

Deloitte.

Private 5G networks

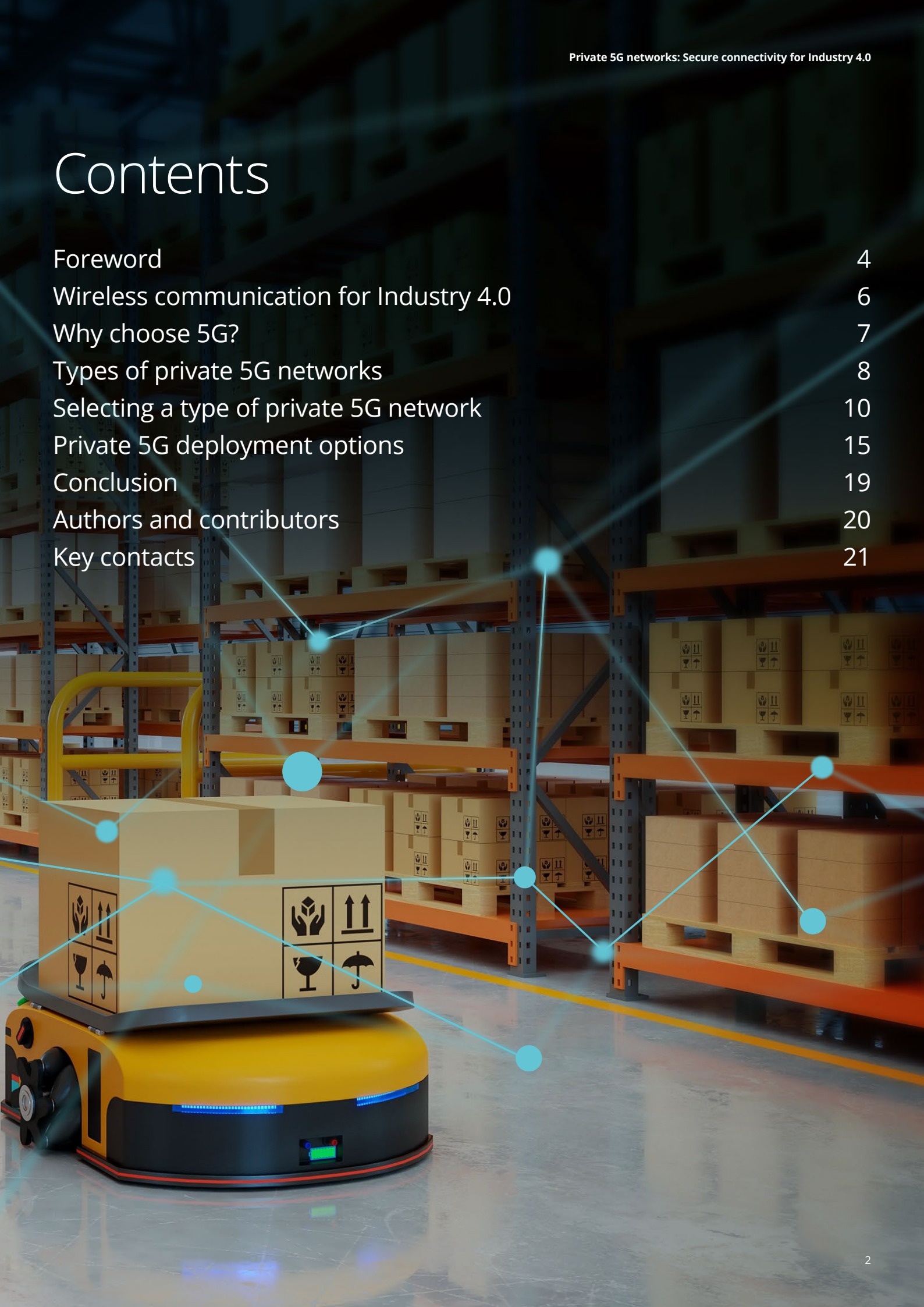
Secure connectivity for
Industry 4.0

**MAKING AN
IMPACT THAT
MATTERS**
since 1845



Contents

Foreword	4
Wireless communication for Industry 4.0	6
Why choose 5G?	7
Types of private 5G networks	8
Selecting a type of private 5G network	10
Private 5G deployment options	15
Conclusion	19
Authors and contributors	20
Key contacts	21





Foreword

The advent of Industry 4.0 technologies and use cases promises to revolutionise manufacturing, with new capabilities unlocking tremendous performance gains from Overall Equipment Effectiveness (OEE) to waste reduction and supply chain optimisation. Early adopters are further integrating information technology (IT) with operational technology (OT) to implement use cases ranging from predictive maintenance to remote support via augmented reality applications. Others are deploying intelligent autonomous vehicles in factories and warehouses to optimise efficiency and reduce errors which can lead to safety incidents.

What do all these use cases have in common? They are data driven. They require advanced, flexible, and increasingly mobile connectivity.

But while some forms of wireless connectivity are already employed for select manufacturing operations, previously available technology has typically not met operational requirements for broader use in factories. Safety, reliability, and uptime are of the utmost importance in manufacturing, and the technology was simply not robust enough. Nor was there such a pressing need for more modern wireless technology.

In this report, we examine key operational requirements in manufacturing operations and how these translate to network communications in OT. We then explain how 5G wireless technology provides the reliability, security, flexibility, and performance required by industrial applications. We introduce different types of 5G deployment scenarios and highlight key factors for factory owners to consider while embarking on this journey.

It is fair to assume that, going forward, wireless communication is going to play a more prominent role in factories than it does today. 5G in particular is expected to seamlessly replace or integrate with existing wired connections. With robust built-in functionality, security and flexibility, the technology caters well to many industrial applications and is positioned to become a ubiquitous communication backbone for smart factories.

We hope that this report provides you with helpful insights as you prepare to enhance connectivity in your factories and leverage the enormous potential of Industry 4.0 use cases.

