ericsson are active proponents of standardized technologies such as 3rd Generation Partnership Project (3GPP)-based solutions. Emerging 3GPP standard technologies such as the network exposure function (NEF), the service enabler architecture layer (SEAL) for verticals and the common API framework (CAPIF) have the potential to address the exposure-related requirements of the verticals by offering integration points between automation systems and the 5G network.

3GPP standard exposure technologies hide the complexity of 5G and offer industry verticals a simple, secure, use-case-oriented configuration interface to the 5G system. The exposure interfaces will be invaluable to a multitude of industrial use cases, allowing industry verticals to make use of the key features and performance that 5G has to offer in a simple and straightforward manner.

> “ 3GPP STANDARD EXPOSURE TECHNOLOGIES OFFER INDUSTRY VERTICALS A SIMPLE, SECURE, USE-CASE-ORIENTED CONFIGURATION INTERFACE ”

The 3GPP has already made significant progress toward exposing the capabilities of mobile networks through APIs. While it is well known that the 3GPP core network capabilities are exposed by the NEF, since release 16 the 3GPP has also been standardizing higher-level APIs to address requirements from various vertical applications, with further enhancements specified in release 17, and additional functionality currently under study for release 18.

Figure 3 provides an overview of 3GPP standards that are applicable for IIoT use cases, as defined by the 3GPP SA6 working group. From the bottom to the top, the following three layers of 3GPP exposure are depicted:

1. The network exposure layer, which exposes core network capabilities
2. The SEAL, which exposes common service enablers for verticals
3. The vertical application enabler (VAE) layer, which exposes vertical-specific service enablers.

3GPP network exposure function

The basic 3GPP core network exposure layer consists of the 5G NEF, which offers network capabilities exposure of the 5G Core toward external applications integrated with the 3GPP network. The following subset of NEF APIs [8] are relevant for IIoT use cases:

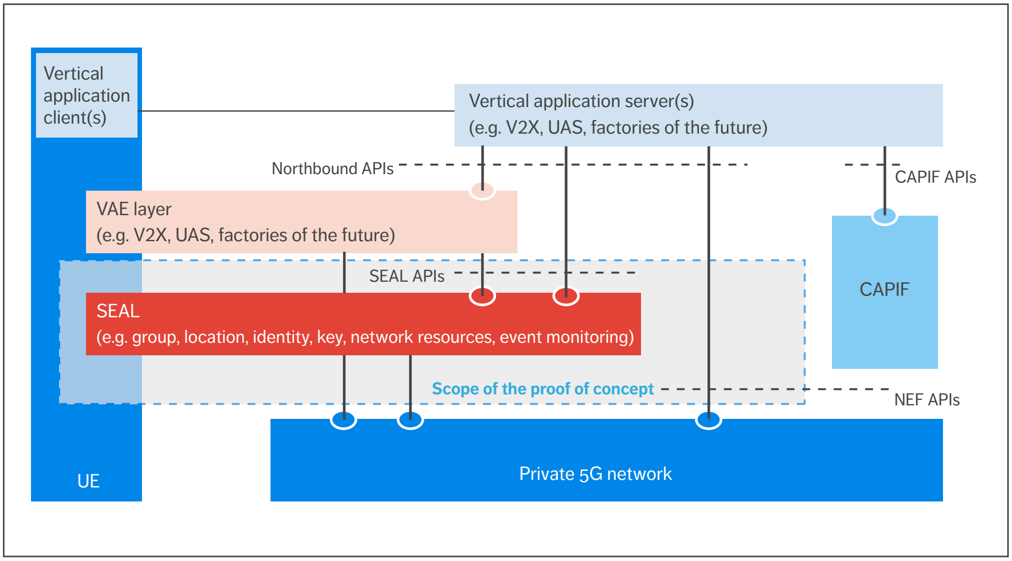

Vertical application client(s)
Vertical application server(s)
(e.g. V2X, UAS, factories of the future)
Northbound APIs
CAPIF APIs
VAE layer
(e.g. V2X, UAS, factories of the future)
SEAL APIs
CAPIF
SEAL
(e.g. group, location, identity, key, network resources, event monitoring)
Scope of the proof of concept
NEF APIs
UE
Private 5G network

Figure 3 Overview of 3GPP standards applicable for IIoT use cases

- Event monitoring (device location, reachability, connection status)
- AF session with QoS (on-demand QoS for IP and Ethernet connections)
- Analytics exposure
- 5G LAN parameter provisioning (device group management)
- Service parameter provisioning (route selection parameters)
- Time sync exposure
- UE ID retrieval (AF-specific device ID retrieval, such as GPSI)

> “THE SEAL ENABLES COMMON SERVICES THAT APPLICATIONS CAN UTILIZE FROM VARIOUS VERTICAL DOMAINS”

3GPP service enabler application layer

Because the NEF APIs expose network capabilities in a highly granular manner, application developers that use them must have a good understanding of the underlying network concepts. To simplify application development and deployment, 3GPP has specified a new layer of simplified service enablers. The SEAL [9] consists of service enablers that provide services that are not specific to any vertical – that is, they are common services that applications can utilize from various vertical domains. The APIs currently defined by SEAL are for group management, location management, identity and key management, and network resource management (NRM).

