

5G in the Operating Room

Experimental Study Outcomes

Contents

Abstract	2
Introduction	2
Wireless devices in healthcare.....	3
5G technology overview	4
Haventure experimentation	6
Safety & cybersecurity considerations.....	8
Key learnings and recommendations.....	10
Enabler for remote access to MD	11
Conclusions and Future Outlook.....	12
Glossary	13

Abstract

This white paper presents the outcomes of a three-year experimental project investigating the use of private 5G networks in the operating room (OR). Conducted in collaboration with French and German partners, the study explored how 5G can address challenges such as cable-related hazards, limited data access, and the need for remote expertise. The experimentation focused on wireless medical devices—namely tablets and augmented reality headsets—used to support robotic surgery.

Demonstrators in Grenoble and Aachen validated the feasibility and benefits of private 5G, including enhanced sterility, improved workflow efficiency, and secure real-time data access. The findings also highlight safety and cybersecurity considerations, regulatory constraints, and barriers such as slow device adoption and operational costs.

Key recommendations emphasize the importance of operator involvement for reliable deployment, as well as the growing role of 5G in enabling remote connectivity for medical devices.

Overall, the study concludes that private 5G offers a promising, secure, and high-performance infrastructure tailored to the specific needs of healthcare environments.

Introduction

Healthcare is a field in constant evolution, driven by the dual pressures of innovation and necessity. While the demand for more efficient, personalized, and cost-effective care continues to grow, some technologies remain underutilized, sometimes due to a lack of field validation or real-world experimentation.

Challenges in the operating room (OR) are numerous and include safety issues due to cables and other tripping hazards or crowded space around the patient, as well as efficiency with an improved availability of data during a surgery or a remote expertise.

Our main thought was that wireless connectivity could address these challenges by freeing space in any type of OR, giving more information to surgeons while keeping the environment sterile. This would be particularly true with 5G technology which comes with very interesting features detailed later in this report.

In 2022, our team embarked on a three-year experimental journey to test 5G technology in a real healthcare setting in an international environment. We did it jointly with several partners in France and Germany, collaborating with medical professionals and technical experts. We sought to measure the impact, usability, and limitations of 5G technology.

This white paper is the result of that journey. It aims to provide an actionable account of our experiment — from design to practical outcomes. Whether you're a healthcare decision-maker, technology developer, or policy advisor, this document offers data, insights, and recommendations that can inform your strategies for adopting 5G in the medical field.

Wireless devices in healthcare

The integration of wireless technology into healthcare systems is becoming increasingly common, to the benefit of both patients and care providers. This is particularly true in high-stakes environments such as the OR. In many industries, wireless devices are now considered the gold standard for greater efficiency. This also applies to healthcare with hospitals and surgical centres eager to improve usability of medical devices in order to deliver safe care.

The rapid growth of this sector has been emphasized in recent market studies. The global wireless medical device market is projected to reach US \$30 billion by 2025, with a compound annual growth rate of 12%. This increase is driven by many factors in constant growth like the prevalence of chronic diseases, remote health services, and the demand for real-time patient monitoring.

The trend towards wireless technologies is also observed in the OR, enabling a new era of surgical innovation. Wireless medical devices are used in the operating theatre for applications such as monitoring of vital signs, smart surgical instruments, implantable sensors and real-time data transmission systems. These devices enhance intraoperative decision-making, streamline workflows and eliminate cables for improved safety. Wireless connectivity relevant to the OR, which enables real-time data exchange and coordination, is a fast-growing subset within the broader medical device connectivity market. This market was valued at US\$3.4 billion in 2025 and is growing at an annual rate of **20%**.

Some of the conclusions of this white paper apply to any wireless technology like 5G, Bluetooth or Wi-Fi. However, this report focuses on 5G and we will explore the potential benefits of this technology.

5G technology overview



5G stands for 5th Generation of mobile network technology. It corresponds to a standard defined by 3GPP and ensures interoperability between manufacturers. This is even more important in 5G as it introduced the notion of Open RAN paving the way for greater openness.