Sincerely,

Dr. Anand R. Prasad

Asia Pacific Cyber Technology, Media
& Telecommunications leader
Deloitte



Wireless communication for Industry 4.0



Ubiquitous connectivity is one of the main drivers of the fourth industrial revolution. It is about increasing efficiency in the production process through a higher degree of automation supported by machine-to-machine communication. It is also about a higher degree of flexibility where machinery can freely move, or be moved, around the factory floor. At the same time, workers should be able to continuously monitor the system state, location, and production processes while safely working alongside machines.

Under these circumstances, it is fair to assume that wireless communication is going to play a more prominent role in factories than it does already today. But how can one be sure that the communication is secure? How reliable is wireless communication? How can wireless communication be effectively used in factories? And which wireless technology is best suited for these scenarios? Many factory owners planning on using wireless communications will ask these types of questions. In this section, we will elaborate on what security means in terms of factory automation.

Security equals safety on the factory floor

One of the most fundamental tenets of information security is the triad of confidentiality, integrity, and availability—in short CIA. In many IT scenarios the order of priority is exactly that—first C, then I, and lastly A. However, industrial applications, i.e. OT scenarios, commonly have different priorities. Whereas ensuring confidentiality is most often a secondary concern, availability, integrity, and latency are of utmost importance because they are essential prerequisites for the uptime, reliability, and safety that is expected in industrial settings.

Availability relates to the uptime of the system. In the context of network communication, this also includes the reachability of connected system components. If reachability over the network cannot be ensured, it can have a significant impact on the operation, resulting in interruptions or even a complete shutdown of the production line.

Integrity relates to the correctness of information being processed. In a smart factory scenario, connected machinery is expected to be controlled and monitored remotely. To ensure the reliability of data transmissions for

remote control and monitoring, communication over the network needs to be protected.

In addition to traditional security objectives, network communication in industrial settings may also be subject to strict performance requirements. One such performance aspect is latency, which shapes timely and deterministic transmission of information over the network. Certain OT use cases have hard latency requirements to ensure reliable operation of the system. Introducing wireless connectivity in scenarios that have so far been connected by cables must not result in a deterioration of networking performance.

OT is where cyber security incidents turn into real-world safety incidents

The differences between IT and OT do not end there. Due to the nature of industrial applications, OT systems pose additional safety requirements that are of little concern to the IT domain. Preventing physical harm to factory workers, the environment, and the public is a key requirement during the design, development, and build of any industrial control system. Since much of said machinery is controlled or monitored remotely, the network plays an essential role in assuring safety as well.

Factory owners must consider the safety perspective, especially if the system handles dangerous substances or works side-by-side with humans. It is here that cyber security incidents turn into real-world safety incidents.

Why choose 5G?



The question that remains is why factory owners should choose 5G over other wireless technologies. The short answer is that 5G provides the reliability, security, and performance they need.

5G is expected to seamlessly replace, or integrate with, existing wired connections

Availability and reliability

5G is a more reliable alternative to other wireless communication technologies. In fact, three aspects make 5G so reliable that it is expected to seamlessly replace, or integrate with, existing wired connections:



5G networks often use a licensed radio spectrum reserved exclusively for the network owner. This means that the network is free of interference, which in turn enables further optimisation.



5G includes advanced real-time optimisation and reliability features allowing it to work exceptionally well even under adverse circumstances which could affect reception. For example, if wireless devices are moving around the factory floor, a 5G radio tower can direct and optimise its transmission to them based on their precise locations. In another example, two radio towers can coordinate with each other to increase reliability through redundant data transmissions.



5G is 'time-aware'. This means that radio transmissions in 5G can be done in such a way that latency is not only low, but also can be determined in advance.

Together, these properties make 5G uniquely suited for smart factories requiring highly reliable, low-latency, and predictable connectivity as they allow control engineers to leverage 5G connectivity for time-critical operational tasks such as remote monitoring and steering.

Flexibility and control

5G networks can adapt to targeted use cases. Factory owners can select the feature set and configuration that they need. Whether that means optimising for maximum bandwidth, low latency, or the battery lifetime of devices, 5G is flexible enough to excel at a wide range of applications. This makes it suitable not only for connecting the factory floor, but also for replacing other wireless technologies used across IT and OT environments.

Confidentiality and integrity

The 5G technical specifications come with many proven security features out of the box. This makes 5G suitable for applications handling sensitive data or requiring high availability. Important security enhancements compared with earlier cellular network generations include improvements to authentication, subscriber privacy, and air interface protection. Perhaps more importantly, the flexibility of 5G extends to key security features such as authentication and encryption, as deployments can be set to use configurable security protocols commonly used in complex IT environments. In essence, 5G is designed to be both future-proof and customisable without compromising on security.

However, factory owners adopting 5G should realise that neither fitness nor features come preconfigured. Critical industrial applications require a comprehensive set of security controls to protect the communications between the machines or devices and the network. Such a holistic security framework goes beyond what is written in the 5G technical specifications. This is particularly true for factory owners considering deploying their own private 5G network to optimise operations and enable smart factory use cases. These factory owners should clarify their requirements in terms of security, performance and investment, and match those with a suitable 5G deployment option.

