Master's Thesis

Software Engineering and ICT

YICTIK21

11.7.2024

Ari Pitkäranta

Wireless networks in cleanroom environments

TURKU AMK

TURKU UNIVERSITY OF APPLIED SCIENCES

Master’s Thesis | Abstract

Turku University of Applied Sciences

Software Engineering and ICT

2024 | 42 pages

Ari Pitkäranta

Wireless networks in cleanroom environments

This master´s thesis was done for Bayer Oy in Finland as a part of its internal digitalization project and to build and commission a new factory in Turku.

The need to modernize and digitalize working methods in cleanrooms also brought up a need for wireless devices within the whole facility. This need for wireless access also included the cleanroom areas, which are highly regulated.

This thesis reflects the work process behind choosing the current method to simulate and implement wireless networks and the process of choosing the correct technology to best suit the needs.

The most difficult thing in the cleanrooms was the metal structure blocking the passage of wireless signals, which formed a Faraday cage in each room. These difficulties were solved by simulating the environment with software and by using antenna solutions, which enabled the network to be installed in a compliant way in cleanroom environments.

Opinnäytetyö (YAMK) | Tiivistelmä

Turun ammattikorkeakoulu

Ohjelmistotekniikka ja ICT

2024 | 42 sivua

Ari Pitkäranta

Langattomat verkot puhdastilaympäristöissä

Tämä lopputyö tehtiin Bayer Oy:lle Suomessa osana sen sisäistä digitalisaatioprojektia sekä uuden tehtaan rakentamista ja käyttöönottoa Turkuun.

Tarve modernisoida ja digitalisoida työtapoja puhdastiloissa toi myös langattomien laitteiden tarpeen koko toimipisteessä. Tämä langattoman yhteyden tarve sisälsi myös puhdastila-alueet, jotka ovat erittäin säänneltyjä.

Tämä opinnäytetyö heijastaa langattomien verkkojen simulointi- ja toteutusmenetelmän valinnan taustalla olevaa työprosessia sekä puhdastila asennusten tarpeisiin parhaiten sopivan tekniikan valintaa.

Puhdastiloissa vaikeinta oli langattomien signaalien kulkua estävä metallirakenne, joka muodosti Faradayn häkin jokaisesta huoneesta. Nämä ongelmat ratkaistiin simuloimalla ympäristöä ohjelmistoilla ja käyttämällä antenniratkaisuja, jotka mahdollistivat verkon asennuksen yhteensopivalla tavalla puhdastilaympäristöihin.

Content

Pictures

List of abbreviations (or) symbols

Abbreviation	Explanation of abbreviation (Source)
AP	Access Point
ATEX	Atmospheres Explosibles
BLE	Bluetooth low energy
BS	Base Station
BSC	Base Station Controller
BTS	Base Transceiver Station
dBm	Decibel-milliwatt
DNS	Domain Name System
GSM	Global system for mobile communication
HLR	Home Location Registers
IEEE	Institute of Electrical and Electronic Engineers
IoT	Internet of Things
IPS	Intelligent Protection Switching
IrDA	Infrared Data Association
LAN	Local Area Network
LTE	Long Term Evolution
MAC	Media Access Control
NFC	Near Field Communication
OFDM	Orthogonal Frequency-Division Multiplexing
OFDMA	Orthogonal Frequency-Division Multiple Access
PSTN	Public Switched Telephone Network
RSSI	Signal Strength
SNR	Signal-to-Noise Ratio
WLAN	Wireless local area network
Wi-Fi	Wireless Alliance trademark

1 Introduction

"It will not be long before travelers by air, land, and water, will be no longer alone. That they will be able to converse with their homes may seem no advantage, but that they can remain in touch with the rest of mankind is most obviously desirable." This was stated by Archibald Montgomery Low in his book “Wireless Possibilities” in 1924.

This thesis is intended to give an overview and solutions for deploying the most common techniques and frequencies used in medical industry cleanroom wireless solutions, focusing on Bayer Oy Turku manufacturing plant implementations of different wireless solutions for production process support on two sites in Finland.

This subject was chosen mainly to support ongoing digitalization projects in the production areas at the Bayer factory in Turku, and the results can be directly used at Bayer and other pharma manufacturing sites around the world. On the conclusion part, I focused mainly on the chosen technologies. The technologies were Wi-Fi for the production network and 4G as a test environment for how a private mobile network could be used in the production environment. Wireless solutions are evolving constantly as modern technologies are developed and pushed to market, so the network is also evolving along with them.

Similar approaches to cleanroom wireless solutions were not found, as most of the cleanroom wireless documentation and papers focused on devices and cleanroom systems themselves and not the network. Solutions on how to build or design the networks for cleanrooms were not available outside of network device manufacturer advertisements.

Cleanrooms present a challenging environment for wireless solutions for several reasons. The main reason is that the room structure is commonly made of metal sheets, which creates a faraday cage that is effective in blocking all radiation from entering or leaving the room. Within the room, there are large metal machines that also present obstacles and reflective surfaces. In many cases, the machines also have moving arms and conveyor belts with products and packaging. There are other objects and personnel in the area that create a dynamic and hostile environment for radio waves.

This dynamic environment and monitoring of the machines and circumstances in it are the reasons why wireless solutions would be the preferred solution in cleanrooms. In addition, the possibility of reducing the amount of cabling and, in that way, eliminating difficult cleaning surfaces, tripping hazards, and foreign material hazards is highly appreciated. This work describes the process that we used to determine the best practices and solutions to use.

