NOKIA

Airport private wireless solutions

The essential wireless foundation for the digital airport

White paper

The adoption of Industry 4.0 digital technologies, such as IoT, AI, machine learning and data analytics are expected to revolutionize the operations of airports, introducing greater automation, improved processes, better tracking and handling of everything from aircraft to baggage — all with the goal of improving the passenger experience. Essential to this digital transformation will be high performing, secure and very reliable wireless communications. Neither the Wi-Fi networks currently in operation in most airports nor the public mobile networks that serve them have what is required to support the most ambitious digital transformation of the airport.

In this paper, we examine the goals of this transformation, the key requirements that will have to be met, and the strengths and weaknesses of the various wireless technologies available today — keeping in mind what is coming in the future, as well. We argue that airports have to think in terms of a purpose-built private wireless network to support their operations. This is a different approach then they have used previously, and it affords them an opportunity to step up to a new generation of private network technologies: 4.9G/LTE today and 5G tomorrow. We examine these technologies more closely and discuss in detail what airports need to consider as they embrace their digital future.

NOKIA

Contents

Introduction

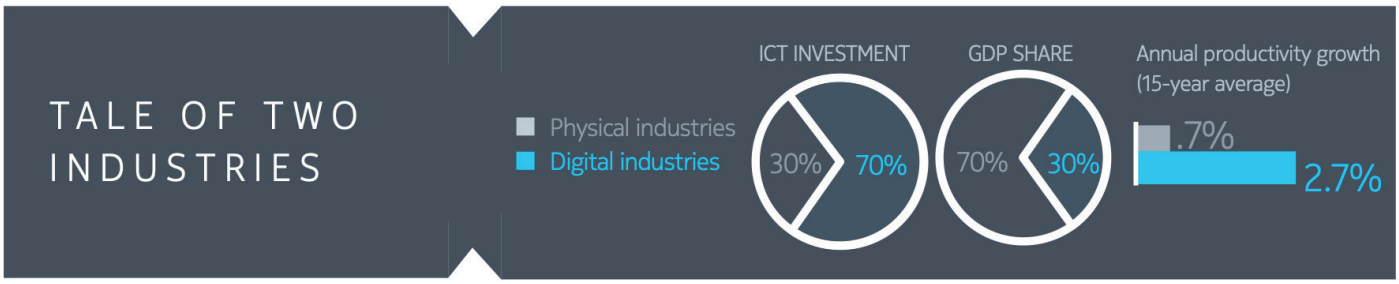
Global industry, including the Aviation Transport Industry (ATI), is driven by a constant quest for productivity and efficiency. These industries pursue all means to most efficiently produce and deliver their goods and services. Growth in productivity and efficiency is among the leading indicators of economic value and a strong measure of progress in the industrial age.

Yet, in the last few decades, global productivity and efficiency growth has slowed dramatically. That is surprising to many, given the unprecedented advancements in information and communications technology (ICT). After all, we have witnessed massive innovation in the internet era, and the digital transformation of enterprises, including airports, is well underway.

A closer look at US economic data reveals that it is just 30 percent of industries that are benefiting most from digitalization and automation[1]. Information economy segments and IT-centric verticals such as financial services have made the lion's share — 70 percent — of total investment in ICT. As a result, they are benefitting from a nearly 4x faster productivity growth rate.

In contrast, traditional asset-intensive industries have lagged in the transition to the digital economy and thus have not yielded their share of benefits from the transformation. Even as the companies in this "physical economy" collectively represent 70 percent of US GDP and employ three-quarters of the US workforce, these industries have experienced a productivity rut over the past two decades.

Figure 1. A tale of two industries



This pattern has begun to shift. Industries in the "physical economy" such as the ATI have begun their digital transformation. The opportunity for realizing a much bigger productivity and efficiency boom is before us. As the Internet of Things (IoT), edge computing, cloud, deep analytics based on artificial intelligence/machine learning (AI/ML), biometric scanning, augmented reality (AR), remote control and digital twinning technologies mature and reach a critical mass of adoption, the opportunities to energize traditional industries are countless and within reach.

Technologies that can bring the physical and digital economies together will drive commercial and social value like never before. Augmented intelligence and automation will drive productivity and efficiency while dramatically reducing risks.

Today we stand at the cusp of the next major industrial revolution, Industry 4.0, which promises to unlock trillions of dollars of economic value in the next decade[2] by driving massive improvements in productivity in physical and digital industries alike, enhancing quality of life in safer, healthier and more sustainable communities.

1 Michael Mandel, Brett Swanson, The coming productivity boom, The Technology CEO Council.
2 Source: McKinsey - The Internet of Things: Mapping the value beyond the hype June 2015 ($3.8-$11T of economic value by 2025)

For quite some time, connectivity has been treated as a commodity. This has hindered the ability of the OT world to connect in a secure and reliable way to the IT world, despite the pivotal role connectivity or high-performance networking plays in achieving the vision of Industry 4.0.

As airports digitally evolve towards more efficient and aware operations, an increasing number of airport applications will rely on wireless connectivity for critical voice, broadband data, video and IoT. Operational efficiency is about better and faster decision making, which will require unified communications between stakeholders and the elimination of communication silos at the airport.