5G is designed to be both future-proof and customisable without compromising on security

Types of private 5G networks


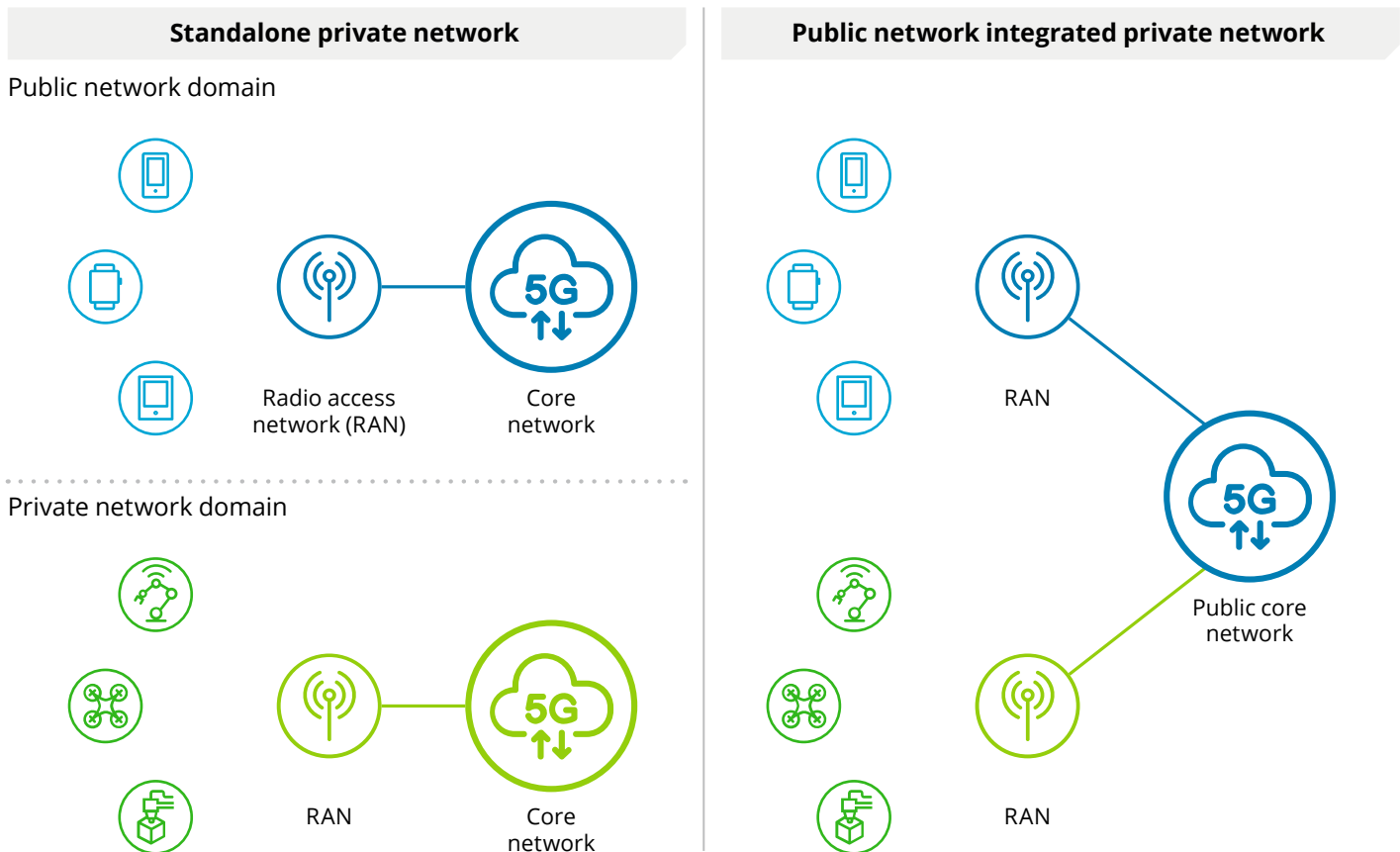
 **Public mobile networks are what enable your everyday mobile communications. They are usually operated by a service provider that also manages your subscription. In contrast, 'private 5G' refers to a 5G mobile network for a specific group of users or devices. These private networks are further divided in two fundamental types: 1) standalone private networks; and 2) public network integrated private networks.**

Figure 1: Standalone versus integrated private networks



The difference between the two is that *standalone private networks* are completely decoupled from any infrastructure of public telecommunications service providers. As such, they implement the entire technology stack. This includes the radio access network (RAN) made up of radio transceiver stations, and the core network, which controls the radio access and implements other functions necessary for mobile connectivity. *Public network integrated private networks* are provisioned using infrastructure of a public network. Such

networks can be considered to 'piggyback' on an existing public telecommunications network. What both types have in common is that any 5G network can be tuned to certain use cases, requiring fast data rates, low latency, or high reliability.

The world of private 5G networks, however, is not black and white. Between the standalone and integrated private network types exists a whole range of deployment options, which we will explore further.



Selecting a type of private 5G network



Factory owners will have to choose between a standalone, integrated, or hybrid network deployment. To select an appropriate design, factory owners will need to weigh key parameters such as security, functionality, and costs. For example, a standalone network can be fully adjusted to the factory's needs, but may not meet all requirements or could be too costly. Here, we explore these three parameters and their implications.

Security: Risk exposure and degree of network control

The most profound difference between standalone and integrated 5G networks in terms of security is in who controls the subscription. If a standalone network is deployed in a factory, the factory owner controls the entire technology infrastructure and services. As such, the factory owner has full control over who can access the network and how. Instead of using the well-known SIM card, it is possible for factory owners to choose a different authentication method. For example, a factory owner could choose to authenticate devices using digital certificates or even usernames and passwords. They may choose to do so as it could make

the onboarding of new devices easier or they may already have existing infrastructure for managing credentials. The downside is that it requires securely storing those certificates or passwords in the device.

Conversely, public network integrated deployments will always rely on a subscription with a public mobile network operator. This means that the credentials provided by these companies have to be used and also that there has to be a secure element within the device. Hence, devices will use either a physical SIM card or an embedded SIM in most scenarios.