This thesis is separated into a research part and an analysis part, along with the conclusions. The research part consists of cleanroom definition, techniques used for connectivity in them, and measuring the wireless networks. The measurement part holds actual simulation and installation results derived and done in the Bayer environment. The last chapters are done by analyzing the results from the measurements and simulation, along with the theory part, and concluding them in the end.

2 Cleanroom definition

A cleanroom or clean room is an isolated space that filters and keeps the selected area clean of contaminants like dust, aerosol particles, and airborne microbes, providing the cleanest possible area to work in. It is isolated, well controlled from contamination, and actively cleaned. They also control variables within the room, such as temperature, humidity, and air flow, to fill the needs of production done in them. This is stated in Standard ISO 14644-1:2015

Scientific research and industrial production often require such rooms for various nanoscale processes. A clean room is needed for quality purposes in semiconductor manufacturing, life sciences, the rechargeable battery industry, and all other fields that need to protect the products from environmental contamination. (Ramstorp, 2008, 61-73)

A cleanroom can, and is often used, to prevent materials from leaving the area. This is in most cases the primary reason to use such rooms or areas in hazardous work, such as nuclear work, biology, pharmaceutics, and virology, where the materials handled are dangerous to living organisms without proper attire or for the environment. In addition, all materials, including the clothes and attire used in the area, must be specifically approved, and designed for cleanroom use. (Cleanroom and Controlled Environment Attire, 2015)

This separates cleanrooms into positive and negative pressure types. Positive-pressure rooms keep particles out, so the air is pushed actively out. Negative pressure is used in rooms where the escape of particles is important to be prevented. Therefore, hazardous materials, particles, dust, etc. are filtered with air ventilation to prevent contamination or spreading to other areas. In both cases, controlled airflow is through filters, and uncontrolled airflow is prevented as much as possible. This causes the rooms to be extremely tight and well-sealed for airflow, and this means that the room is very well protected from radio waves either entering or leaving, as the material to build such rooms is often metal or otherwise dense and multilayered. (Kozicki, et al. 2012, 49-57)

Cleanrooms range in size from single room to whole buildings. A single-user laboratory can be built to meet cleanroom standards within square meters, and on the other hand, entire manufacturing buildings and sites can be built to fulfill cleanroom standards, spreading even several thousands of square meters, and covering whole factory areas. (Ramstorp, 2008, 61-73)

There are also modular cleanrooms, which can vary in size. They have been argued by manufacturers to lower the costs of scaling the technology and be less vulnerable to catastrophic failure. They are also easier to scale for different needs. Picture 1 is an example of a cleanroom structure cutout, and Picture 6 is an example of a 2D image of a larger area sectioned according to cleanroom classification and use. Modularity can also be achieved using panels that can be reused or replaced in the case of breakage or changes in needs. (Technical Air Products, 2021)

Picture 1. Cleanroom example cutout (Picture from Bayer documentation)

With such a wide application area, not every cleanroom is the same. For example, the rooms utilized in semiconductor manufacturing need not to be as sterile and free of uncontrolled microbes, whereas those used in biotechnology usually must be. And the other way around, semiconductor operating rooms need not be cleaned of all nanoscale-sized inorganic particles, such as rust particles, dust, and other smaller particles. Other applications also absolutely require that there are no nanoparticles in the air, not to mention larger particles. (Whyte, 2001, 9-37)

All cleanrooms share the same feature of having a strict control over airborne particulates, which may also involve secondary decontamination of air, surfaces, workers, chemicals, and machinery. This also applies even to the physical appearance of machines, as they need to be easily cleaned. (Whyte, 2001, 9-37)

In the Bayer case, hormonal substances in powder form need to be filtered from exiting the room to prevent them from entering the ventilation system and spreading outside of the handling area. This includes the machines used there that need to be protected and stay in the area.

Equipment inside any cleanroom is designed to generate minimal air contamination or additional airflow, which means fanless devices or controlled air circulation. Choosing materials for a cleanroom's construction must avoid producing particulates, so it is best to use monolithic epoxy, polyurethane, or a combination of both for the floor coating. Buffed stainless steel or powder-coated mild steel sandwich partition panels and ceiling panels are used instead of iron alloys, which are prone to rusting and then flaking. Other metals cannot withstand the cleaning processes as well as steel can. Corners like wall-to-wall, wall-to-floor, and wall-to-ceiling are prevented by using a coved surface, and all joints should be sealed with sealant to prevent particles from accumulating and new particles from being created at the joints due to vibration and friction. (Whyte, 2001, 223-235)

Installing antennas in cleanrooms requires special antennas and installation procedures that can withstand solvents, disinfectant and/or ethanol spraying, and constant cleaning in the rooms, which can be installed tightly to the sealing or walls to prevent unwanted airflow.

Antennas and all other equipment related to networks also need to comply with cleanroom requirements, along with all equipment entering the areas, which means that they need to be easy to clean, fanless, and not provide any surfaces that can gather or spread particles or dust. These requirements rule out many devices that are otherwise suitable for the environment. In some cases, explosion prevention standards (ATEX) must also be considered in the design to prevent gases, dust, or other flammable or explosive materials from exploding or catching fire by eliminating external sparks or excess heat from the environment.