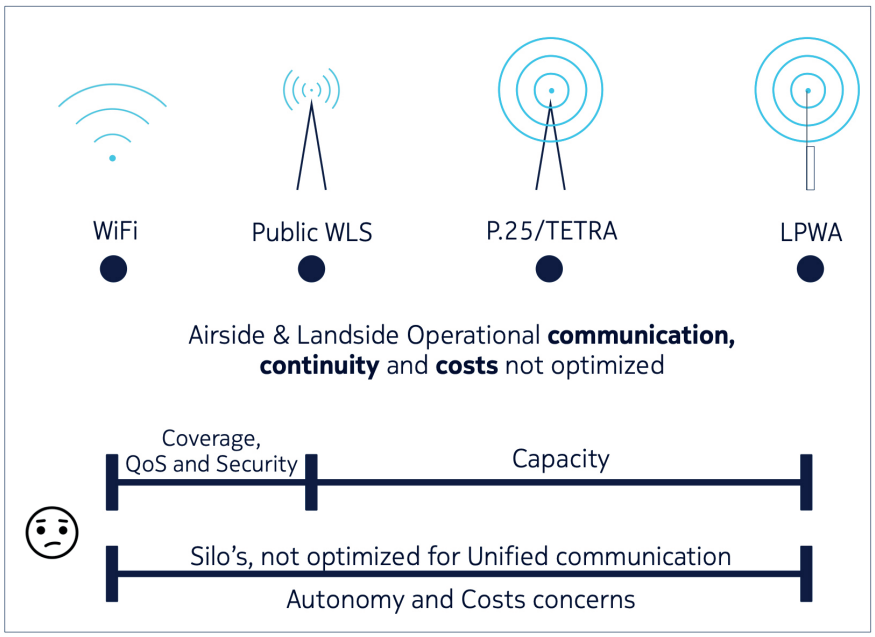
This whitepaper describes strategy considerations for airports around wireless connectivity, with a prime focus on wireless services for operations to all airport stakeholders. The wireless strategy will become the foundation for the digital airport to enhance operational efficiencies, better decision making and operational awareness.

Need for a change

Most airport operators today have implemented a wireless network infrastructure that is shared between passengers and operations, using a combination of Wi-Fi and public cellular connectivity. The latter is provided by one or more mobile service providers to deliver a broad mix of landside and airside services and applications. In addition, airports typically have a separate, dedicated PMR/LMR radio network for mission-critical services, predominately carrying voice communications.

While this kind of shared network environment has performed well in the past, airports are facing increased concerns over this strategy. With the digitization of many airport processes, an increasing number of services will rely on the wireless platform. As a result, there are a number of key considerations driving airports to consider new network strategies. These include greater reliability and autonomy, reduced costs and unified communication across stakeholders and domains.

Figure 2. Concerns over existing airport wireless solutions



NOKIA

The shared Wi-Fi/public wireless networks in use today are susceptible to traffic congestion and poor signal strength (resulting in non-predictable performance). They are unable to prioritize bandwidth for critical applications because Wi-Fi does not support proper QoS management. And they cannot scale easily in a purpose-built way to support future growth.

Capacity issues increasingly arise because passengers use the public wireless network for high bandwidth services such as video and gaming. Given the best effort nature of the public wireless network, this means that even a few passengers can consume the available bandwidth and degrade performance for all users, including operations. This is especially salient in the event of an incident, when capacity is not guaranteed for the staff who especially need it.

The individual components that make up the shared silo environment can be costly and time-intensive to maintain and some will soon be outdated, unable to meet changing operational requirements and unsuitable for today's bandwidth-hungry applications.

There are other wireless communications solutions intended for aviation use. For instance, Aeromacs, which is based on 802.16e WiMAX technology, is in the process of being validated by the International Civil Aviation Organization (ICAO) and Eurocontrol for surface communications and ground-to-aircraft communication in the domain of air traffic management (ATM). Aeromacs can be relevant to aviation but is targeted at a very specific use case. The ecosystem behind Aeromacs is clearly limited and could jeopardize airport total cost of ownership (TCO) targets. It is also not well-suited to providing a uniform private wireless platform connecting people and things for the digital airport. Fortunately, there is also a trend in ATM modernization programs to adopt 3GPP-based technologies for ground-to-aircraft communications that avoid the limitations of Aeromacs.

Operational connectivity issues are not minor to the success of the airport. They directly impact the passenger experience by causing operational efficiencies that may delay flights and reduce passenger services. In the worst cases, poor connectivity may even lead to airlines reducing their presence at the airport.

The digital airport calls for a change in wireless strategy. Fundamentally, the airport has two distinct categories of users of wireless services:

1. **Passengers**
2. **Staff** (airport, ground handlers, security, first responders, airlines)

Passenger wireless services can continue to rely on best-effort networks, such as Wi-Fi and public wireless services.

Services for operations, in contrast, need to be secure, reliable and capable of being prioritized. This can only be achieved by a technology that is dedicated to the airport and operates in licensed spectrum, which would give the airport "private right to use". To enhance airport collaboration and communication efficiency, and optimize OPEX, the target technology should allow for multiservice support delivered in a secure and reliable way. Services should include voice, push to talk, data, video and IoT support.

With this private multiservice wireless platform, airports can offload their operational services from the mobile network operator's public service and airport Wi-Fi, migrating them to the private wireless environment. This will also enhance passenger connectivity experience at the airport because more capacity will be available to the passengers on the Wi-Fi and public cellular networks.

For airports investing in their digital airport strategy, their private wireless network becomes a strategic asset, a unique purpose-built network, which is as important in its own way as the airfield and runways. All digital applications rely on it for business- and mission-critical tasks. It is the key means to unify operational communications between all staff, partners and tenants at the airport. And, in the age of IoT devices and sensors, it is the essential fabric that connect all 'things'.

The private multiservice wireless platform is the essential foundation for the digital airport, addressing the following business considerations:

Airport Digital Transformation: The aviation industry increasingly relies on digitization of processes and assets with the goal of improved decision-making between stakeholders.

Investment Protection: Any investment in a new technology should demonstrate an evolution path to the next generation of technology.

Situational Awareness: Increased use of sensors placed on airside vehicles and cameras will improve awareness and consequently create efficiencies as well as improving security.