Glossary

- **Radio Access Network (RAN):** Mobile network domain responsible for radio communication with wireless devices and data transmission with the core network.
- **Core network:** Centralised network and set of functions responsible for managing the radio access network and provisioning other network services, e.g., authentication, session management, and communication with external data networks.
- **Control Plane:** Network traffic controlling the interaction between the 5G network elements including wireless devices, radio equipment, and network functions in the core network.
- **Latency:** The time it takes for network traffic to reach its destination. Also referred to as delay.
- **Network slice:** A way to create a logically isolated 'virtual network' on top of a shared 5G network infrastructure.
- **User Plane:** Network traffic corresponding to the user-level data sent between devices or applications.
- **User Plane Function (UPF):** Network function in the 5G core network that carries and routes user plane traffic between wireless devices and external data networks, such as the internet.
- **Extensible Authentication Protocol (EAP):** Generic authentication framework supporting a variety of protocols, often used for network access authentication.
- **3rd Generation Partnership Project (3GPP):** Industry body creating technical specifications for cellular mobile communication systems.

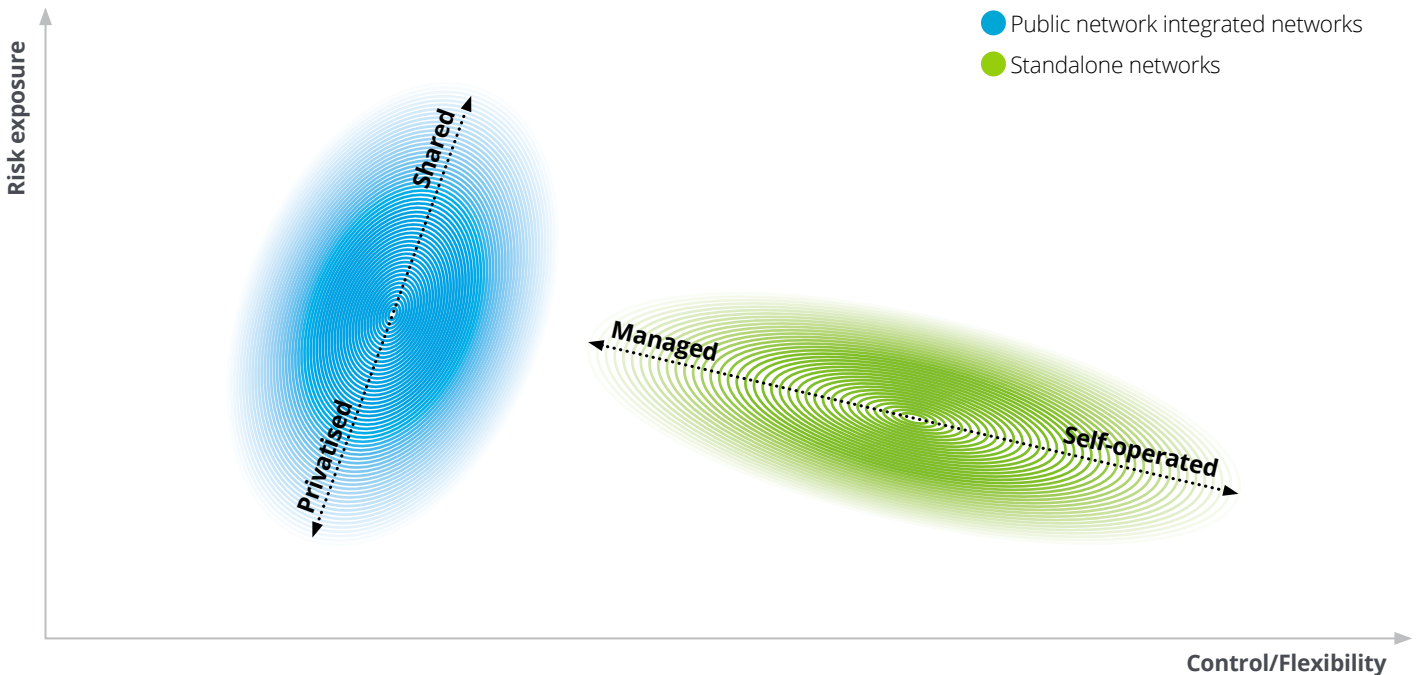
Another area in which standalone networks offer more flexibility and control is the choice of security algorithms. This includes the control over the authentication algorithm for granting network access and deriving security keys. In 5G, this is enabled by the Extensible Authentication Protocol (EAP), an authentication framework commonly used in enterprise environments. This means that factory deployments can reuse existing authentication servers as long as these servers support EAP. By using such a server, devices that support EAP (and 5G) can connect to a private 5G network using their factory credentials. Furthermore, algorithms used for protecting confidentiality and integrity of data sent over the air are also configurable. Private network operators can choose between different options specified in the 5G standard, or in some cases even specify their own algorithms.

Lastly, security risk exposure needs to be considered. Both private and public 5G networks are exposed to varying

degrees of risk. Public network providers might have larger, specifically trained security teams and may be able to respond faster to security incidents. However, the use of shared infrastructure and services naturally comes with an increased level of exposure. For example, the public network provider's centralised systems and services may be attacked, which could potentially also impact the private network. Due to their application in very specific scenarios and fewer interactions with third parties and their infrastructure, private 5G deployments are likely to offer a smaller attack surface. Furthermore, many security issues targeting legacy technology can be completely ruled out if these technologies are not present at all, for example Short Message Service (SMS).

Figure 2 depicts the relation between risk exposure and the degree of control generally associated to integrated and standalone deployment options.

Figure 2: Relation between risk exposure and control in different deployment options



Shared deployment: Most of the 5G infrastructure and functions are managed by the public network operator and shared with other customers. Logical isolation is used to provide a private network to the customer.

Privatised deployment: Some of the 5G infrastructure and functions, such as the RAN, are dedicated to the customer.

Managed deployment: Operation of the private 5G network infrastructure and functions is outsourced to a specialised provider.

Self-operated deployment: The private 5G network is operated by the customer itself.