Before going deeper into this technology, it's important to point out the presence of 2 major branches and to explain their differences:

PRIVATE 5G

A private 5G network is a dedicated infrastructure built for a specific organization (a clinic or an hospital in our case) covering a local area or a set of areas. This network is designed to meet with the organization's needs in terms of connectivity and can be highly customized for that purpose.

- **Our experimentation has been rolled out in that context**, looking at very detailed characteristics that could be exploited to fit with OR needs and challenges to tackle.

PUBLIC 5G

It is also known as "5G" for the general public.

Such networks are provided by mobile operators like Vodafone, AT&T, Orange, Deutsche Telecom and many more. They usually cover a full country and are accessible by the general public.

- Not directly linked with the experiment, this network type **can be considered to setup a secured and remote access to medical devices** like described later in this report.

In both cases, users are identified with a SIM card or an eSIM and networks grant access to resources based on that identity. Of course, the number of resources shared in a public 5G network is greater than in a private 5G network, where the load on each resource can be precisely tuned.

The main differences between these network types are ownership, radio coverage, performance, security and costs. But compared to previous standards of 3GPP, the 5th generation takes the concept of privacy further, aiming to customise a mobile network for specific uses, such as in healthcare.

Beyond wireless and remote aspects, 5G is interesting in the OR due to the following characteristics:

QUALITY OF SERVICE

5G comes with a very interesting feature called slicing. It dedicates network resources to each slice which are isolated from each other and can support different performance commitments. This comes in addition to standard 5G Quality of Service management associating different guarantees, such as bit rate or latency for example, with each data flow.

This characteristic is extremely important in the OR where priorities differ between services, with some being critical for patient safety.

SOVEREIGN NETWORK

The advent of both private 5G networks and the Open RAN alliance enables the creation of sovereign networks with a wide choice of suppliers. The radio planning of such a network can also be designed to benefit from indoor coverage which is a requirement for some hospitals or clinics which host their operating rooms in the basement. Last but not least, 5G edge computing capabilities allow the hospital to efficiently process patient data close to the point of acquisition, keeping it confidential to help fulfilling GDPR or HIPAA constraints for instance. A private network designed, implemented and operated for a healthcare centre can therefore be tailored to meet specific medical needs and to take into account the local environment.

NO INTERFERENCE

The radio frequency spectrum for mobile networks has been extended to include millimetre waves in 5G. There is a large band above 26GHz that is far removed from the frequencies of electromagnetic waves used by medical devices. This prevents potential interference. In addition, this frequency range offers higher data throughput and allows the size of the antenna to be reduced, making it ideal for indoor coverage of small areas, like OR in hospitals.

Private 5G is often compared to Wi-Fi for wireless communications. Indeed, Wi-Fi has proven its efficiency and reliability and became a reference in the industry for many wireless devices. However, private 5G offers advantages over Wi-Fi which are key when implementing such wireless technologies in healthcare centres :

ENHANCED SECURITY

In terms of access control, 5G benefits from its licensed access to radio frequencies whereas Wi-Fi doesn't require any permission. The radio layer mechanisms in a 5G network are far more advanced than those in a Wi-Fi network when it comes to combatting saturation or DDoS attacks. In addition, a SIM card or eSIM must be provisioned for the user equipment to exchange with the network using 5G bands.

Authentication mechanisms themselves differ between these technologies. 5G

relies on user identity with secrets stored in the device (SIM) and in the network (UDM) and the AKA mechanism. Unfortunately, even the latest 3rd generation of WPA used by WiFi has already been hacked..

LATENCY RELIABILITY

Ultra low latency (below 5ms) is a strong requirement in 5G and the standard has been written to achieve that goal. Even if the Wi-Fi standard is improving in that area, first the service level is not guaranteed and second, we can observe a high variability with high-latency peaks occurring from time to time.