Group management allows the application to create and manage device groups for different purposes such as group communication and location-based groups, while the SEAL ensures that the devices are properly notified and joined into the group. Location management makes it possible to provide device location information from different sources – both 3GPP and non-3GPP (such as Global Navigation Satellite Systems) – to an application

Industry vertical requirements (5G-ACIA)	3GPP exposure capabilities
Device connectivity management	• SEAL NRM QoS and TSC APIs • NEF QoS API • NEF time sync exposure API
Device connectivity monitoring	• SEAL NRM event monitoring and QoS monitoring APIs • NEF event monitoring API • NEF QoS API • NEF analytics API
Device group communication management	• SEAL group management APIs • NEF 5G LAN parameter provisioning API
Device provisioning and onboarding	• Provided by the APIs of business support systems
Device identity management	• GPSI is supported as the device identifier • An IP/MAC address can be used to identify a device • SEAL identity and key management APIs can be used as part of the security framework
Device location information	• SEAL location management APIs • NEF event monitoring API (UE location reporting)

Figure 4 Summary of 3GPP exposure capabilities and APIs that satisfy the requirements of IIoT use cases

either on demand or upon change, and to define location areas of interest for specific use cases. Identity and key management support applications in managing security material used in the authentication and authorization of users and devices.

Lastly, NRM enables application-specific usage and monitoring of network resources used by the devices covering:

- Unicast and multicast connection activation, deactivation and modification including QoS parameters
- Unicast connection QoS monitoring including packet delay, packet loss rate, data rate and traffic volume
- Event monitoring including device mobility, communication, loss of connectivity, location reporting and connection status
- Time-sensitive, deterministic device-to-device and device-to-enterprise-network communication.

The SEAL is expected to evolve and grow with additional service enablers in the upcoming 3GPP release 18.

3GPP vertical application enabler layer

In contrast to the SEAL, the VAE layer is tailored to satisfy specific vertical applications. These types of vertical service enablers are currently defined for automotive applications referred to as vehicle-to-anything (V2X) communication and drone applications known as unmanned aerial systems (UAS). VAE for factories of the future will include future enhancements specific to OT verticals.

Meeting IIoT requirements with 3GPP exposure capabilities

Figure 4 shows how the IIoT requirements outlined by 5G-ACIA match up to 3GPP release 17 exposure capabilities and APIs.

Conclusion

Widespread use of private 5G networks in the Industrial Internet of Things (IIoT) ecosystem will require a standards-based exposure solution that makes it possible to flexibly configure the 5G system according to the specific communication requirements of individual production processes. Communication service providers (CSPs) have an excellent opportunity to monetize the IIoT with a service offering that exposes the powerful capabilities of 5G networks to industry verticals. The reduction in manual network configuration tasks allows customer support departments of CSPs to scale up the number of enterprise customers they can serve.

A standards-based 5G IIoT exposure solution will enable industrial enterprises to use 5G as a part of system infrastructure, increasing production flexibility and scaling up to a large number of 5G-connected devices in an organized and secure manner. It will also open the door for IT/OT platform vendors to develop their own products that take advantage of 5G capabilities and enable system integrators to simplify the integration of operational technology applications with the wireless connectivity that 5G systems provide.

Terms and abbreviations

3GPP – 3rd Generation Partnership Project | **5G-ACIA** – 5G Alliance for Connected Industries and Automation | **AF** – Application Function | **AGV** – Automated Guided Vehicle | **API** – Application Programming Interface | **AR** – Augmented Reality | **CAPIF** – Common API Framework | **CNC** – Centralized Network Configuration | **CSP** – Communication Service Provider | **GPSI** – Generic Public Subscription Identifier | **IO** – Input/Output | **IoT** – Internet of Things | **IIoT** – Industrial IoT | **LAN** – Local Area Network | **NEF** – Network Exposure Function | **NRM** – Network Resource Management | **OT** – Operational Technology | **PLC** – Programmable Logic Controller | **QoS** – Quality of Service | **SEAL** – Service Enabler Architecture Layer | **TSC** – Time-Sensitive Communications | **TSN** – Time-Sensitive Networking | **UAS** – Unmanned Arial Systems | **UE** – User Equipment | **V2X** – Vehicle to Anything | **VAE** – Vertical Application Enabler | **VLAN** – Virtual Local Area Network | **VN** – Virtual Network

Further reading

- **Ericsson blog, How enterprises can exploit the exposure capabilities of private 5G networks, available at:** *https://www.ericsson.com/en/blog/2020/7/private-5g-network-capabilities-enterprise*
- **Ericsson, Network exposure, available at:** *https://www.ericsson.com/en/service-orchestration/network-exposure*
- **Ericsson blog, Network programmability in 5G, available at:** *https://www.ericsson.com/en/blog/2019/1/network-programmability---in-5g-an-invisible-goldmine-for-service-providers-and-industry*
- **Ericsson, Dedicated networks, available at:** *https://www.ericsson.com/en/portfolio/enterprise-wireless-solutions/dedicated-networks*
- **Ericsson, Industry 4.0, available at:** *https://www.ericsson.com/en/industry4-0*
- **Ericsson, 5G for manufacturing, available at:** *https://www.ericsson.com/en/5g/manufacturing*