Functionality: Service diversity and operational complexity

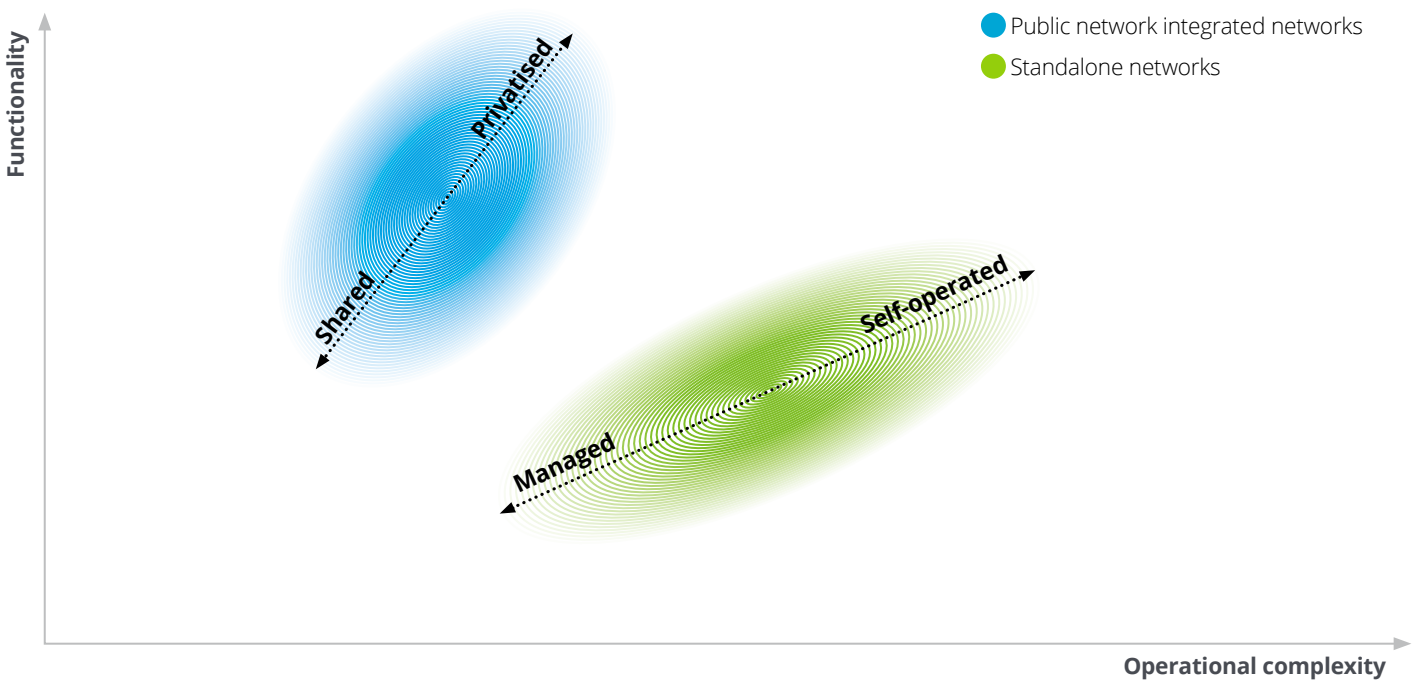
Factory owners deploying their own private network should keep additional considerations in mind. Certain functions are simply not available or are much more difficult to provide in a standalone, private environment.

Firstly, the integration with other mobile services beyond data, such as SMS or voice telephony, is only possible to a limited extent in private deployments. Without connection to a public network, such services are only available amongst users and devices of the private network. The complexity associated with deploying telephony and SMS services will mean that only very few private networks will provide these services. Anything beyond data transfer will therefore be a niche application when it comes to standalone private 5G networks.

Secondly, if connectivity is required beyond the boundary of a localised, private 5G deployment (e.g., a factory site), the standalone option is not ideal either. If devices leave the local private 5G network, they would need to connect (or 'roam') to a public network. To enable roaming into public networks, an inter-connection with a public network is a fundamental prerequisite. That would also mean being compatible with public network operator rules which would impose limitations on choices that factory owners can make. Examples would include agreeing with the public network operator on the charges for the usage of the public network, as well as having to use SIM cards issued by a public network operator.

Figure 3 illustrates the relation between functionality and operational complexity in the different deployment options described.

Figure 3: Relation between functionality and operational complexity in different deployment options



Shared deployment: Most of the 5G infrastructure and functions are managed by the public network operator and shared with other customers. Logical isolation is used to provide a private network to the customer.

Privatised deployment: Some of the 5G infrastructure and functions, such as the RAN, are dedicated to the customer.

Managed deployment: Operation of the private 5G network infrastructure and functions is outsourced to a specialised provider.

Self-operated deployment: The private 5G network is operated by the customer itself.

Cost aspect: Upfront investment and operational costs

Factory owners will also have to consider the costs of building and operating a private 5G network. Deployment of a private network, whether standalone or integrated, usually involves a significant upfront investment and substantial operational costs. Key requirements for private 5G networks include:

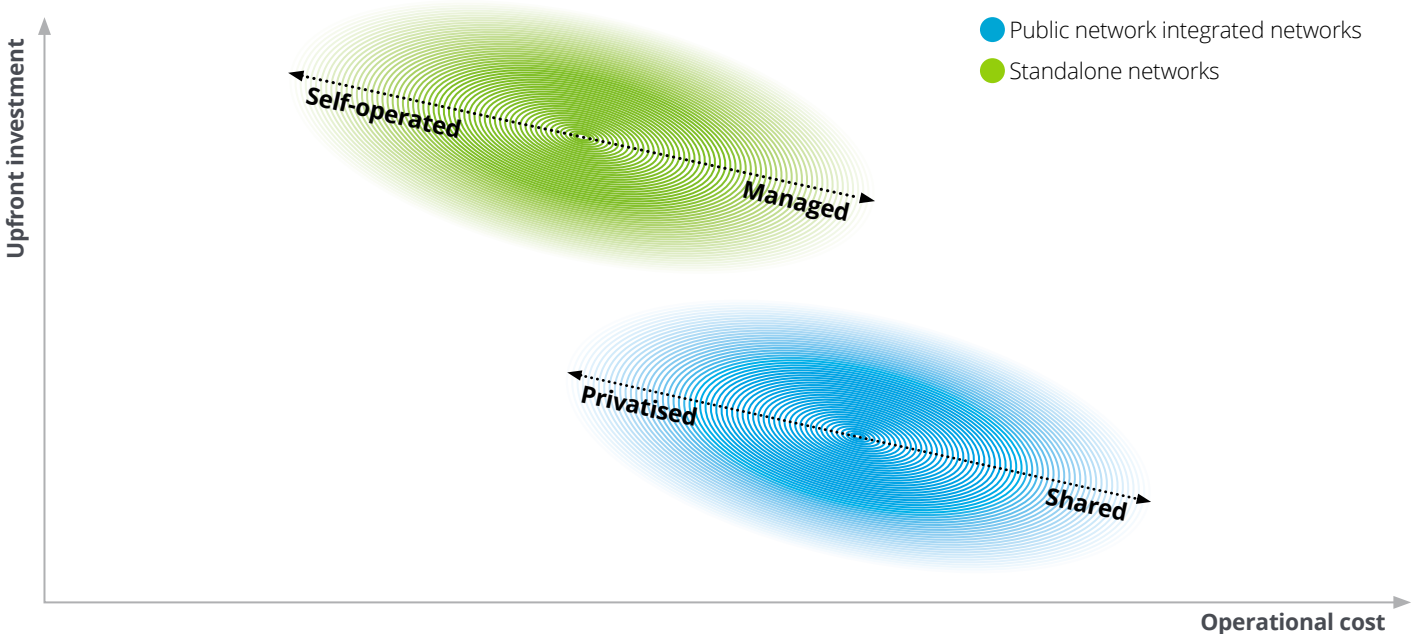
- Spectrum:** Wireless communication relies on certain bands in the radio frequency spectrum to transmit information. 5G can be operated in both unlicensed and licensed radio frequencies. For the best reliability, a licensed spectrum should be used as it is dedicated to the licensor and therefore interference free. Depending on the jurisdiction, licenses may be granted in a tender process requiring a lot of effort for participation. For factory owners this means that if they want to use a licensed spectrum, their options and costs also depend on the jurisdiction. Factory owners could participate in a tender, apply for a spectrum separately, or lease a spectrum from a public mobile network operator and, depending on the jurisdiction, this might come with a considerable upfront cost.
- Technology:** 5G networks are composed of many individual network functions, each catering to a specific part of the communication service. Setting up this entire

ecosystem independently not only requires a significant upfront investment, but also continuous operations and management effort. Factory owners have options at their disposal. If they would like to reduce their upfront cost, leasing equipment is one such option. They should further consider to what extent network sharing is acceptable for their use case. The degree to which the network utilises dedicated or shared infrastructure (e.g., RAN, core network, cloud) influences the upfront cost significantly.

- Skills:** Deploying, operating, and protecting 5G networks requires deep experience and knowledge in information and communication technologies and cyber security—a diverse set of capabilities that only a few organisations will find internally. Factory owners could consider outsourcing the skills to cloud providers, public mobile network operators, or system integrators. Already today, there are commercial private 5G offerings geared specifically towards factory owners that lower the barrier to entry significantly by outsourcing network operations and management.

Figure 4 depicts the relation between upfront investment and operational costs that are typically associated with different deployment options.

Figure 4: Relation between upfront investment and operational costs in different deployment options



Shared deployment: Most of the 5G infrastructure and functions are managed by the public network operator and shared with other customers. Logical isolation is used to provide a private network to the customer.

Privatised deployment: Some of the 5G infrastructure and functions, such as the RAN, are dedicated to the customer.

Managed deployment: Operation of the private 5G network infrastructure and functions is outsourced to a specialised provider.

Self-operated deployment: The private 5G network is operated by the customer itself.



Private 5G deployment options



Technological complexity and adaptability can make it seem daunting to get started with 5G connectivity. To simplify this process, we take a closer look at three concrete deployments options, selected to highlight very different 5G capabilities. We focus specifically on how design decisions affect security in these examples.

Deployment option 1: Optimised for availability and reliability

If availability is of utmost concern, private 5G networks can be optimised for reliable connectivity and data transmission. In the context of connected manufacturing, this may be especially important in factories where industrial equipment moves around the factory floor.

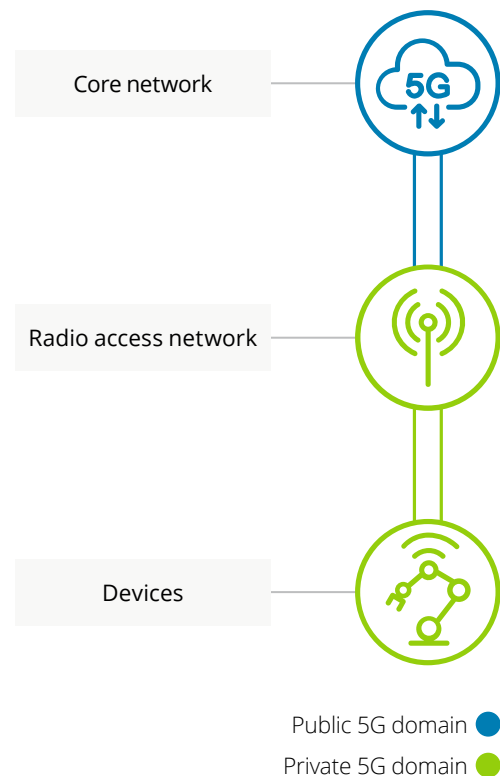
Figure 5 shows a possible deployment optimised for availability. In this integrated deployment scenario, the industrial site leverages a privately deployed radio access network (RAN) and the public core network of a telecom service provider. When using a third-party core network, the factory owner could request dedicated and isolated resources for increased availability. The telecom service provider can provision these resources, for example, by creating a private network slice for the factory network. Network slicing is a way of provisioning a virtual private network on top of shared 5G infrastructure to ensure a guaranteed service level and isolation from other network tenants. This approach can mitigate some of the availability risks associated with sharing the core network with other organisations.