GUARANTEED QoS

We already pointed out the importance of the quality of service (QoS) of the network in healthcare. Wi-Fi can only manage QoS locally on its air interface and doesn't necessarily map the request in the IP header with its priorities. Therefore, it's clearly a best-effort mechanism whereas 5G can deliver guaranteed performances end to end. For critical applications, resources can be reserved to ensure a certain bit rate throughput for example.

Haventure experimentation



The 5G Forum (Flexible OR Use and Monitoring) project was initiated in 2021, with a Franco-German consortium, aiming at demonstrating the benefits of Private 5G in the operating room. Thanks to 5G, the objective was to solve problems such as the excessive number of cables in the

OR, limited or unavailable data access for surgeons, and time lost due to a lack of assistance. To demonstrate the efficiency of this technology, two demonstrators were built in clinical environments in Aachen (Germany) and Grenoble (France).

As a leader of the French project, Haventure managed the entire program from voice of the customer to final demonstrations, passing through research and development and regulatory affairs.

CONTENT OF THE EXPERIMENT

In the area of digital and robotic surgery, the project started with an assessment of users needs when addressing problems exposed earlier. The requirements of surgeons and nurses led to the use of two wireless devices : a **medical tablet** and an **AR headset**.



These devices are intended to act as accessories to a surgical robot, in order to support the following use cases :

- Surgery workflow control
- Surgical plan adjustments
- Access to patient data stored in PACS
- Videoconference with remote users

The common characteristic behind these operating cases is the use of wireless devices, allowing surgeon and his assistant to accurately and efficiently control their robotic devices without breaking sterility.

EXPERIMENTATION OUTCOMES

The demonstrator was successfully developed and rolled out, with in-house developed applications, leading to interesting presentations to medical users. The ability to adjust a surgical plan intraoperatively, while staying in position beside the patient and maintaining sterility, was greatly appreciated.

Haventure, and its associated partners in the consortium, acquired a strong experience in areas such as:

- Medical staff requirements around wireless devices in the OR specifically
- Private 5G in practice with its features and performances
- Safety and security risks inherent to wireless medical devices
- Regulatory constraints applicable to such accessories

OBSTACLES

As early adopters of an emerging technology, we necessarily faced many barriers. While we overcame most of these, there are remaining hurdles that could slow down deployment:

SLOW ADOPTION OF 5G

5G networks are now widespread, but device manufacturers are not necessarily incorporating 5G chipsets into their hardware. This is even more common in

specific industries where volumes are limited. In the healthcare industry, for example, medical tablet manufacturers are not prioritising 5G.

ENTRY AND OPERATION COSTS

There is a huge step going from an experimental network to a production network that fulfils all regulatory requirements. 5G networks are reassuring in terms of security and reliability but they must be managed. Thus, there are many costs including, among others, architecture design, users provisioning, detailed configuration and 24/7 operations. We conclude that hospitals should delegate such activity to local mobile operators.

Safety & cybersecurity considerations

As with any medical device, we followed both safety-by-design and secure-by-design approaches throughout the project. As part of this process, Haventure experts conducted several risks analysis that consider both safety and security of the medical device accessories connected in 5G.

SAFETY

Wireless, and consequently 5G, is transformative for several reasons:

TRIPPING HAZARDS

Regardless of the size of the operating room, the medical staff are always concerned about the amount of cabling. The fewer cables around the patient's table, the fewer tripping hazards that could result in serious injury to the staff and the patient.

STERILITY

In the OR, the area around the patient must meet very strict sterility requirements. As the surgeon works in this area, it is easier to maintain sterility by providing them with wireless tools (such as a medical tablet or headset). This also prevents the surgeon from moving around the room and risking touching non-sterile equipment.

In terms of usability, some risks are mitigated by clearly displaying the 5G connectivity status in the medical device interface. This represents a minor change in the UX design to remove cables.

CYBERSECURITY

Among all the **security control measures** identified, some measures **benefit from 5G features** such as:

MUTUAL AUTHENTICATION

This feature has been introduced by design in 5G networks. Mutual authentication between a wireless accessory and the medical device station is facilitated by SIM cards and eSIM. The network authenticates the device and verifies that it is indeed a valid subscriber. Likewise, the device authenticates the network to make sure it's talking to the right service provider.