Autonomy: A private wireless network allows airport operators to reduce the dependency on third party wireless service providers — although deployment options exist which don't require them to become experts themselves.

Operational Continuity: Reliability is crucial for every airport. With a dedicated, purpose-built private wireless network for operations, airports can create a secure, reliable wireless infrastructure that will ensure predictable, continuous communications services.

The Solution

Technology

Selecting the right technology to build the wireless platform for the digital airport is essential. This platform will become the wireless foundation for the digital airport enabling enhanced operational efficiency, situational awareness and unified communications for all stakeholders with better decision-making all around.

Ten parameters, driven by airport use cases and requirements, are of key importance:

- **Reliability**
- **Security**
- **Scalability**
- **Multiservice**
- **Latency**
- **TCO[3]**
- **Migration path**
- **Predictable**
- **Throughput**
- **Coverage & Penetration**

3 Total Cost of Ownership

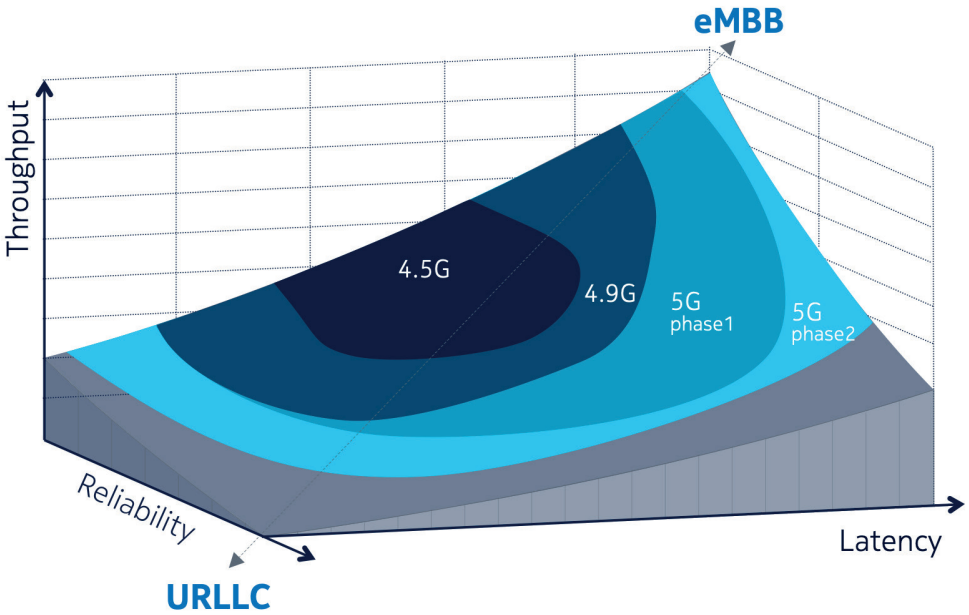
The fourth generation of mobile communication technology standardized by 3GPP (the mobile communications standards organization) is alternatively referred to as 4G, LTE or 4G/LTE (depending on the market). LTE addresses all of the above parameters in a way that best fits the airport critical communications environment. As discussed above, LTE is also deployed by mobile network operators in public networks, however, airport operations call for a private, purpose-built deployment (although there are private LTE deployment options that can be provided by public mobile operators, as well. Reference is made to section “Business models” of this whitepaper). A private deployment ensures a secure network that enables service prioritization. Typical for a private network is the deployment of an on-site wireless core, to ensure data that should stay at the airport will stay at the airport. Data that requires public cloud connectivity can be securely connected to such public cloud.

The 4G standards have now evolved to a higher capacity version, called 4.9G, that contains support for a.o. critical communications and higher throughputs. The next evolution is called 5G and introduces an improved set of characteristics — see figure 3. The figure specifically shows improvements in capacity & throughput (eMBB – enhanced Mobile BroadBand), latency and reliability (URLLC – Ultra Reliable Low Latency Connectivity). The initial rollouts of 5G will require 4G as an anchor technology and are focused on higher bandwidth wireless access services. This mode of operation is called “Non-StandAlone” or 5G NSA. For airports, the subsequent release of 5G of most interest is the “Standalone” version or 5G SA.

It is important to understand, keeping in mind investment protection, that there are migration paths available from existing 4.9G/LTE deployments to 5G deployments irrespective of the mode of operation.

5G is a technology that introduces the concept of service slicing, being able to fulfill each users’ service requirements with the right set of service parameters in a dynamic way. With many tenants on site, airports will benefit from this concept. However, it should be noted that, next to slicing, the concept of purpose build network is important to ensure coverage and capacity can be guaranteed in every zone at the airport. Nevertheless, 4.9G/LTE does address the majority of airport use cases in a reliable and secure way today.

Figure 3. Evolution of throughput, reliability and latency



Some use cases will call for a specific 5G deployment. One example is the telemetry offload of aircraft. Today, aircraft either offload their data to aircraft operational control (AOC) over a 3G/4G public wireless network or airport Wi-Fi (gatelink). 4.9G/LTE will be more than capable to continue doing this, however, as predictive maintenance for aircraft becomes more prevalent, the connected aircraft is expected to generate terabytes of data on route. Downloading this massive telemetry/IoT data will require much more throughput than the existing technologies can handle so as not to jeopardize the turnaround time of the aircraft: 5G will be able to address this challenge.

Latency is another important parameter for certain airport use cases. LTE has made significant advancements in reducing latency by introducing edge computing functionality for private networks. Private 4.9G/LTE performance can deliver round trip latency under 10ms for those applications that require it. Adopting edge computing architectures will result in a major improvement in latency compared to standard public wireless services.