Turning to the RAN itself, the 5G specifications allow for further availability and reliability optimisations. In this scenario we include redundant connections between the RAN and the public core network, and similarly between the RAN and industrial devices. From a technical perspective, the 5G specifications allow for redundant transmission of the device communication on different layers. Network operators may employ and combine any of the following options to ensure reliable data transmission:

- Set up parallel end-to-end sessions between the core network and the wireless device connected to multiple RAN nodes
- Establish separate logical or physical connections between the RAN and the core network
- Utilise core network redundancy for selected network function instances.

Which option factory owners should choose depends on the particular deployment, the available network infrastructure, and the offering of the telecom service provider. For example, enabling redundant logical connections will be much easier than deploying a physically separate connection between the RAN and the public core network. At the same time, logical connections do not provide the same degree of redundancy as two separate physical links and factory owners would need to weigh the pros and cons of each option before deciding.

Figure 5: Integrated deployment with private RAN and redundant data transmission



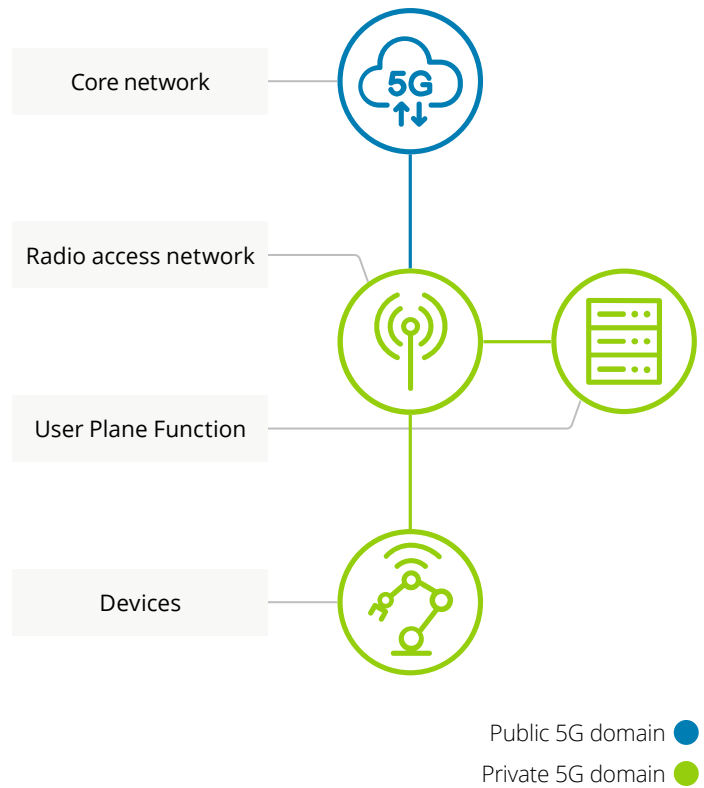
Deployment option 2: Optimised for confidentiality and/or integrity

In addition to availability, it is fair to assume data confidentiality and integrity will be among the motivating factors for some factory owners to consider private 5G deployments. These requirements are particularly essential for industrial use cases that involve the transmission of highly sensitive information over the 5G network, such as intellectual property related to the manufactured goods or the production process.

To ensure confidentiality most cost-effectively, factory owners could consider a public network integrated deployment with local processing of User Plane data, as visualised in Figure 6. In this example, the factory owner deploys and maintains the RAN elements as well as a local User Plane Function (UPF). The UPF is the network function forwarding User Plane traffic between the RAN and other data networks, for example, a private cloud deployment hosting applications for the factory automation. By operating this element locally, one can ensure that data sent to and from the UPF does not leave the premises and is adequately protected.

Despite the locally processed User Plane data, there is still management traffic between the devices and radio network on the one side and the core network on the other side. This traffic is required to manage the radio access network and to manage the device traffic. Of course, factory owners should take care not to expose that traffic to any third parties. Dedicated RAN elements managed by the private network operator have the benefit that the factory owner can ensure that data transferred over the link between the RAN and core network is protected in transit.