3 Different techniques for industrial connectivity

3.1 Wired networks

In addition to wireless networks, the most common method to build networks is to use cabled connections. The first connected industrial devices were cabled. There are several ways to connect devices by using wires. Ethernet (IEEE 802.3), as the leading standard, is the most common method, but other methods also exist. (Ethernet Media Standards and Distances, 2023)

Ethernet and wired connections do not offer flexibility to move devices, but on the other hand, the network is robust and can handle large amounts of data in a cost-effective way. Additionally, if there is existing cabling available, it is easy to implement. (Ethernet Media Standards and Distances, 2023)

In addition, in almost every implementation, the wired network functions as a platform to extend to wireless network; therefore, it is still a highly crucial part of all implementations of any wireless solution. There are very few wireless end-to-end solutions available that use wireless connections for the backbone. Possibly Zigbee, etc. could be constituted as such because they use mesh technologies in network construction, but even so, it still needs one gateway, usually wired, to reach outside of the mesh. (Frenzel, 2012)

For cleanrooms, wired networks provide a solid connection that is relatively easy to manage. Issues come with keeping the airtightness with cable throughputs and with cleaning the rooms with a lot of cables that are difficult to clean. (Whyte, 2001, 9-37)

Despite the wireless connectivity providing multiple benefits, still a lot of the IOT devices are connected to wired networks and will be connected in that way due to restrictions in the environment. So, the wired method can still be the chosen and preferred connectivity method. It is an inexpensive, robust, and widely supported method for connecting devices to each other and outside networks and systems. (Elliot, 2018, 13-25)

3.1.1 Ethernet

Ethernet has been in use for a long time. It has proven to be a reliable workhorse, and it offers speeds to any need. Wired devices in Ethernet networks can have one benefit compared to wireless: adding PoE (Power over Ethernet) so the device is not depending on the battery or power source close by. It can perform measurements and other tasks relentlessly with high frequency if the cable is connected to a POE feeding switch or injector. The power needed by the IoT device determines the PoE level. (Ethernet Media Standards and Distances, 2023)

The benefit of Ethernet is that it is widely used, well-standardized, and available in most buildings as a standard cabling system. Thus, there are a wide variety of different devices and additions to existing systems for connectivity available at reasonable prices.

Usually, IoT devices do not use too much power, but all connected devices can take a toll on the power output of the LAN switch. In addition, some LAN switches do not support powering up all the ports.

Another downfall of Ethernet is the length limitation of most twisted copper cables used. They can only provide connectivity with copper cabling of up to one hundred meters without extenders or other technologies. (British FibreOptic Industry Association, 2002)

Of course, fiber is one of the methods for ethernet connectivity needs that require a longer reach but still need speeds exceeding the wireless capabilities. Fiber has its limitations, which can also be cost-related. On the other hand, fibers can extend the range significantly, allowing connections up to tens of kilometers without loss of speed or delay degradation at affordable prices.

In close ranges, the fiber type that is mostly used is multi-mode, and for longer connections, it is single-mode. Although now using only a single mode has become more common, even for shorter distances. This difference in fiber types is due to the light emitted within the fiber and the fiber core thickness. Single-mode fibers have a smaller core than multi-mode fibers, and they can be used for longer distances. Multi-mode fiber has a working range of a few hundred meters, and single-mode fiber can reach tens of kilometers or more. (British FibreOptic Industry Association, 2002)

3.1.2 DSL technologies

Internet access for a mass of users started first with modems in PSTN (public switched telephone network). Then, digital subscriber line (DSL) technologies arrived. DSL enabled homes to achieve megabit speeds using the UTP (unshielded twisted pair) telephone lines. This allowed connections with lower speeds beyond the Ethernet 100-meter limitation. Speed and distances in DSL are heavily dependent on the quality of the cable in between the connection points. (Elliot, 2000, 55-57)

Beside ADSL (asymmetric digital subscriber line), there are symmetric connection ways such as single-pair high-speed digital subscriber line (SHDSL), very high-speed digital subscriber line (VDSL), and very high-speed digital subscriber line 2 (VDSL2). They are digital subscriber line technologies that provide data transmission faster than ADSL. Cisco is one of the vendors that provides the Long Range Ethernet (LRE) solution, which uses very high data rate digital subscriber line (VDSL) technology and extends Ethernet speeds from 5 to 15 Mbps service over existing copper telephone or Ethernet cabling and distances up to 1,5 km. (Elliot, 2000, 55-57)

DSL techniques provide relatively steady and cheap connections, although the speeds and delays can present an issue in modern applications. DSL is not widely used for industrial connectivity within or between machines.

3.1.3 Other technologies

There are various other technologies that can be used to connect devices in a wired way. Cable modems, for example, are commonly used in urban areas to deliver connectivity to places where such, normally coaxial cabling, is available. These are used almost only for customer internet access. There are no IoT or other industry applications widely available.

Integrated Services Digital Network (ISDN) was a circuit-based telephony technique also used in the past besides telephones to connect devices to the internet. It provided two channels of 64 kbit/s per channel in the Basic Rate Interface (PRI) for digital transport. This technology is not being actively developed and is rarely used any more. (Elliot, 2018, 61-62)

In addition, old normal dial-up modems in analog telephony systems could be used to connect various devices to the network. They can work both ways, receiving connection requests or initiating them. It is slow, and connection initiation is slow. These connections are used only for emergency connections in case anything else fails.

3.2 Short range wireless networks

Wireless networks have been developing for a long time. They were initially used for simple message delivery or broadcasting but have been developed to serve multiple purposes since then. There are several ways that are provided by different technologies to connect devices wirelessly over short ranges. Varying in speeds, ranges, and other connection variables.

Short range wireless networks consist of the most common technologies, such as Wi-Fi, Bluetooth, Zigbee, and Z-wave. The purpose of using short range wireless connectivity is to have an affordable and versatile connection that has good battery operational times. Of these, Wi-Fi devices usually have the shortest battery life, but they provide the best speed and range. 4G and 5G networks are also built as short-range networks for private use by companies.