References

1. **Ericsson Technology Review, Boosting smart manufacturing with 5G wireless connectivity, February 20, 2019, Sachs, J; Wallstedt, K; Alriksson, F; Eneroth, G, available at:** *https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/boosting-smart-manufacturing-with-5g-wireless-connectivity*
2. **Ericsson-Hexagon Report, Connected Manufacturing – A guide to Industry 4.0 transformation with private cellular technology, November 2020, available at:** *https://www.ericsson.com/en/enterprise/forms/connected-manufacturing*
3. **German Federal Ministry for Economic Affairs and Energy (BMWi), Fortschreibung der Anwendungsszenarien der Plattform Industrie 4.0 (Continuation of the Application Scenarios of the Plattform Industrie 4.0), October 2016, available at:** *https://www.plattform-i40.de/IP/Redaktion/DE/Downloads/Publikation/fortschreibung-anwendungsszenarien.pdf*
4. **5G-ACIA white paper, Exposure of 5G Capabilities for Connected Industries and Automation Applications, February 2021, available at:** *https://5g-acia.org/wp-content/uploads/WP_039_Network-Exposure-Interface_single-pages.pdf*
5. **IEC, Understanding IEC 62443, February 2021, available at:** *https://www.iec.ch/blog/understanding-iec-62443*
6. **IEC 62443-3-3, Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels, available at:** *https://webstore.iec.ch/preview/info_iec62443-3-3%7Bed1.0%7Db.pdf*
7. **ABB, ABB Ability, available at:** *https://global.abb/topic/ability/en*
8. **ABB, ABB Ability Edgenius Operations Data Manager, available at:** *https://new.abb.com/process-automation/edgenius*
9. **3GPP Technical Specification 23.502, Procedures for the 5G System (5GS): Stage 2, available at:** *https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3145*
10. **3GPP Technical Specification 23.434, Service Enabler Architecture Layer for Verticals (SEAL); Functional architecture and information flows, available at:** *https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3587*

THE AUTHORS

Gergely Seres

◆ is an expert and chief architect of software technology and application architecture at Business Area Cloud Software and Services, currently working with 5G and the Internet of Things (IoT). Since joining Ericsson in 1998, he has held several research, technical and managerial positions. He holds a Ph.D. in electrical engineering from the Budapest University of Technology and Economics, Hungary.

Dirk Schulz

◆ is a senior principal scientist with ABB Research, responsible for the communication architecture of industrial automation systems. He has been with ABB since 2006, working in different scientific and project management roles. He holds a Ph.D. (Dr. rer.-nat.) in communications engineering from the University of Mannheim, Germany.

Ognjen Dobrijevic

◆ is a principal scientist with ABB Corporate Research. He is working on different aspects of future industrial communication systems, with a focus on wireless connectivity and edge computing. Dobrijevic has been with ABB since 2018 and holds a Ph.D. in electrical engineering from the University of Zagreb, Croatia.

Abdulkadir Karaağaç

◆ is a scientist with ABB Corporate Research, working on communication and interoperation solutions for industrial automation systems. Karaağaç holds a Ph.D. in computer science from Ghent University in Belgium, and he has been with ABB since 2020.

Hubert Przybysz

◆ is an expert in core network exposure at Business Area Cloud Software and Services. He joined Ericsson in 1990. His current assignments are focused in the areas of Industrial IoT (IIoT) and exposure of 5G system capabilities. Przybysz holds an M.Sc. in telecommunications from the Warsaw University of Technology in Poland.

Ala Nazari

◆ is an expert in media delivery architecture and in 5G for critical IoT. He joined Ericsson in 1998 and has been working with 3G/4G/5G, broadband access, transport and media delivery. He has also worked as a senior solution architect and engagement director. Nazari holds an M.Sc. in computer science from Uppsala University in Sweden.

Peter Chen

◆ is the system owner of core network exposure at Business Area Cloud Software and Services, where he focuses on technology strategy and evolution in the network exposure area. He has been working in different areas within the core network since he joined Ericsson in 2006, and contributed more than 20 patents within Ericsson. He holds a B.Sc. from Dalian University of Technology, China.

Márk László Mikecz

◆ is an architect of 5G network exposure at Business Area Cloud Software and Services. He joined Ericsson in 2016. His current assignment is focused on the 5G exposure interface proof of concept. Mikecz holds a B.Sc. from the Eötvös Loránd University in Budapest, Hungary.

Áron Dénes Szabó

◆ joined Ericsson in 2021 as a system architect of 5G network exposure at Business Area Cloud Software and Services. His work focuses on standardization and prototyping in 5G IIoT. Szabó holds an M.Sc. in engineering physics and a Ph.D. in electrical engineering from the Budapest University of Technology and Economics.

ISSN 0014-0171
284 23-3383 | Uen

Ericsson
SE-164 83 Stockholm, Sweden
Phone: +46 10 719 0000