Spectrum

A private multiservice wireless network requires licensed spectrum; it is one of the essential cornerstones for reliable and secure services. The value of licensed spectrum should not be underestimated in a world where most people are connected through (free) Wi-Fi using unlicensed spectrum. Licensed spectrum will provide the airport with a "private right to use" that ensures predictable and reliable services.

Today, there is widespread pressure on governments across the globe to free up spectrum for use by enterprises in industrial and other applications. In a number of markets spectrum is currently being allocated. This type of spectrum will be suitable for deploying 4G and 5G private networks.

There are several options for airports to gain access to spectrum for private networks. Below three spectrum models are discussed.

Direct access

One model for supplying spectrum to private enterprises is direct access to dedicated spectrum, as has been proposed in several countries. Examples include Germany, which is allowing enterprises to operate private networks in the 3.6–3.8 GHz band. In a similar vein, Sweden is considering allocating spectrum for local enterprise/industrial use in the 3.5 GHz band and the UK in the 3.8-4.2GHz band. Other examples of countries allowing direct access to spectrum are France, Japan and Finland. Airport operators are advised to check with their country telecom regulator on their latest position regarding spectrum availability as well as conditions and associated costs. Different from the traditional commercial spectrum used by mobile network operators, the costs associated with spectrum to enterprises is kept at a very low (administrative only) level[4].

Dynamic sharing

A second model involves making spectrum available in local areas on a dynamic 'shared' basis. The most well-known example of this is the US Citizens Broadband Radio Service (CBRS) model in the 3550-3700 MHz band, which allocates at least 80 MHz of spectrum to 'General Authorized Access' on a first-come, first-served basis and does not require a license. In addition, up to 70 MHz will be made available in 7 x 10 MHz swathes on a licensed basis for Priority Access Licenses (PAL) which require an auction. Similar to direct access, the costs associated with the use of dynamic sharing spectrum is kept at a significantly lower level compared to spectrum used for nationwide commercial usage by mobile network operators.

4 This statement reflects the situation in 2019, exceptions may apply going forward.

NOKIA

Sub-licensing

A third model involves sub-licensing mobile operator spectrum to enterprises for use in hyper-local network contexts. This model could apply for those airports that are not able to get access through direct or dynamic sharing.

The model allows for various sub-variants such as:

- Direct spectrum sub-licensing: the mobile network operator owns spectrum that is currently not in use
- Shared spectrum sub-licensing: the mobile network operator proposes to use spectrum that is in commercial use. Wireless and spectrum resources will be split into consumer best effort and prioritized enterprise use.

Mobile network operators are not forced to deploy such services nationwide; sub-licensing implementations might be limited to a campus environment.

Addressing the airport environment

The airport is a complex structure with many unique zones to cover. The technology chosen will have to be able to address it with solutions that fit the zone in a cost-efficient way. A couple of examples are:

Table 1. Airport zones

Airside		Terminal Side	
Zone	**Characteristic**	**Zone**	**Characteristic**
Apron / Stand	Dense, complex area, capacity and coverage driven	Passenger area	Complex indoor morphology – moderately open; potential to leverage existing asset such as DAS. Driven by coverage and need to extend capacity.
Remote Apron	Moderately open area, coverage driven	Baggage handling	Deep indoor with lots of metal. Coverage driven
Airfield / Taxiways / Runways	Wide (open) area, coverage driven	Offices, APOC	Lots of distinct rooms, coverage driven
Hangars, Cargo	Remote area with potential challenging morphology, capacity and coverage driven	Tunnels	Deep indoor, coverage driven

As can be seen from Table 1, the airport has various zones, each with their own characteristics. It requires various radio form factors to address these zones effectively, reference is made to Table 2. It is important to note that both 4G/LTE and 5G support high power radios that can cover wide areas such as an airfield in an effective, cost-efficient way. Technologies such as Wi-Fi, operating in license-free spectrum, are constrained by limited power, hence, airports would be challenged to cover such a wide area in a cost-efficient way; assuming it is even possible, from a practical point of view.

Table 2. Radio types

Type	Comment
Small Cell Indoor	Terminal Side • (Deep) indoor coverage wherever access to DAS is not feasible • Indoor coverage wherever there is a need for additional capacity (augmenting the DAS network)
Mini Macro	Airside • Targeting those zones that are difficult to cover by macro or micro radio • Targeting hot spot zones requesting high capacity and challenging environment (e.g. Stand)
Micro RRH	Airside • Wide area coverage to remote APRON
Macro RRH	Airside / Terminal side • Wide area coverage for full airfield coverage • Driver for DAS network

Examples of radio form factors

Small Cell Indoor
~3.5L[5]