Short range wireless is quite suitable for cleanrooms, where signals are even preferred to not travel to other areas for machine security. In addition, many machines use the same types of connectivity devices, which are preferred not to interfere with each other, which can be prevented by the structures in cleanrooms.

In cleanrooms, these short-range wireless connections are limited in range to single rooms. They do not reach outside, which is also a benefit, because that is also a security measure to prevent unnecessary usage or access to systems, as well as isolating them from each other and preventing them from interfering with other devices using the same technology or frequency.

3.2.1 Wi-Fi, Wlan

Wi-Fi, or Wireless LAN (Wlan, also referred to falsely as Wireless Fidelity) as definition is a large family of wireless network protocols based on the IEEE 802.11 standards that are used for local area networking of devices. These technologies have been developed for a long time since 1985, when the commonly used 2,4 GHz spectrum was released for use in the US. The development is ongoing, and new versions come to market at a steady pace. The current version has reached number 7, and speeds have increased to tens of gigabytes per second. (Generational Wi-Fi User Guide, 2023)

Wi-Fi Generations:

Generation (IEEE) Maximum Link rate	Adopted	Frequency
Wi-Fi 7 (802.11be) 1376 to 46120 Mbit/s	2024	2.4/5/6 GHz
Wi-Fi 6E (802.11ax) 600 to 9608 Mbit/s	2020	6 GHz
Wi-Fi 6 (802.11ax) 600 to 9608 Mbit/s	2019	2.4/5 GHz
Wi-Fi 5 (802.11ac) 433 to 6933 Mbit/s	2014	5 GHz
Wi-Fi 4 (802.11n) 72 to 600 Mbit/s	2008	2.4/5 GHz
Wi-Fi 3 (802.11g) 6 to 54 Mbit/s	2003	2.4 GHz
Wi-Fi 2 (802.11a) 6 to 54 Mbit/s	1999	5 GHz
Wi-Fi 1 (802.11b) 1 to 11 Mbit/s	1999	2.4 GHz
Wi-Fi 0 (802.11) 1 to 2 Mbit/s	1997	2.4 GHz

(Wi-Fi Generation Numbering, 2021)

Wi-Fi is part of the IEEE 802 Ethernet protocol family. The data is organized into 802.11 frames that are very similar to Ethernet frames at the data link layer, but with additional address fields. MAC addresses are utilized as network addresses for routing across the local area network. (Wi-Fi Generation Numbering, 2021)

Wi-Fi is a widely used technology for wireless networking that offers a lot of benefits, but it also has its limitations and downsides.

Wi-Fi signals have a rather limited range, typically less than hundreds of meters indoors, even in open space. Range is limited depending on obstructions, walls, other structures, and interference. In addition, transmission power is limited by local restrictions. Useable frequencies depend on the location, where available usable frequencies are limited by local laws. These reasons usually result in dead zones and signal degradation. (Generational Wi-Fi User Guide, 2023)

Wi-Fi speeds can vary significantly depending on, for example, distance from the router, the number of connected devices, and interference. These variations can reduce the usability of the network.

Multiple Wi-Fi networks can overlap and lead to network congestion and slower speeds, especially during peak usage times. When more devices are added to a network, each device may have reduced bandwidth, leading to slower speeds. This also happens because many users use their handheld devices as hotspots, even in office areas, which leads to congestion and overlapping channels. Wi-Fi operates in the 2.4 GHz and 5 GHz (in Europe) frequency bands, which are shared, or close by enough, with many other device technologies (e.g., Bluetooth, microwave ovens in 2.4 GHz). Interference from these devices can lead to signal disruption and reduced performance. (Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 2020)

Wi-Fi radios in handheld or portable devices can consume a significant amount of battery power when actively connected to a network. Heavy battery usage is increased if the signal levels are low, and the devices need higher transmitting power levels to stay connected. This can lead to reduced battery life and heating issues on the devices.

Wi-Fi networks and devices are vulnerable to security attacks and breaches if they are not properly configured and secured. Unauthorized access, hacking, and data interception are potential risks if sufficient security measures are not in place. In addition, as with any software, ensuring that Wi-Fi routers and devices are updated with the latest security patches can be a challenge in a wide spectrum of use cases. Outdated firmware can leave networks vulnerable to security threats and attacks. This is an issue, especially with older Wi-Fi devices that may not support the latest Wi-Fi security standards, leading to compatibility issues and potential security limitations because they are lacking the needed support for them. (Generational Wi-Fi User Guide, 2023)

Still, Wi-Fi remains a fundamental and standardized technology for wireless communication. Many of these limitations can be mitigated with proper planning, good configuration, and equipment selection. Recent advances in Wi-Fi technology are aimed at reducing or removing some of these limitations and providing improved performance and reliability.

3.2.2 Bluetooth

Bluetooth is a short-range radio wave based wireless technology that was intended to replace all short-range cable needs near PCs or mobile devices. It has been used to connect mice, keyboards, and other peripherals. It is an open standard for short range wireless communication. (Didcott, 2004)

Bluetooth also practically replaced Infrared Data Association (IrDA) connections because it does not require devices to be visible to each other physically, and it is more versatile and reliable in use. Bluetooth consists of three parts: a Bluetooth radio, a link controller, and a link manager. Unlike IrDA, Bluetooth technology can also use authentication and encryption for data. (Woolley, 2019, 6-8)

Bluetooth theoretical data transmit speeds in symmetrical transmit are 432,6 kbit/s, and in asymmetrical transmit sending 721 kbit/s and receiving 57,6 kbit/s. With the smallest transmit power of 1 mW (Class 3) the connection distance can be about one meter. With 2,5 mW (Class 2) up to ten meters, and by increasing the transmit power to 100 mW (Class 1) up to 100 meters can be reached. Newer standards, specifically Bluetooth 5.0 and later versions, have improved speeds and range for specific applications. (Naresh Gupta, 2016, 35-36)

The Bluetooth operating frequency is between 2.402 - 2.480 GHz, or 2.400 - 2.4835 GHz in the unlicensed band, including guard bands of 2 MHz at the bottom end and 3.5 MHz at the top.

