Ericsson White Paper
3/221 09-FGB 1010949
December 2019

Critical capabilities for private 5G networks

A new generation of private 5G networks is emerging to address critical wireless communication requirements in public safety, operations of industries and critical infrastructure. These private networks are physical or virtual cellular systems that have been deployed for private use by a government, company or group of companies.

Critical capabilities are network features and services that are needed to serve mission-critical or business-critical use cases. Mission-critical functions are vital to an organization's or society's operation, such as public safety services and electricity. On the other hand, for a company to be successful, business-critical functions like production and sales are essential.

3GPP 4G and 5G technologies offer a powerful platform with built-in support for the necessary critical capabilities, increased reliability, lower latency and improved security, meeting the requirements of business- and mission-critical applications.

Historically, this space has been dominated by networks based on technologies such as ethernet, fiber, Wi-Fi, WiMAX, CDMA450 or Bluetooth, or LMR networks (based on P25 or TETRA standards). However, these networks still fail to solve key customer issues. Given communications incidents can have a significant negative impact on business and operations and, at worst, result in loss of life, we are seeing a migration towards 3GPP-based networks.

Introduction

A new generation of private 5G networks is emerging to address critical wireless communication requirements in public safety, infrastructure and industry. These private networks are physical or virtual cellular systems that have been deployed for private use by governments or companies. Non-public network (NPN) is the term adopted by 3GPP for such networks.

Critical capabilities are network features and services that are needed to serve mission-critical or business-critical use cases. Mission-critical functions are vital to an organization's or society's operation, such as public safety services and electricity. On the other hand, for a company to be successful, business-critical functions like production and sales are essential. Business-critical services exist in multiple industries, such as utilities, rail, natural resources, airports, ports and manufacturing.

Driven by industry digitalization, new technologies such as 5G and IoT are being applied to industrial networks. Another trend in the market is the modernization of land mobile radio (LMR) systems. What links these trends is that the transformations are happening at the same time, in the same industries, with one technology and network serving all use cases.

3GPP 4G and 5G technologies offer a powerful platform with built-in support for the necessary critical capabilities, increased reliability, lower latency and improved security, meeting the requirements of business- and mission-critical applications.[1]

Definitions

- Mission-critical communications represent voice and data services that help to prevent loss of life and injuries, and minimize economic impact during disaster and emergency situations.
- Business-critical communications represent voice and data services that help prevent severe financial and economic issues involving property, business and/or society.

These services demand more from the network in terms of higher availability, reliability, security, coverage and capacity, and sometimes lower latency.

The opportunities and challenges

Historically, this space has been dominated by networks based on technologies such as ethernet, fiber, Wi-Fi, WiMAX, CDMA450 and Bluetooth, and by LMR networks (based on P25 or TETRA standards). However, these networks still fail to solve key customer issues. Given communications incidents can have a significant negative impact on business and operations and, at worst, can result in loss of life, more reliable and capable networks are required.

Some of the opportunities and challenges that are driving this migration are as follows:

- Existing narrowband mission-critical networks reaching the end of their life cycle. This has been particularly visible in public safety — the early adopter of new technology — and is triggering other verticals with critical needs to follow suit.
- Industry 4.0-related productivity gains through more flexible production, increased mobility (in over 10 million mobile unconnected sites) and enterprise connectivity.
- A need for improved data security, to make critical assets unbreachable and to dynamically customize the network in challenging situations.
- Data-heavy use cases for new augmented reality (AR), virtual reality (VR) and HD video-based applications, for remote inspection, monitoring and surveillance.
- Continuous investments and innovations in 3GPP technologies, making them more attractive to industries and governments that were not previously addressable.

Industry digital revolution

Digital transformation has long remained at the top of many business agendas and has spread across multiple industries. The Industry 4.0 vision calls on industries to collect and utilize data in order to tap into new IoT revenue streams and cost savings.

Practically all industry sectors are pursuing enhanced operating models that improve security and productivity through analytics and automation.

Use cases typically discussed are as follows:

- factory-floor automation and flexibility
- real-time situation awareness solutions (including sensors, HD video surveillance and massive diagnosis data upload)
- preventive maintenance
- workforce management
- machine utilization optimization
- risk management (safety area management)
- remote asset control (sensor monitoring)
- worker health and safety (with AR/VR or push-to-talk voice)

These use cases require high network performance levels, together with data management capacity, reliability, quality of service (QoS), latency, security and flexible coverage. Business-critical cellular connectivity solutions are well suited in providing the different characteristics necessary for these use cases.