Mini Macro
~9L

Micro RRH
~4L

5 Indicative figure, actual physical dimensions can differ, depending on model, frequency, etc.

Private wireless architecture

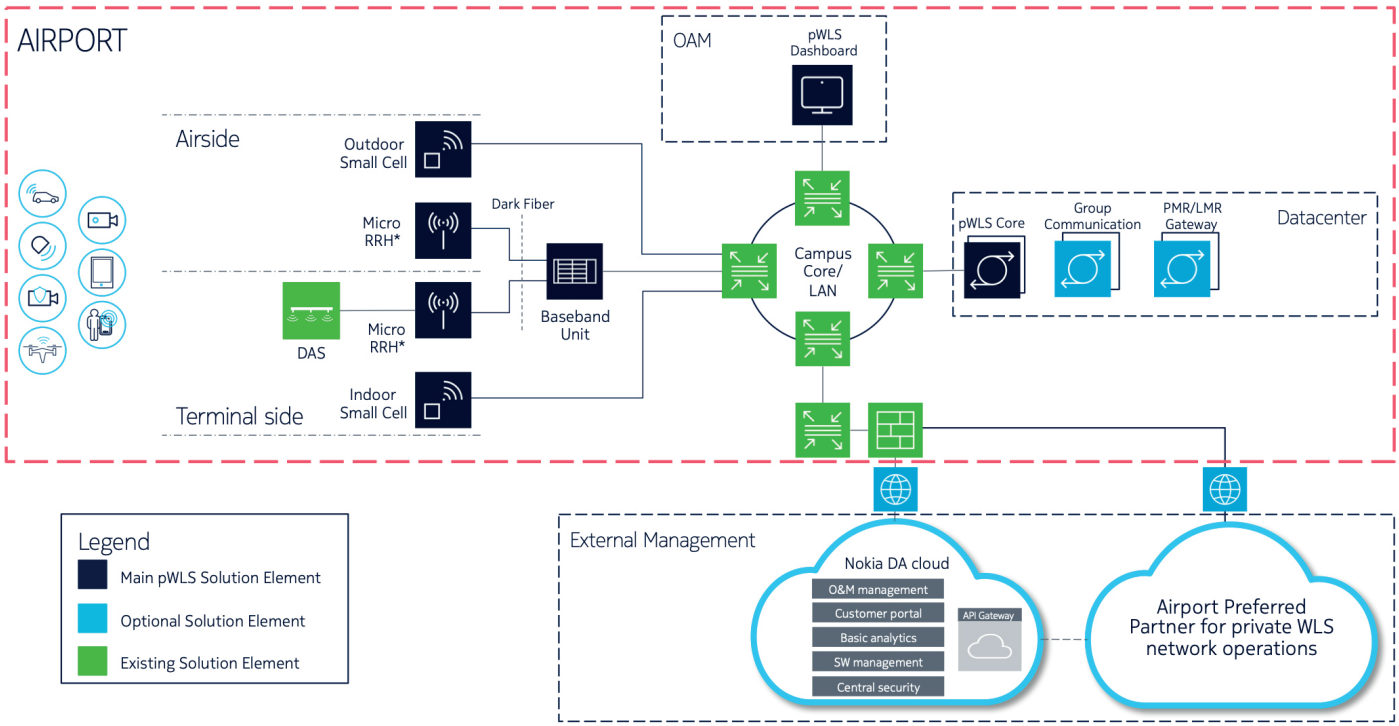
A high-level architecture of a private wireless network is shown in figure 4. The main components of the architecture are the private wireless core and the connected radio's in various form factors as explained in the previous section. Depending on the actual situation of the airport, terminal indoor coverage may be realized by using an existing airport asset, the distributed antenna system (DAS).

Operations of the network and implementing services is possible using either a full operations, administration, maintenance (OAM) system or a simplified dashboard to configure the most relevant service characteristics and monitor them. In the case of a dashboard, the complexity of a full OAM system would be assumed by an external management entity, such as the Nokia Secure Digital Automation Cloud or an airport-preferred partner. Such an entity would take care of the private wireless network lifecycle, including software upgrades among other tasks. It is important to note that in the case of external management, the private wireless network would still operate in isolation and would not be dependent on the link to the external operations. In other words, the private wireless core will be located at the airport data center, keeping all operational traffic local, thus private and secure.

Other important optional elements are:

- Group communications application – to allow for Push to Talk and Push to Video services
- PMR/LMR gateway – to realize connectivity between existing TETRA/P.25 networks and the private wireless network.

Figure 4. Private wireless architecture



NOKIA

Wireless service characteristics

Critical communications

Today, there are two separate technology families for critical mobile communications:

- 3GPP-based (2G, 3G, 4G, 5G and beyond) for commercial cellular networks that serve consumers and businesses
- Dedicated LMR, including P25 and TETRA, for public safety organizations as well as mission-critical services at airports (first responders, security, airline, ATC, etc.)

With the phenomenal market acceptance of next-generation LTE mobile services, the public has been enjoying enhanced multimedia capabilities and instant access to a plethora of information on the Internet, enabled by high–bandwidth LTE data services and innovative personal devices and applications that are not available to LMR/PMR users. Recognizing that the real-time sharing of multimedia information and instant access to databases can enable public safety users to more quickly respond and provide critical support, major public safety associations such as TCCA have endorsed[6] 3GPP-based technologies such as LTE or 5G as the successor technology of existing LMR/PMR systems.

Transportation is the second largest industry using PMR/LMR and aviation is a significant and large share of the transportation domain. Given its need for more advanced critical communication services, we believe this segment is a key driver for a 3GPP-based critical communication ecosystem.

3GPP has taken on the challenge, starting from release 11.3GPP. Release 13 LTE further incorporates mission-critical push-to-talk (MCPTT) and E-UTRAN isolated operation to strengthen resiliency, as well as additional proximity services enhancements.

Among other additions, 3GPP's Release 14 has defined specifications addressing enhancements to MCPTT, new features for MCData (Mission-Critical Data) and MCVideo (Mission-Critical Video), and a common framework which facilities standardizing additional MC (Mission-Critical) services.

Release 15, which represents the first release of the 5G system, further enhances mission-critical services with new functionalities and support for interoperability with existing PMR/LMR systems[7], among other additions. Release 15 also introduces the 5G NSA, discussed earlier. Other common functional enhancements for mission-critical services covered in Release 15 include enhanced MCPTT group call setup procedure with MBMS bearer and enhanced location management, information and triggers.

Examples of Public Safety references using LTE for their mission-critical services are Nordic Telecom in Czech Republic and Needa in UAE.

Service Availability

The foundation for service availability is good network coverage and well-planned load control and prioritization. Additionally, the network and services must be resilient to various failures and outages to support critical communication services: for example, extended power backup systems at wireless sites and radio duplication.

6 Both the Association of Public-Safety Communications (APCO) and the TETRA and Critical Communications Association (TCCA) have endorsed LTE as a standard for emergency communications broadband network.