This mechanism is also applied in the upper layers such as the application layer, and it ensures an in-depth protection preventing any unauthorized tablet from accessing the network.

END-TO-END CYPHERING

Our medical solution doesn't necessarily connect two wireless devices, but a wireless medical accessory to a station. A 5G network provides encryption of data between the user equipment (UE) and the packet data network (PDN). Since this PDN and the station are connected to the same local private network or possibly physically connected, the link between the accessory and the station can be encrypted. This mitigates the threat of tampering at the radio interface and beyond.

Regarding the **physical layer** and wireless aspects in particular, the [AAMI TIR69 guidance document](#) is a good reference for radio frequency wireless coexistence for medical devices. It provides interesting insights into testing in a healthcare environment, and we have used this document for several purposes:

- definition of tests related to the wireless interface, resulting in a performance report
- commitment to radio frequency specifications such as bands and transmission power
- hardening of devices to avoid other wireless and less secure connections

Our demonstrator in France relied on a 100 MHz band of electromagnetic frequencies between 3.9 and 4 GHz, granted to us by ARCEP for a predefined geographical area. As explained above, the need for a license for the electromagnetic spectrum greatly enhances security compared to other wireless technologies. In addition, millimeter waves with frequencies above 26 GHz could provide even greater safety by not interfering with other medical devices. Note that in the USA, the allocation of frequency bands is different. In fact, private 5G deployments must use the Spectrum Access System (SAS) to avoid interference and comply with FCC regulations.

When it comes to **network layers** and the 5G network itself, several studies have been released by highly qualified cybersecurity organisations such as ANSSI in France and CISA and NIST NCCoE in the USA. These documents are continuously updated with new details and new recommendations, with some being release just a few months prior

to this white paper. Key recommendations from these studies are applicable to our context and we report here a few of them:

NETWORK SECURITY CONFIGURATION

No two 5G networks are the same, and the 3GPP specifications allow for the security level to be adjusted to fit our needs. Given the vulnerability of the healthcare sector to cyberattacks and the level of safety expected in the operating room, it is essential to configure optional standardised cybersecurity and privacy features.

Many optional features are related to accesses authorization like the use of concealed identifiers (SUCI) and the reallocation of temporary identifiers. There are also optional controls to be configured both in the control plane and the user plane.

Finally, network infrastructure should follow security design principles such as the isolation of distinct traffic types (data, signalling and operation & maintenance) from each others.

SELECTION OF SUPPLIERS

Security risks may arise from counterfeit or inherited components, particularly in a highly modular 5G network. In terms of hardware, roots of trust are required to ensure authenticity. On the software side, suppliers must allow easy vulnerability monitoring, which is particularly important in a software-designed network.

NETWORK OPERATION

Alongside all these design-stage measures, network monitoring is essential to preserve its security over time.

User and slice management is key, as both are central to cybersecurity, even though slicing can also improve security by isolating data.

Key learnings and recommendations

Voice of Customer sessions conducted by Haventure with surgeons and nurses clearly confirm the **interest in wireless devices** in healthcare, and in the OR in particular, for all the reasons outlined above. Some medical device manufacturers are already incorporating it into their designs, but it will likely become a necessity for any manufacturer who wants to stay ahead of the market.

The **benefits of private 5G** are clear for any hospital and were clearly seen in both our French and German demonstrators. With this technology, the hospital can design a wireless network tailored to its needs in terms of privacy and performance. As shown above, 5G ensures an in-depth security of the network and its features are ideal for

mitigating cybersecurity risks.

Despite being introduced some years ago, **5G adoption** is still relatively slow compared to predictions and may be suffering from a negative image in the public's mind. This has a double negative effect, as 5G-specific devices, such as medical tablets, are rare or non-existent, and investment in private 5G networks is very limited. As this affects both the devices and the network, it is a chicken-and-egg problem as to who will invest first.