The more use cases consolidated in the same network, the stronger the dependency on network service by enterprises or government entities. To ensure QoS over the wireless medium, private networks operating on licensed spectrum are a good option. Access to licensed spectrum can primarily be achieved through mobile communications service providers. In addition, several countries are currently considering directly licensing 4G and 5G spectrum to enterprises and governments. The US and Germany are among those announcing licensed spectrum allocation for mission-critical and industrial use.

Bridging the communications gap

Critical capabilities target the fulfillment of multiple key performance indicators (KPIs) in a 3GPP cellular connectivity solution. Private networking is related to the degree of control that the given industry has over the provided service.

Although a wide variety of IoT use cases can be run over private networks, most use cases' similar connectivity needs are covered by standardized critical 3GPP functions.

Mobile technologies before, and including, 4G were designed to support voice and best-effort services and were not initially considered for mission- or business-critical communications. However, standardization efforts to better serve such use cases were ramped up with 3GPP Rel-12.

In the mission-critical domain, public safety was an early 3GPP critical communications requirement driver, with several features introduced in LTE Rel-12. Main features for low-end IoT devices, denoted as massive IoT, were introduced in LTE Rel-13 with NB-IoT and Cat-M. In parallel, more capable IoT device categories, the broadband IoT set, have been defined.

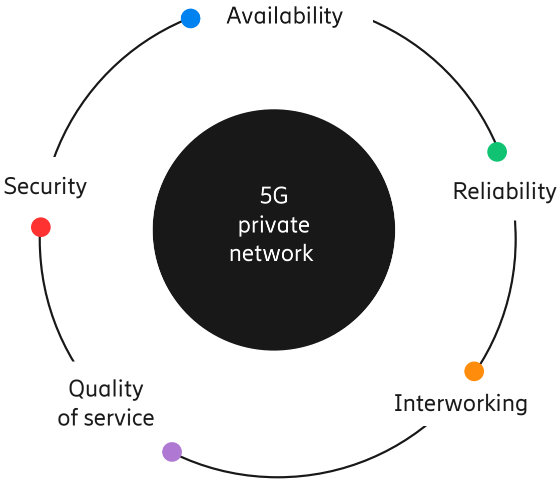
5G, on the other hand, is designed to handle critical communications from the start. A set of critical capabilities are included as intrinsic components in the first 3GPP standard for 5G, Rel-15, in the Ultra Reliable Low Latency Communication (URLLC) feature set.[2] Evolution continues in Rel-16, with industry use case adoption in the form of 5G integration and time-sensitive networking (TSN) as part of New Radio (NR) Industrial IoT. TSN is an extension of the IEEE ethernet standard to provide reliable and deterministic low-latency communication to be used, for example, in future converged industrial communication networks.

Requirements for 5G private networks

Private networks for the public safety segment and essential industrial applications are built to ensure continuity of service even when unpredictable and undesirable events occur. They also ensure that critical civil functions and business processes have access to high-quality communication, even when parts of the system fail due to external factors.

In practice, ensuring continuity of service in critical networks means building secure networks with high availability and reliability. The main critical capability requirements are summarized in Figure 1.

Figure 1: 5G private network requirements



● Availability

High availability means that the end user can always use the service. In practice, the network must be built so that downtime is virtually zero and any system maintenance can be controlled, guaranteeing maximum availability. This may include robust solutions and redundancy constructions of critical elements.

● Reliability

Reliability refers to the capability of transmitting a given amount of traffic within a predetermined duration with high success probability. It requires sufficient network coverage and capacity, as well as robust handover functionality.

● Interworking

Interworking with public networks is an important capability. Many critical services like ambulances need service continuity while moving from one network to another, for instance from a private network to a public network. This requires a level of integration between networks. Possible deployment options are discussed on page 8.

● Quality of service

QoS comprises throughput, latency, jitter, packet drop rate and more. Running private networks on dedicated spectrum offers the possibility to control each. Furthermore, system performance and resource use for different services can be tailored to the specific needs within private network deployment.

● Security

Private networks are expected to provide full end-to-end security to ensure information, infrastructure and people are protected from threats. This involves implementing measures to preserve the three main security principles: confidentiality, integrity and availability.