Microwave ovens and Wi-Fi also operate on the same frequency. In order to reduce disturbance caused by other devices, Bluetooth uses frequency hopping and spread spectrum techniques. (Martin Woolley, 2019, 5-11)

In 2008, the Bluetooth standard adopted Wibree technology by the name of Bluetooth Low Energy (BLE), and it is now a part of Bluetooth v4.0 and later standards. BLE is a short-range low-energy connection method that can operate on end devices for months or years without battery charging or change. (Woolley, 2019, 8)

3.2.3 Zigbee

ZigBee is a short-range, low-power-consuming communication network based on the IEEE 802.15.4-standard. The standard was completed in May 2003. It is often called a Wireless Personal Area Network (WPAN). The planning started already in 1998, when many developers saw that there was a need for a self-organizing wireless network where either Wi-Fi or Bluetooth were not suitable. (Frenzel, 2012)

The name Zigbee comes originally from bees, which live in a colony where communication between members is crucial to survival. The technique that bees use to communicate with each other is called zigbee. It is a silent and effective way for bees to communicate. (Frenzel, 2012)

As a small-power, short-range radio standard, it is at its best in various device-control networks. ZigBee devices require a home automation controller or a bridge to operate.

According to the Zigbee alliance, Zigbee networks can consist of up to 65536 devices. The connection speed for Zigbee is less than 30 ms, and it wakes up from a sleeping state in less than 15 ms and starts transmitting in under 15 ms. This is a significant difference from Bluetooth, for example, which has a longer connection time and no guaranteed time to connect, resulting in longer delays. The distance between devices can be up to one hundred meters, depending on the environment and transmitting power. (Kallioniemi Tapio, 2009, 5)

Frequencies and transmit speeds of Zigbee: 868 MHz, one channel, 20 kb/s used in Europe; 915 MHz, 10 channels with 2 MHz steps, 40 kb/s used in the United States; 2.4 GHz, 16 channels with 5 MHz steps, 250 kb/s used globally. (Kallioniemi Tapio, 2009, 7)

Media access control method type is Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), so it listens to transport media and transmits only when the path is free, same as in Ethernet.

The channeling method is direct sequence spread spectrum (DSSS). The IEEE 802.15.4-standard defines two types of devices: full function device (FFD) and Reduced Function Device (RFD). FFD is a device that fulfills all features dictated in the Zigbee standard, and can function as PAN coordinator, coordinator, or as a regular device. Being a PAN coordinator means that device is responsible for creating the network and naming it. Reduced Function Device, like its name says, has reduced function and works in a simpler way. RFD device must always communicate only with FFD devices, never with another RFD devices. (Frenzel, 2012)

The standard defines two different network topologies: star and peer-to-peer topologies. In star topology, FFD device defines the network and functions as a PAN coordinator. When a coordinator serves as the primary controller of a personal area network (PAN), it is referred to as the PAN coordinator of that network. Other devices communicate via that coordinator. (Frenzel, 2012)

In peer-to-peer topology, the devices can communicate with each other, but in this topology, there is also a PAN coordinator. It announces the network to members that are joining it. The benefit of a peer-to-peer network is that it can be a lot more complex than a star network. (Frenzel, 2012)

The standard defines three different security levels. Level 1 does not offer any security; level 2 relies on access lists (ACL), and level 3 uses symmetric encryption to secure the data (the algorithm is AES). Security can also be improved at the application level. (Kallioniemi, 2009, 16-17)

Zigbee has a rather short wireless range compared to other similar wireless protocols like mobile networks or Wi-Fi. In normal circumstances, Zigbee devices can communicate over maximum distances of up to 10-100 meters, depending on environments and how the network is implemented. Networks can be extended with Zigbee mesh technology. Zigbee is designed for low-power, low data-rates. While this is suitable for IoT and control devices, it is not suitable for applications that require high-speed data transfer or substantial amounts of data. In addition, like Wi-Fi, Zigbee operates in the 2.4 GHz frequency band, which is also used by other wireless technologies and devices. This can lead to interferences, especially with a high density of wireless devices in the same area. Network interference and long distances may also affect at the low power consumption that is one of the main benefits of Zigbee. (Kallioniemi, 2009, 7)

Zigbee networks can be complex to set up and manage compared to other IoT protocols. Zigbee networks require a coordinator device to manage the network, and adding and removing devices can be difficult sometimes. This is usually an issue when using together different brands of devices that may use different versions of technology or their own applications of it. This can also lead to security issues, as older versions might not be as secure as newer ones.

Zigbee is widely used in many IOT applications and has a significant footstep, especially in home automation, where its low power needs and mesh capabilities are useful. It has been spread to IOT in industry as well, but in the medical industry, it has not yet been widely used. (Kallioniemi, 2009, 3-4)

3.2.4 Z-Wave

Z-Wave is a wireless communications protocol used mostly for home automation and similar applications. It is a mesh network that uses low-energy radio waves to communicate from device to device, allowing for wireless control of home appliances of any sort and other devices that do not require large data amounts to be transferred. Examples of such communication are security systems, lighting control, thermostats, locks, garage door openers and window shades.