Nevertheless, recent signs point to initial investments in private 5G in healthcare centres, such as in Oulu (Finland), and Bordeaux (France). This is a first step on the part of hospitals, which should be supported at the device level. We hope that these initiatives will be continued by other medical centres with the support of **mobile operators**. Indeed, we have highlighted the importance of monitoring such networks for security and patient safety. Even if the network is supposed to be private, the involvement of an operator is important to get a well-designed, reliable and efficient network.

Enabler for remote access to MD

This white paper is essentially focused on private networks but there is another **benefit for medical devices hosted in hospitals with public 5G**. To date, most medical devices are totally isolated from external environments, sometimes just connected to the local network to access a PACS for instance.

This posture is beginning to change with the need for interconnection with remote servers to manage the installed base and users, update software, import and export data and access external APIs. This is even reinforced with cybersecurity regulatory requirements forcing the device manufacturer to fix a potential vulnerability on its medical device in a very short time frame.

Today, MD manufacturers are building cloud-based infrastructures, hosting services dedicated to their devices. They are also supported by hyper scalers, which are offering more PaaS services dedicated to the healthcare sector, proving that the need exists.

The network connection between a medical device in the OR and this cloud-based infrastructure becomes critical. A first approach is to use the hospital's local area network with the involvement of its IT department. However, this approach can be cumbersome for many reasons, and 5G could enable this remote access more easily. The security features in 5G technology can ensure a reliable and secure remote connection, if the configuration is done correctly.

Conclusions and Future Outlook

Haventure and its partners have conducted a complete experimentation of private 5G, as well as an in-depth assessment of its impact on medical devices in the OR. The results of this experimental project are encouraging when considering the introduction of private 5G in the OR, which provides a secure wireless environment for improved safety.

A comparison of this technology with other wireless solutions shows that 5G best meets the needs of healthcare and its regulatory requirements, even if it is less cost-effective.

Assuming a continued rollout of private 5G networks around hospitals, there is a clear potential for the deployment of wireless medical devices that become standard and supported by all medical staff working in the OR.

With its practical experience, Haventure can help and advise in this area. Inquiries for more information on the project presented here, or expressions of interest in future collaborations are welcome.



This project has been funded
by the French government
as part of France 2030.

Glossary

5G (Fifth Generation Mobile Network)

The fifth generation of mobile network technology designed by 3GPP.

3GPP (3rd Generation Partnership Project)

International body that defines mobile network standards, including 5G.

AKA (Authentication and Key Agreement)

Authentication mechanism used in mobile networks to secure access.

AR (Augmented Reality)

Technology that overlays digital information on the real world, typically through a headset or tablet.

ARCEP ("Autorité de Régulation des Communications Electroniques et des Postes")

French Regulatory Authority for Electronic Communications and Postal Services, responsible for spectrum allocation.

MD (Medical Device)

Any instrument, apparatus, or software intended for medical purposes.

DDoS (Distributed Denial of Service)

Cyberattack aimed at overwhelming a service to make it unavailable.

GDPR (General Data Protection Regulation)

European regulation governing personal data protection.

HIPAA (Health Insurance Portability and Accountability Act)

U.S. law establishing standards for protecting health information.

LAN (Local Area Network)

A computer network limited to a local area, such as within a hospital.

Open RAN (Open Radio Access Network)

Open and interoperable approach to the radio access part of mobile networks.

OR (Operating Room)

The room in which surgical operations are performed.

PACS (Picture Archiving and Communication System)

System for storing and managing medical images such as X-rays or scans.

QoS (Quality of Service)

Mechanisms ensuring network performance such as latency, bandwidth, and reliability.

SIM / eSIM (Subscriber Identity Module)

Physical (SIM) or embedded (eSIM), used to identify devices on a mobile network.

SUCI (Subscription Concealed Identifier)

Temporary identifier protecting subscriber identity in a 5G network.

UE (User Equipment)

Any device connected to a mobile network (e.g., tablet, AR headset).

Wi-Fi (Wireless Fidelity)

Wireless communication technology commonly used for local area networking.