Private networks utilize network isolation, data protection and device/user authentication to protect key assets. Enterprises can also control retention and data sovereignty to ensure sensitive information is kept on-premises.

Spectrum considerations

In order to minimize or even eliminate external interference, it is important to have control of the spectrum used for over-the-air transmission. In most countries, spectrum is treated as a natural resource, with usage controlled by national authorities which allocate resources according to the country's needs.

Spectrum is divided into several frequency bands. Bandwidths are specified by authorities and depend on the needs of the user and of others competing for the same resource. Some spectrum is aligned with international standard bands, as in 3GPP. Spectrum can be either licensed, which means that the license holder is the only authorized user of that spectrum range, or unlicensed, which means that anyone who wants to use the spectrum can do so, such as for Wi-Fi.

Unlicensed spectrum can be used by anyone, anytime. As a result, it can be unused and support very good service quality, or it can be completely congested and therefore insufficient for supporting good service quality for even simple applications. It is not possible to know the status at any point in time and thus unlicensed spectrum is not a good choice for critical communications with predictable deterministic performance.

A prerequisite for critical communications is full control of the spectrum. Today, only licensed spectrum guarantees control over spectrum usage by the system, making it a preferred option for critical communications. However, unlicensed spectrum can provide an additional resource for scaling non-critical communications.

In order to ensure critical communications, having sufficient and reliable bandwidth to support the required services is also important. Mobile communication spectrum is allocated at the launch of a new generation (such as 4G) and between launches, dependent on need and availability. Up to now, all spectrum dedicated to mobile communications has been allocated to service providers. These licenses have often been associated with coverage requirements and issued across whole countries, or in large regions. Since spectrum is a scarce resource, it is best unfragmented.

For 5G, new spectrum will again be allocated, with a significant part going to service providers, mainly for mobile communication purposes. Non-operator organizations may cooperate with service providers to realize critical communication services. Non-service providers may obtain access through service providers by leasing spectrum, or through other arrangements.

In an alternative model, some countries are now in the process of allocating parts of the 5G spectrum for local use to industries. These non-service providers then have a choice of applying for a license themselves and operating their own network, or cooperating with a service provider.

Spectrum access aside, there are several other reasons a non-service provider might consider cooperation with a service provider, such as service continuity when roaming inside and outside the non-service provider premises. This is further explored on page 8.

Technology evolution of critical capabilities in cellular networks

Mission-critical communications

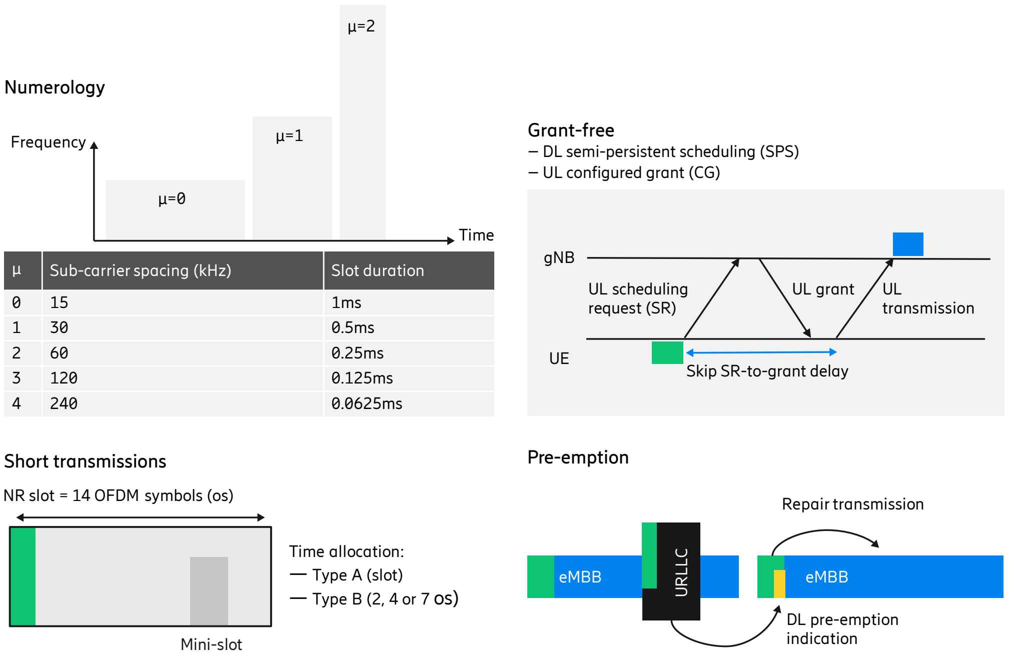
The first steps to address mission-critical services in cellular networks were taken in Rel-12 for 4G LTE, with new additions including mission-critical push-to-talk (MCPTT). The objective was to help national security and public safety (NSPS) organizations, such as emergency services, which today still largely utilize LMR networks, to modernize their networks and allow both MCPTT and critical broadband traffic, in order to enable new services. Further improvements in the mission-critical domain have been added in subsequent 3GPP releases.[3] For 5G, a summary of identified requirements for critical communications can be found in 3GPP TS 22.261.[4]