A Z-Wave system, similar to other systems and protocols that are marketed for the home and office automation, can be remotely controlled from the Internet with a smart phone, computer or tablet, and locally through wireless key fob, smart speaker, or similar end-device with a Z-Wave gateway or central control device serving as both the hub controller and portal to the network. Z-Wave enables home control systems from various manufacturers within its alliance to work together at the application layer. (Frenzel, 2012)

3.3 Long range wireless networks

Long-range wireless networks are most commonly using technologies such as LoRaWAN, GSM technologies (2G, 3G, 4G, 5G, and future 3GPP releases such as 6G), and Sigfox. Often, in the various use cases mentioned, NB-IOT is an example using mobile technology. These technologies offer long operational times, and, in most cases, wide geographical coverage offered by different operators. Private networks are also possible to build using these technologies. The most common of these technologies are explained later in this thesis.

The downside is that, in many cases, there are limitations to latency and speed. One of the difficulties is also the cost which can raise to be quite high, especially in cleanrooms where a multitude of access points or antennas are needed to provide sufficient coverage. This also raises the complexity of the network.

Also, for long-range communication on IOT devices, there are multiple ways available. I will focus on the most used and pass the less used or obsolete systems as smaller chapters.

3.3.1 LoRaWAN

LoRaWAN is a data-transmit wireless network that is meant to be a wireless, fast, low-energy-transmit method. It is especially meant for transmitting and receiving smaller amounts of data.

LoRaWAN is a global and open standard that consists of LoRa devices and routers, which operate on background servers and application levels. It is a wireless Low Power Wide Area Network (LPWAN) network technology that is governed by the LoRa Alliance organization. (LoRa Alliance, 2021)

Most typically, the speed of the LoRa network is around 0,3 - 50 Kb/s and the connecting frequency is 15-60 minutes. Connections are mostly initiated from the device end. So, it is not intended for high-speed data transfer. On the other hand, the battery on a device can last up to 10 years, so solutions are long lasting and almost maintenance free.

The benefits of LoRa technology compared to other modulation solutions are that it has a good range and low battery consumption. LoRa is based on spread spectrum modulation, which can withstand a lot of disturbance, and reflections and diffraction have only a small effect on the signal. (LoRa Alliance, 2021)

In Finland, Digita is providing LoRa networks for customers throughout the country. Although it can provide wide coverage, it is rarely used in the medical industry to provide internal coverage within buildings.

3.3.2 Sigfox

Sigfox is a microwave radiation based IOT network that operates at 868 MHz frequency in Europe and 902 MHz in the US. It is designed for very low data rates. A connected device can transfer a maximum of 12 bytes of data every 10 minutes and 140 times in a day. In the device direction, only 8 bytes of data can be transferred. This is sufficient for many applications, for example, GPS coordinates fit in 6 bytes and temperature in 2 bytes. (LinkLabs, 2015)

Sigfox is a global company that provides network coverage throughout the world to its customers. The technique is based on differential binary phase-shift keying (DBPSK) and Gaussian frequency shift keying (GFSK), which enable communication in the Industrial, Scientific, and Medical (ISM) radio band globally. (LinkLabs, 2015)

3.3.3 Mobile based networks

In 1990, the first second-generation (2G) GSM networks were developed. Unlike the first generation (1G), it was also using the digital transfer method in the radio way. IT improved the communication between the endpoint device and the network. The 2G network was also internationally standardized by the 3rd Generation Partnership Project (3GPP), which made possible the international use of devices in countries that used the same standard. (Dahlman et al., 31-43, 2007)

2G networks had rather advanced data transfer capabilities (see picture 2.), and they were the first generation that made IOT connectivity more popular and easier to access for longer ranges. IT was also the first generation that brought data capabilities to all devices and made connectivity possible anywhere where a 2G network was available.

Technology	Download (kbit/s)	Upload (kbit/s)	TDMA timeslots
CSD	9,6	9,6	1+1
HSCSD	14,4	14,4	2+1
HSCSD	43,2	14,4	3+1
GPRS	80	20	4+1
GPRS	60	40	3+2
EGPRS(EDGE)	236,8	59,2	4+1
EGPRS(EDGE)	177,6	118,4	3+2

Picture 2. Theoretical speeds of 1G and 2G networks (Vilches, 2010, 1)

The next generation of 2G was called the third generation (3G) network. It was developed and brought to market in 2000 and was intended to provide data and multimedia for users via radio technologies. In the beginning of development, the speed was planned to be 2 Mb/s, but it was quickly superseded with further development and faster speeds. 3G networks are either

Time Division - Code Division Multiple Access (TD-CDMA) or Wide - Code Division Multiple Access (W-CDMA) networks. TD-CDMA was the first to come on the market. It was developed with data transfer as a focus. TD-CDMA also allowed the transfer of voice (phone calls), but W-CDMA uses more sophisticated voice controls along with data, which made it rapidly the more popular technique in 3G networks. (Vilches, 2010, 1-2)

Fourth generation (4G) was the next development in the 3GPP line of network standards. It was brought to market in 2010 in its early LTE stage. It was defined by the International Telecommunications Union-Radio Communications Sector (ITU-R), which specified the requirements to fill the standard.