7 For more detailed information, reference is made to ETSI's technical report "TETRA and Critical Communications Evolution (TCCE); Interworking between TETRA and 3GPP mission critical services"

Centralized wireless core sites at the airport can be designed with geo-redundancy support. Resilient transport networks (airport campus core/LAN) between wireless nodes are based on IP/MPLS supporting fast re-routing techniques.

Wireless nodes can be connected to both centralized core nodes in a geo-redundant setup for redundancy purposes as well as load balancing. In LTE this is enabled via the so-called S1 Flex feature.

TETRA networks are generally deployed with a focus on high reliability, and they have support for features such as local trunking (similar to IOPS[8] for 3GPP-based technologies). In table 4 several relevant resiliency features are compared between TETRA and 3GPP-based private wireless.

Table 3. Resilience capabilities of TETRA and 3GPP private wireless

	TETRA	Private Wireless
Core network disaster	Geo-redundant core sites	Geo-redundant core sites, database synchronization
Network element failure	HW and SW redundancy	HW and SW redundancy, S1 flex and pooling, automatic cloud resiliency
Transport failure	Resilient IP/MPLS	Resilient IP/MPLS
Backhaul failure fallback	Local trunking	Rel-13 IOPS
Coverage loss fallback	Direct mode operation	Rel-12/13 Direct communication

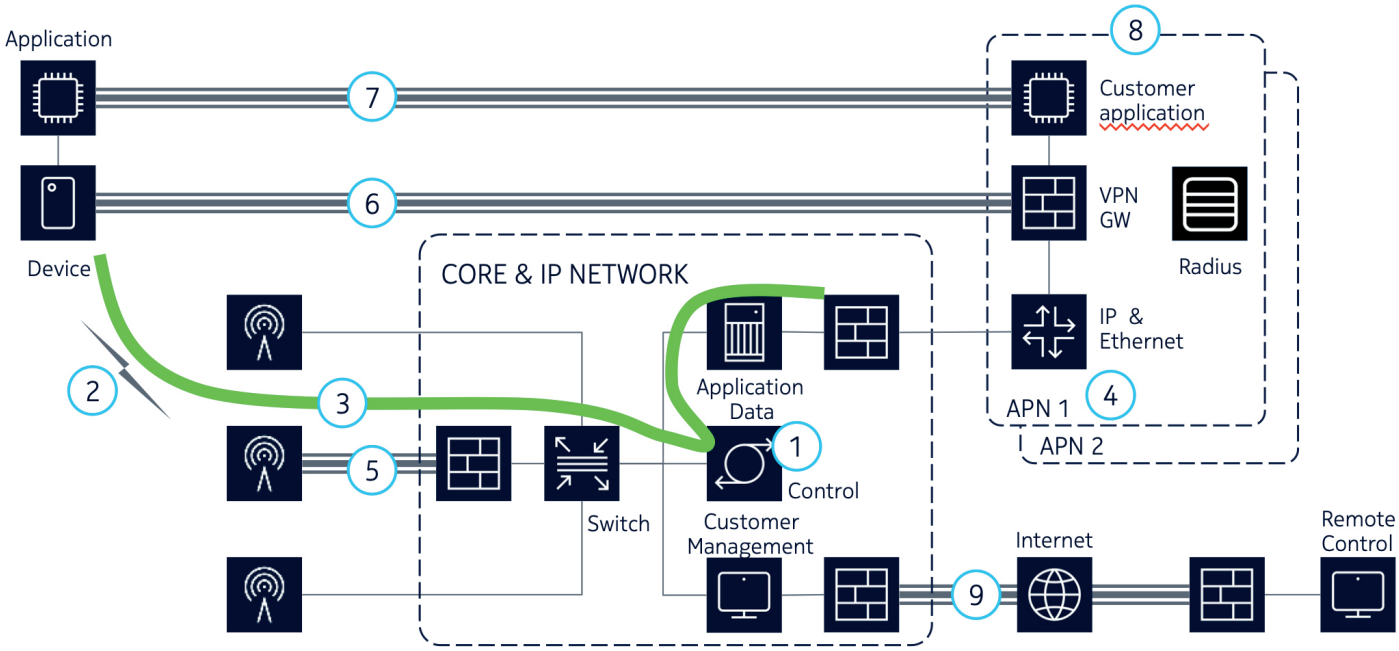
Security

Critical communications networks must be secure, and sensitive communication content must be encrypted. This means that the communication system must be protected with reliable security solutions covering the network, devices and applications. Security is an inherent part of 3GPP standardized systems such as LTE and 5G. 3GPP has defined several security measures, a few of them are listed below:

- **Subscriber database (HSS)**
  - List of users that can access the service – linked to a SIM card in the user equipment
  - Pre-shared encryption keys (SIM/HSS)
- **Radio link is encrypted**
  - Stronger encryption than WiFi, 2G and 3G
- **User traffic is tunnelled (to APN)**
  - User traffic on radio and core runs in a tunnel
- **Allows to maintain different ecosystems in parallel**
  - Different IP networks (APN's), overlapping IP ranges, different user groups.

8 IOPS: Isolated Operation for Public Safety networks. Allows network to operate whilst losing backhaul connection to central core.

Figure 5. Security options for private wireless cellular network



1. User/device is authenticated by SIM and granted allowed services/QOS/APN
2. Radio link encryption
3. User traffic is tunneled and encrypted (SIM) up to APN
4. Device receives an IP address from enterprise IP address space/authentication as usual
5. (Optional) Radio connection can be protected by IPSEC when using open transmission network
6. (Optional) Airport user may use IPsec between device/router and VPN gateway
7. (Optional) Airport application may include data security (e.g. TLS, SRTP, etc.)
8. (Optional) Airport IP network may implement classic cybersecurity applications
9. (Optional) Airport private network may need remote control. An external internet connectivity enabled for VPN/TLS as per industry best practices should be configured.