URLLC

With 5G NR, a new set of business-critical use cases are enabled, such as AR/VR, automated guided vehicles, cloud robotics, factory automation and real-time remote control of machines. A summary of the identified requirements for several industrial use cases can be found in 3GPP TS 22.104.[5] One major feature set addressing critical requirements has been URLLC, with the first features becoming available in Rel-15, while Rel-16 introduces further enhancements.

On a high level, the features introduced in these releases can be divided into low-latency and high-reliability features. The key low-latency features are a new physical layer design with new numerologies, short transmissions called mini-slots, grant-free transmissions, pre-emption, fast hybrid automatic repeat request (HARQ), out-of-order HARQ and PDCCH monitoring, as depicted in Figure 2.

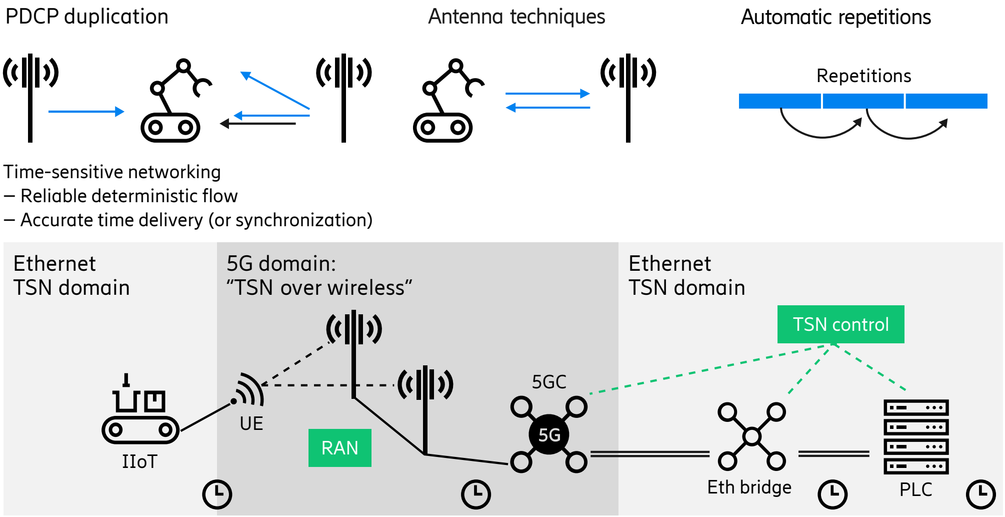
Figure 2: Low-latency features in NR



μ	Sub-carrier spacing (kHz)	Slot duration
0	15	1ms
1	30	0.5ms
2	60	0.25ms
3	120	0.125ms
4	240	0.0625ms

High-reliability features include robust physical channels with lower spectral efficiency, new antenna techniques, automatic repetitions, Packet Data Convergence Protocol duplication, and a TSN level of service with reliable deterministic flows and accurate synchronization, as summarized in Figure 3.

Figure 3: High-reliability features in NR



Industrial IoT

Rel-16 addresses a new set of specific industry automation demands, as well as 5G integration with TSN.[6]

As critical industrial communication is an emerging field, the work will continue in future NR releases. Topics under discussion for Rel-17 include industrial IoT and URLLC enhancements. However, the Rel-17 scope is yet to be determined.