4G is a wider spectrum of technologies bundled under the same umbrella, using various modulation techniques, MIMO, and dual cell solutions to provide maximum speed to users. (Vilches, 2010, 1)

The fifth generation of 3GPP development (5G) is the latest approved and in use standard (6G is in the development phase) in the series. It started its journey in 2019, when the first installations of 5G were done. (Nordrum et al., 2017)

In South Korea, on Wednesday, April 3rd, 2019, at 11 p.m. local time, SK Telecom launched the first 5G network, which was non 3GPP-compliant. On the same day, less than an hour later, Verizon in the US launched its own 5G network, which was also not 3GPP-compliant. The race towards new technology installations had never been this competitive before. (Park et al., 2019)

According to the 3GPP consortium, the development of 3GPP revolves around “releases” and is done through contributions from member companies. 3GPP determines specific requirements, features, and creates consequent work items that are part of a work plan, which includes a schedule for each work item. Work items then consist of technical specifications that are developed by 3GPP partners like chip manufacturers and mobile service providers. Once the work items for a release are complete, they get a sequential number and are published. (Kadia, 2024)

5G speeds range from around 50 Mbps to over 1 Gbps. The fastest 5G speeds are in the millimeter (25-26 GHz, high band n257 - n263) wave bands and can reach 4 Gb/s. High-band does not have wide coverage due to the high frequency. (Nokia, 2021)

Mid-band 5G, with frequencies around 3.5-3.6 GHz, is by far the most used now by operators. In that frequency range, in good coverage areas, it will usually have speeds varying from around 100 Mbps up to even 4400 Mbps. In this frequency range, it has a much longer reach than the higher 25-26 GHz band, especially outdoors. Mid-band, or C-Band, networks (in specifications n77-n79) were already deployed by various operators in 2021. (Nokia, 2021)

The low-band spectrum (around n28, 700 MHz, in Finland) offers the longest range and better coverage, but speeds are lower than in the mid- and high-bands. This band is also used by many other systems, which has delayed its usage. (Nokia, 2021)

What is special about 5G is its latency. Whereas older generations had latency at a minimum of 20 ms, 5G has been promised to have latency in milliseconds. So, in general, 5G is expected to bring all the benefits of an Ethernet cabled solution to mobile networks and provide connectivity at the same level. So far, the promises have not been fully fulfilled. (Nordrum et al., 2017)

The public 5G network also provides opportunities to use private networks within the public network. This is called virtual slicing. It offers a quick and scalable deployment option. Only 5G-compatible devices are necessary to use since the network hardware is shared with the public traffic and virtual gateways are used for separating enterprise traffic. 5G also offers a larger number of devices that can be connected to a single cell. This is ideal for IOT deployments. Also, the battery usage is more optimized for IOT use. (Kadia, 2024)

In Finland, the use of private 5G is more limited compared to other countries since the full spectrum of mid-band is reserved for operator use and only 4G (2300-2320 MHz) and high-band 5G (24.25-25.1 GHz) are available for private use. At Bayer, we have a 4G test network (access point in picture 10) that we have used for testing in cleanroom and factory environments in the 2300-2320 MHz range. (Traficom, 2023)

4 Signal propagation and fading

4.1 Free air propagation

According to Ampere’s circuit law and Maxwell's equations, in a perfect vacuum, radio waves travel at the speed of light. When going through any material medium, they are slowed down. Slowing depends on the medium's permeability and permittivity. Permittivity is a measure of a materials’ ability to store energy within the material itself. Permeability measures the ability of a material to format magnetic fields within the material. Air is thin enough, lacking slowing components, that radio waves in it travel remarkably close to the speed of light.

Free-space path loss (FSPL), also referred to as Free Space Loss (FSL), is the reduction of radio energy between two antennas caused by the sum of the receiving antenna's coverage area and the unobstructed, direct path through open space (typically air). The "Standard Definitions of Terms for Antennas", IEEE Std 145-1993, defines "free-space loss" as "the loss between two isotropic radiators in free space, expressed as a power ratio.” (Rappaport, 2002, 70-76)

This free-air loss can be calculated and estimated. But if there are walls and structures in the way, the exact calculations become much more difficult and turn to estimates rather than exact calculations. There are a substantial number of variables to be taken into consideration. Tightness of the room, windows, doors, reflections, other sources of frequency, etc. With the assumption that the antennas used in transmission and receiving the signal are completely lossless, this calculation assumes that the polarization of the antennas is the same, there are no multipath effects, and the radio wave path is sufficiently far away from all obstructions, it works exactly as in free space. This final restriction requires that an ellipsoidal area around the line of sight to the calculated area, known as the Fresnel zone, is free of obstructions. The Fresnel zone increases in diameter along the wavelength of the used radio waves. (Sheriff, 1996, 1-2; Rappaport, 2002, 91-100)

The concept of free space path loss is often applied to radio systems that don't fully meet these ideal conditions. However, any imperfections can be taken into account by including small constant power loss factors in the link budget. (Rappaport, 2002, 70-74)

4.2 Propagation in medium

The obstruction produced by the material is measured by its permittivity. And the ability of the material to allow magnetic lines to conduct through it is known as permeability.

Identifying known RF absorbers, reflectors, and interference sources while in the field before the installation phase is critical. It also helps in simulations to identify all materials beforehand to get the most accurate simulation possible. It is even more crucial that these sources are taken into consideration when installing an access point at its fixed location. In mediums, there are three kinds of propagation mechanisms. Reflection, diffraction, and scattering, depending on the medium type. (Rappaport, 2002, 77-79)

RF absorbers include, for example, cement or concrete, which is an effective block depending on its structure thickness and reinforcements. Old concrete has high levels of water dissipation, which dries out the concrete, allowing for potential RF propagation. New concrete has high levels of water concentration, which is blocking RF signals. This is even more likely to happen with higher frequencies. Even after drying up, concrete includes rebars, metal mesh, and other reinforcements that block signals and cause reflections that dissipate the signal. Concrete is usually used as a thick supportive layer that effectively, with rebars especially, is highly likely to block the whole signal.