Security in LTE is similar to standard TETRA technology, supporting mutual authentication, air interface encryption, as well as end-to-end communication encryption (see Table 4).

Table 4. Tetra vs. LTE security

	TETRA	LTE
Access authentication	Mutual authentication and key generation based on pre-shared key in MS and AuC.	Mutual authentication and key generation based on pre-shared key in USIM and AuC/HSS[9]
Air interface protection	Dynamic (class 3) TETRA encryption: TEA1, TEA2, TEA3 and TEA4. TEA2 is restricted to Europe.	NAS signaling and Radio Resource Control (RRC) signaling protection and user plane encryption: 128-bit SNOW 3G, AES, ZUC (256 future option supported).
Group communication protections	End-to-end encryption for example based on 64-bit IDEA or 128-bit AES.	Service authentication and authorization. SIP and HTTP protection. End-to-end secure media and floor control with SRTP and SRTCP based on 128-bit AES-CM.

Latency

Latency is becoming an ever-increasing characteristic of many airport use cases. Known examples are Push-to-Talk voice services and baggage scanner response time. New use cases such as collision avoidance of (automated) airport vehicles, augmented reality for maintenance, biometrical scanning and automated remote-controlled gate bridges, will increase the pressure on networks to even further reduce latency. As such, it is essential that end-to-end network performance supports this latency requirement.

From a wireless perspective, it is essential to make the right choice in technology. 4.9G/LTE private wireless already features latency performance of around 10ms. Such performance already allow airports to support a range of use cases that require low latency performance. For those use cases that require even more stringent latency performance, down to 1ms or lower, 5G becomes the target technology.

The latest release of Wi-Fi, 802.11ax or WiFi 6, is expected to support latency performances down to 1ms, as well. However, it is critical to understand that these latency figures can only be achieved in unloaded conditions. The Wi-Fi latency performance under load condition will be significantly higher. Again, this addresses service reliability and predictability, which can be guaranteed by 4.9G/LTE and 5G solutions but not by Wi-Fi.

In summary, given the increasing importance of latency, airports will have to carefully select the technology and its future capabilities for wireless access. Driven by many industrial use cases, 4G and 5G are designed to optimize on latency performance. The chain is only as strong as its weakest link!

9 AuC: Authentication Center; HSS: Home Subscriber System.

NOKIA

Commercial considerations

Business models

Business models for airport private wireless networks can vary in a number of ways. Drivers for the model type are the local spectrum situation and the airport's preferred financial model. Although there can be quite some variety in preference of business models between airports, it is clear that the majority of airport operators are not expecting themselves to become technology experts and have full ownership of 4G/5G radio and core management.

Taking the above into account two possible examples of a business model could be:

- **Airport owns spectrum**
  In this case, the Airport could own the private wireless hardware. In addition, the airport would have access to the most relevant monitoring and configuration parameters for the private wireless network. Remote OAM via a service subscription can be done by:
  - A hardware vendor like Nokia
  - The airport's preferred entity
- **Airport does not own spectrum**
  In this case there is a dependency on a mobile network operator (existing public or critical communications operator) or a license holder willing to sublease to build a private wireless network. Traditionally mobile network operators offer this as a service (OPEX) to their customers. Depending on the local situation, a mobile operator may be able to offer some control and real time monitoring information to the airport.

Alternative models may apply and will be driven by local situation, airport requirements, etc.

Total cost of ownership

Today, airports rely on a combination of public wireless services, Wi-Fi and PMR for their operations. 4.9G/LTE and in the future 5G will be able to collapse these silos into a single multiservice wireless network for all of airport staff and their tenants.

Wi-Fi is often seen as a very cost-effective solution and its cost/simplicity combination is its strength in IT-like applications. However, as outlined in this whitepaper, we strongly advocate, given the characteristics of Wi-Fi versus the airport requirements on reliability and predictability of services, to position Wi-Fi for passenger connectivity rather than operations.

Calculating total cost of ownership of a private wireless network should include savings from subscriptions to public wireless services and PMR OPEX costs. In addition, LTE/4.9G and 5G can replace cabled infrastructure like CAT-x or fiber. Especially at airside where new cables are prohibitive in terms of costs, reliable wireless connectivity will allow airports to cost-efficiently introduce connectivity for example for additional cameras (security, stand analytics, etc). Similar CAT-X/fiber considerations apply for example to kiosks, biometric scanners and gate-readers at terminal side to allow more flexibility in airport setup and to reduce connectivity re-arrangement costs.

As mentioned before, Wi-Fi has its own unique strength at the airport by realizing an excellent customer connectivity experience. Nevertheless, for comparison reasons we'd like to highlight a couple of aspects of a private 4.9G/LTE or 5G deployment in comparison to a Wi-Fi deployment.

- A 4.9G/LTE or 5G Base Transceiver Station (BTS) or even a small cell, is more expensive than a Wi-Fi access point. There are two technical design factors that contribute the most to the cost difference:

  1. Higher power radios
  2. Scheduler capabilities

  These two factors are also related to what makes 4.9G/LTE and 5G perform much better than Wi-Fi at addressing the critical application requirements of industrial users. The future standard of Wi-Fi (Wi-Fi 6) is proposing the addition of such a scheduler on the Uplink, which is yet to be implemented on any commercial product. We expect these Wi-Fi 6 AP's with a scheduler to have a significant cost bump. The higher-powered radios in a 4.9G/LTE or 5G BTS are one of the reasons why this technology provides a much wider coverage and penetration capabilities (e.g. covering aircraft inside from nose to tail) than Wi-Fi. For any given site area including full airfield, the number of BTS's will be much less than with Wi-Fi.