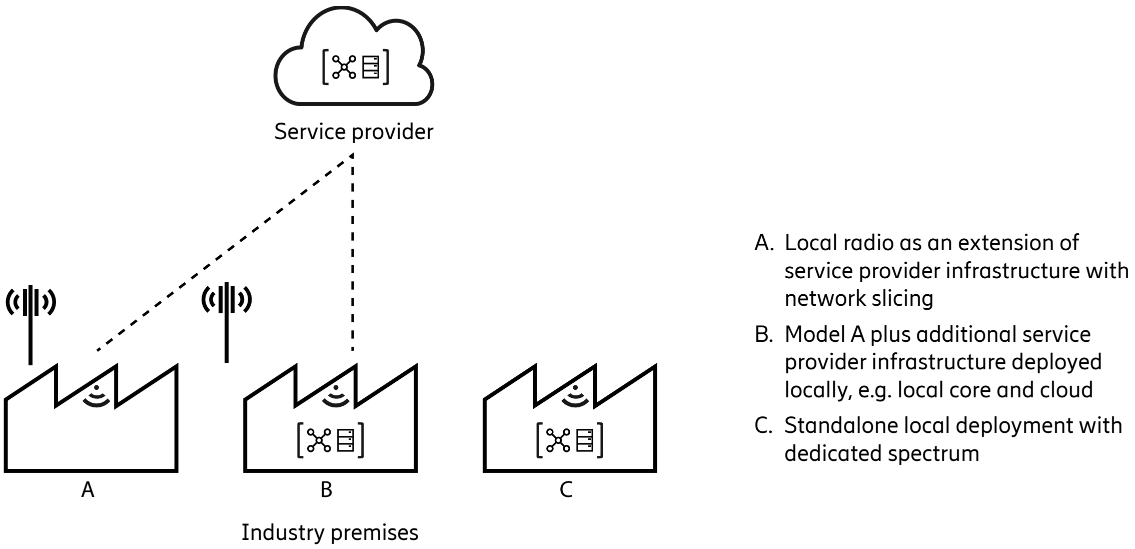
All in all, the 3GPP process is embracing industrial requirements with continued evolution for advanced industrial use cases.

Deployment models

A non-service provider may need to cooperate with a service provider to supply critical communication services. Examples where cooperation may be required for service continuity include roaming inside and outside the non-service provider network and gaining access to spectrum regions in order to support high-bandwidth services in wide area deployment. There are numerous other reasons, mostly relating to business efficiency, such as local network management, and leveraging functions in the central network. To facilitate the varying needs of different stakeholders, networks must be deployed flexibly.

In contrast to today's typical public mobile network services, 5G private networks (the term "non-public network" is used in 3GPP) are intended for the sole use of a private entity, such as an enterprise. Although these networks could cover one or multiple industrial sites like a campus or a factory, or could be country- or region-wide, the term "5G private network" is commonly linked to the former group. 3GPP distinguishes two types of NPNs, namely standalone NPN and NPN in conjunction with a public network. Different levels of integration to the public network are possible, with a few of the main options depicted in Figure 4.

Figure 4: Deployment models for private networks



A. Local radio as an extension of service provider infrastructure with network slicing
B. Model A plus additional service provider infrastructure deployed locally, e.g. local core and cloud
C. Standalone local deployment with dedicated spectrum

In Figure 4, model A shows a network where the only element added is private coverage, while all user plane and control plane elements are provided by the public network. Model B shows a network where the radio access network (RAN) and some control plane elements are shared with the public network but the NPN has its own local services too, while model C is the isolated network, where the whole network is deployed on-premises as a standalone NPN.

One possibility is that a service provider builds and operates a dedicated network for providing an NPN to industry customers. The dedicated network can be easily integrated into the service provider's network – i.e. they can either use parts of their own spectrum or spectrum acquired by the non-service provider. Several potential benefits result, including roaming between the dedicated and public networks, a tight integration that enables service continuity.

Another aspect to consider is the operation and maintenance of the network. In the standalone model, these activities need to be arranged for the NPN, while with the public network integrated model, the public network operator may take care of part of these services, according to the integration level. This will be discussed in more detail in the next section.

Operation and management of private networks

The operations and life cycle management (LCM) of a critical system are as important as the system itself. The system must be designed to guarantee automated deployment and configuration, and efficient operation and maintenance throughout its life. Monitoring of relevant functions will be necessary to secure full reliability and to predict and avoid incidents. Possible predictive maintenance solutions may be based on artificial intelligence and machine learning, together with relevant KPI monitoring and early issue alerting. Another very important aspect is to avoid system obsolescence through regular updates. With efficient LCM, the system should always have access to the latest technology options. Although industries are just beginning their digital transformation, the right balance should be struck between system capabilities, management and evolution.