Figure 6: Integrated deployment with local User Plane processing

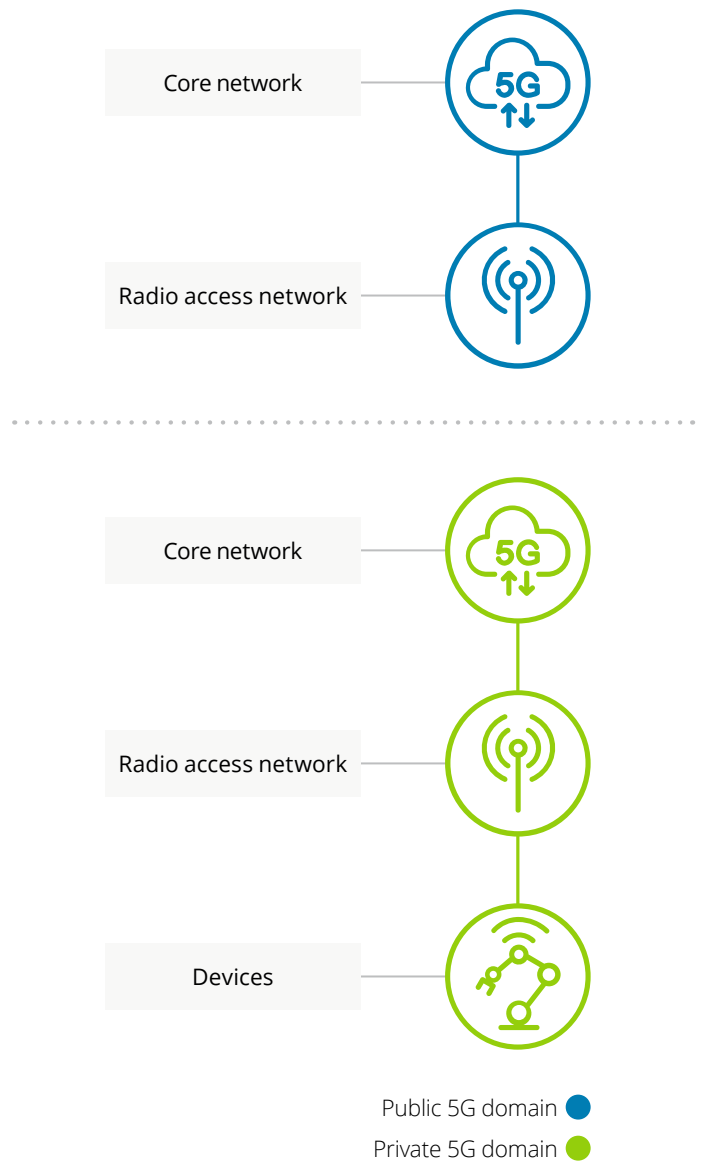


Deployment option 3: Optimised for control and flexibility

If the goal is maximum control and flexibility, and the required investment is of secondary concern, factory owners could consider a standalone private network as depicted in Figure 7. Considering the associated upfront and operating costs, this option will likely be most relevant for large-scale deployments serving many devices. Without any interaction with public mobile networks—and therefore the greatest level of independence from telecom service providers—this deployment option differs significantly from the previous options.

Opting for a standalone mobile network does not necessarily require implementing or maintaining the entire end-to-end technology stack. For example, one can imagine a scenario in which the spectrum and RAN equipment are leased from a telecom service provider, whereas 5G core network components are deployed in a local data centre or in the cloud. While such a model poses a lower barrier of entry, it also counteracts some of the benefits a standalone network promises. For those factory owners looking to achieve maximum control, data security, and minimal external dependencies, a fully self-managed deployment will likely be the way to go.

Figure 7: Standalone deployment





Conclusion



The first step towards any Industry 4.0 use case is defining concrete requirements. Once the connectivity expectations are clear, the selection of a suitable deployment option and feature set become significantly easier. In this paper, we only highlight some of the many options available in the 5G specifications.

5G has reached a level of maturity that ensures a solid foundation for industrial use cases. Technical specifications offer a wide variety of features catering to these applications. Public mobile network operators and other service providers have also gained first experiences with this type of 5G deployment. Moreover, the 3rd Generation Partnership Project (3GPP), which defines the 5G technical specifications, is continually working towards further enhancements. Even though the specification may be ready, the majority of factory owners are just starting. Naturally, this carries a lot of uncertainty, but also opportunity for businesses in these sectors.

The nature of factory applications means that factory owners should consider security and safety aspects from day one. Identifying security risks, requirements, and a suitable deployment model are the first steps towards building a secure private 5G communication network.

Factory owners should start thinking about their strategic direction towards future connectivity and automation

Current market trends suggest that for the majority of industry sectors, the path towards private 5G is most feasible when partnering with a telecom service provider. In fact, in November 2021 the Global mobile Suppliers Association (GSA) identified more than 70 public mobile network operators supporting private networks to some extent¹. The relatively low entry barrier of integrated deployments should make this model particularly interesting for factory owners. That said, telecom service providers need to develop 5G offerings that can adapt to a diverse range of requirements to truly deliver on the promised flexibility.

While standardisation bodies continue to expand and enhance the 5G feature set², the technical specifications will only ever be a foundation. Telecom service providers and industry sectors will need to jointly make it a reality. Depending on the required security, performance, flexibility, and economics, this implementation can look vastly different for different organisations.

1. Global mobile Suppliers Association (GSA), "[Private Mobile Networks Summary – November 2021](#)," accessed June 15, 2022.

2. 3rd Generation Partnership Project (3GPP), "[Release 18](#)," accessed June 15, 2022.

Authors and contributors

Authors

Sander de Kievit

Senior manager

+81 80 4299 0554

sander.dekievit@tohatsu.co.jp

Hans Christian Rudolph

Senior consultant

+81 70 3330 5469

hanschristian.rudolph@tohatsu.co.jp

Key Contributors

Dr. Anand R. Prasad

Partner

+81 80 3718 1454

anandraghawa.prasad@tohatsu.co.jp

Etienne Janot

Senior manager

+886 2 2725 9988 (ext. 7766)

etjanot@deloitte.com.tw

Key contacts

Max Lin
Asia Pacific Cyber Emerging Technologies leader
+886 2 2725 9988 (ext. 7779)
maxylin@deloitte.com.tw

Dr. Anand R. Prasad
Asia Pacific Cyber Technology, Media & Telecommunications leader
+81 80 3718 1454
anandraghawa.prasad@tohmatsumatsu.co.jp

Australia

David R. Owen
Partner
+61 2 8260 4596
downen@deloitte.com.au

Korea

Young Soo Seo
Partner
+82 2 6676 1929
youngseo@deloitte.com

Southeast Asia

Gerry Chng
Partner
+65 6800 3875
gchng@deloitte.com

Chinese Mainland/Hong Kong

Boris Zhang
Partner
+86 21 6141 1505
zhzhang@deloitte.com.cn

New Zealand

Anu Nayar
Partner
+64 4 470 3785
anayar@deloitte.co.nz

Taiwan

Max Lin
Partner
+886 2 2725 9988 (ext. 7779)
maxylin@deloitte.com.tw

Japan

Haruhito Kitano
Partner
+81 80 3591 6426
haruhito.kitano@tohmatsumatsu.co.jp

South Asia

Gaurav Shukla
Partner
+91 80 6188 6164
shuklagaurav@deloitte.com



Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which are separate and independent legal entities, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms or their related entities (collectively, the “Deloitte organization”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.