- LTE requires a core network, which Wi-Fi does not (except for management and user authentication). 4.9G/LTE or 5G requires coordination between the BTS and other features that operate "centrally" This core network enables device mobility at very high speed, coordination for multi-cell deployments, better interference management, QoS differentiation and improved security and availability. All these capabilities add to a reliable service and addresses the technology's capability to address a variety of tenants with different service requirements.
- 4.9G/LTE and 5G require SIM cards to authenticate users. Although this adds some complexity and cost, it strictly controls who has access to the network, hence, immediately improves security of the service (most Wi-Fi hacking techniques rely on breaking the authentication methods used).
- In the past, 4.9G/LTE networks were complex to manage — much more complex than Wi-Fi. Today, private wireless networks can be managed through a simple dashboard, focusing on the most relevant parameters in the network for the airport to be in control of the configuration.

As can be seen, there are many parameters that influence TCO and there is no generic "one size fits all" approach for airports. Also, comparing the TCOs of several technologies isn't straightforward given that such technologies have different strategic targets.

For airports investing in private wireless for their digital airport strategy, the wireless network becomes a strategic asset, a unique purpose-built network that is an essential platform for the digitization of the airport's operations. Its reliability, coverage, security and resilience is essential to establish both outstanding operational efficiency and an excellent passenger experience.

Non-aeronautical revenue

Introducing a high reliable wireless service at the airport also allows airport operators to consider monetizing wireless services to tenants. Examples could be third-party companies, such as de-icing companies, supporting their digital process. It could also include airlines for below- and above-wing processes, including aircraft telemetry offloading to AOC.

NOKIA

Use cases

As mentioned at the very beginning of this whitepaper, a private wireless network will form the foundation of unified communications between all airport stakeholders, with each stakeholder having their own set of communication requirements (QoS, type of service, bandwidth, etc).

In the table below, a number of use cases are described, a majority of which can already be implemented with 4.9G/LTE. Obviously, this is a limited set and there will be a myriad of other airport cases where private wireless connectivity will fit well.

Table 5. pWLS airport use cases

Use case name	Description
Follow me car	Marshal to have real-time visibility in vehicle of runway activity and upcoming flights.
De-Icing	De-icers have real-time visibility of which aircrafts will require de-icing and can populate digital log book.
Enhanced situational awareness - vehicles	Vehicles (common use or first responder) are equipped with a wireless connected pan-tilt-zoom (PTZ) camera in order for the APOC to receive enhanced situational awareness, anywhere at the airport.
Enhanced situational awareness - bodycam	Security officers will be equipped with wireless body cameras or use their smart phone camera to stream video images to security office / APOC and push to video to security colleagues.
Asset connectivity	Airport assets can be connected wirelessly, avoiding the need for expensive CATx or fiber installation and introducing flexibility. Examples can be kiosks, biometric scanners, CCTV, etc.
Baggage scanning	With IATA resolution 753 in place, the necessity to scan at predefined points becomes obvious. This requires scanners to be connected to a network that is guaranteed available and with low latency to support quick response times.
Telemetry offload	The connected aircraft is becoming a reality. With Terabytes of data being generated during a flight, this data needs to be offloaded while at the airport in a secure and efficient way for further analytics.
Passenger bus	For a more efficient passenger transportation from/to the airplane, bus drivers need clear directions on where they need to drive. A connected display/tablet will provide them with real-time information regarding directions.
Stand automation	Airports are required to keep on enhancing their efficiency. This is especially true for the densest use case environment: the stand. Wireless connectivity should be guaranteed in this environment, including coverage, capacity and QoS. Use cases such as automated gate bridge, turnaround optimization analytics, autonomous vehicles will be depending on reliable wireless connectivity.
Critical communications	Private wireless supporting critical communications such as Push to Talk or Push to Video used by many tenants at the airport.
Asset awareness	Connected assets can be tracked in terms of location in order to improve the operational efficiency.

The majority of the use cases in table 5 can be covered with private 4G/LTE taking into account throughput requirements. Some of the use cases are candidates for 5G, for example telemetry offload. It is one use case that could take advantage of 5G's enhanced Mobile BroadBand (eMBB) ability to offload large amounts of data in a short amount of time that does not jeopardize the aircraft's turnaround time.

Conclusion

Like many infrastructure players, today's airports are keen to adopt digital technologies and integrate them into their day-to-day operations. These Industry 4.0 technologies, such as IoT, AI, machine learning and data analytics, hold great promise for improving the experience of passengers, while lower operating costs, improving security and expanding the kinds of services that airports can offer to partners and tenants.

One of the key pillars in an airport's digital strategy is pervasive, reliable and secure wireless communications able to support a diverse set of use cases and applications. Currently airports typically employ publicly accessible Wi-Fi, which is shared by passengers and operations staff. They also normally have a choice of several locally available mobile operator services. Neither of these wireless services is up to the task of supporting the digital transformation of airport operations, as we have discussed. Airports need to consider a separate, purpose-built private wireless network to support their digital operations and mission-critical communications.

The most promising technology, widely touted for Industry 4.0, is 5G. Given that the majority of use airport use cases can be deployed using a 4.9G/LTE network, this technology will provide the wireless foundation for the airport with a clear evolution path to 5G. With the availability of smaller modular private network solutions from vendors such as Nokia, the operational expense and TCO of 4.9G/LTE networks has been brought in line with other networking options. With the increasing availability of spectrum being released by governments for private use, airports now have the opportunity to deploy the wireless communications support they will need to pursue their most ambitious digital goals.

Nokia Oyj
Karaportti 3
FI-02610 Espoo, Finland
Tel. +358 (0) 10 44 88 000

Document code: SR1911039962EN (October) CID191881