Future-proof solutions

Leveraging 5G technologies for industries is in its early stages and most of the new use cases are still being defined and tested. At the same time, many requirements can already be fulfilled with mature 4G solutions. Finding the right balance between what is necessary today and what is needed for the future is important, in order to avoid sitting on obsolete systems soon after deployment. Flexibility and partnerships hold the key to addressing these concerns, with solutions that allow for a stepwise, "building block" approach holding the ability to take evolutionary needs into account.

As an example of partnerships and flexible deployment, a company may commence a joint solution with a service provider by leveraging the service provider's 4G network assets.[7] Later, private 5G components may be added to the network, as well as control systems and applications. Alternatively, a company may completely outsource the solution and just agree connectivity capabilities and service level agreements with a service provider directly, without defining whether 4G or 5G technology is used.

Today's introduction of 3GPP cellular connectivity is just the beginning of the journey for industries and governments, where the expected evolution needs will be important in defining the future solution.

Conclusion

Be it a mission-critical public safety service or a business-critical industrial site, 3GPP-based wireless private networks — deployed either standalone or in conjunction with public networks — enable the use of wireless communication for critical applications, with stringent communication requirements for many use cases. The global 3GPP ecosystem secures cost-efficient, future-proof products and services for evolution. Through 5G critical wireless private networks, industries can faster realize Industry 4.0.

References

[1] Sachs, J., Wallstedt, K., Alriksson, F. & Eneroth, G., 2019. Boosting smart manufacturing with 5G wireless connectivity. Ericsson Technology Review, January.

[2] Liberg, O. et al., 2019. Cellular Internet of Things – From Massive Deployments to Critical 5G Applications. s.l.:Academic Press.

[3] Liberg, O. et al., 2019. Cellular Internet of Things – From Massive Deployments to Critical 5G Applications. s.l.:Academic Press.

[4] 3GPP, n.d. *TS 22.261* "Service Requirements for the 5G System". [Online].

[5] 3GPP, n.d. *TS 22.104* "Service Requirements for Cyber-Physical Control Applications in Vertical Domains". [Online].

[6] Farkas, J., Varga, B., Miklós, G. & Sachs, J., 2019. 5G-TSN integration for industrial automation. Ericsson Technology Review, August.

[7] Sharing for the best performance – Stay ahead of the game with Ericsson Spectrum Sharing.

Author biographies

Anna Larmo
Anna Larmo joined Ericsson in 2004 and currently serves as a Principal Researcher at Ericsson Research, Finland, leading cross-functional manufacturing and industrial IoT activities. In addition to 3GPP, she has worked on Bluetooth and Wi-Fi standardization. Other research interests include simulators, software, inventions and innovation.

Peter von Butovitsch
Peter von Butovitsch joined Ericsson in 1994 and currently serves as Technology Manager within Systems & Technology. He has held various positions at Ericsson Research and in RAN system design, and from 1999 to 2014 worked in Japan and China. He holds both an M.Sc. in Engineering Physics and a Ph.D. in Signal Processing from KTH Royal Institute of Technology in Stockholm, Sweden. In 2016, he earned an MBA from Leicester University, UK.

Patricia Campos Millos
Patricia Campos Millos has been Ericsson's Business Development Director for Mission Critical and Private Networks since 2016. She holds an M.Sc. in Telematics Engineering and a Bachelor's degree in Telecommunication Technologies Engineering from the University of Vigo, as well as a Master's degree in Business and Administration from the IEDE Business School in Madrid. Since joining Ericsson in 2005 she has held a number of business development, product management, R&D system and technology positions.

Patrik Berg
Patrik Berg is Head of Mission Critical Applications at Ericsson, with the global responsibility of defining Ericsson's portfolio in this area. He also works on strategic partnerships and participation in 3GPP standardization, and has more than 20 years' experience in different management positions at Ericsson. His career began with the emergence of mobile broadband, where he was part of the first mobile broadband design team. In the last 10 years, his focus has been on public safety and defense. He holds an M.Sc. in Electrical Engineering from LTH, Lund University, in Sweden.

Acknowledgments
The authors would like to thank Bob Gessel, Fredrik Wallgren, Jason Johur, Fiona Fan, Anders Hellström, Danielle Francis, Per Ljungberg, Joachim Sachs, Elvin Chong, Ali Zaidi, Klaus Mehler, András Zahemszky and Scot Harris for their help.