Naturally, water rich Items like fish tanks, water fountains, ponds, and trees. Basically, anything containing highly absorbing material, such as water, stone, and other materials, is degrading the signal, so it no longer acts as in a vacuum or ideal environment and causes the signal to fade.

RF reflectors include, for example, metal objects in the area. Metal pans between floors, rebar, fire doors, air conditioning, heating ducts, mesh windows, blinds, metal mesh fences (depending on hole size), refrigerators, racks, shelves, and filing cabinets. Basically, anything metal that is located in the way of the signal. As an example, access points should not be installed between two air conditioning or heating ducts, as the ducts can block and function as reflectors, which block the whole signal or cause significant loss in it. Access points should always be placed below ducts to avoid RF disturbances from them.

RF interference sources include, for example, microwave ovens and other 2.4 GHz or 5 GHz emitting objects for Wi-Fi, Bluetooth, Zigbee, etc. devices that work in the 2.4 GHz frequency range. Other sources for other frequencies, such as cordless phones, cordless headsets, or other wireless devices that use the free spectrum of radio waves. All devices that function on the same frequency as the access point and the required equipment itself perform as interference. Transmitting at the same frequency can block the signal effectively. This affects especially freely usable frequencies but can also affect frequencies that are restricted to specific uses.

Destructive interference can also occur by the signal itself, with reflections and absorbing of the signal in such a way that two waves with the same amplitude phase shift by half of the wavelength and match up, canceling each other. This is called phase shift, which is the displacement of a waveform in time.

In mobile communication, absorbing may also be caused, for example, by weather conditions, multipath propagation, or the fact that the mobile station moves to a place where radio waves are shadowed behind an obstacle that prevents the signal from reaching the antenna directly.

So, in principle, all traffic without a clear line of sight is propagated through or by some media. A signal can also reach its destination via reflection from an appropriate surface or material. This makes the signal calculations difficult and even more difficult in a dynamic environment such as areas where there are moving parts, like robot arms and conveyor belts, that constantly alter the signal paths and reflections, so that the calculations done by the radio transmitters can be difficult and slow to adapt to changes.

4.2.1 Types of mediums in cleanrooms, case Bayer

In cleanrooms, the devices receiving the signal are typically within the machines. The antennas, or access points, will be located within the room. In some cases, even locating them in the next room can provide sufficient coverage, depending a lot on the medium of the walls. In most cases, the structure of the cleanroom wall will prevent signals from reaching the intended device, so the antennas need to be inside the same room where the usage is.

An optimal situation is when the access point or antenna is in the same room, or the device is within line of sight of the antenna. Even then, reflections of the signal can cause interference and degradation of the signal level.

In cleanrooms, the devices can be handheld devices, which are easier to manage (see picture 3. handheld tablet device), or devices gathering data within the production or other machine. These wireless devices that are inside the production machines are more difficult to manage since they can be deep within the manufacturing device and hence covered with metal, creating an additional layer of RF insulation to block the signal and in addition being in motion during operation.

Picture 3. Blueline cleanroom tablet

Handheld devices themselves can also be less optimized for wireless usage since most of the devices need to be enclosed so that they meet the cleanroom specifications. (See picture 4 of the enclosed cleanroom PC.)

In our environment, we have also found out that these enclosed devices are prone to overheating and thus breaking, causing disruptions. This causes the device itself to work in addition as a medium for the wireless signal and function as a reflector, diffractor, or scatterer.

Machines themselves can contain RF devices transmitting and receiving information within them. These machine radio networks can also provide additional RF interference to the network. Also, the other way around, they can be interfered with by outside signals and create functional errors. We have had examples of this with machines using Bluetooth connections in internal networks. This is why manufacturers need to follow URS (User Requirement Specifications) and inform us of all networks within the machines.

Cleanroom or cleanroom machine manufacturers do not consider wireless signals and designing radio environments as high priority or at all at the moment. This needs to be taken into consideration in the future, or at least leave room for antennas or other installation solutions as a reserve.

Picture 4. Systec cleanroom PC (tabletop enclosure)

In wall structures, stainless steel is not widely used without a coating. It is durable, easy to clean, and resistant to corrosion and chemical damage, but it is also easy to scratch and hard to fix, and the surface makes it difficult to install other equipment on it. It is often used in high-sterility areas. In addition, machines in the cleanroom are often made of stainless steel (see picture 4. of the cleanroom- approved stainless steel and glass enclosure).

Usually, walls are made of metal that is epoxy-coated, which provides a seamless and easy-to-clean finish, reducing contamination risk. Also, PVC (Polyvinyl Chloride) panels are used, which provide smooth, non-porous, and easy-to-clean surface areas. All of them are resistant to chemicals and microbial growth, which is essential. Bayer is using at Turku factories this kind of structure that has proven to be easy to maintain and clean.

Modular panels are used in most cases with smooth surfaces, metal or coated other materials, and minimal seams to reduce particle accumulation. Panels are changeable in case of damage or in case of changes are needed because of installations on them that caused structural damage. Floors are coated with polyurethane, epoxy, and other approved, easily cleanable materials that are also relatively wear-resistant and easy to fix.

Coated metal sheets are mostly used because, with reinforcements, the installation of equipment on them is easier than with softer PVC or other materials that otherwise could be suitable for cleanrooms.

Tempered glass windows are used as they are easy to clean and provide visibility without compromising the cleanroom's integrity. Also, in case of an accident, they are preferred for their ability to shatter without sharp edges. Workbenches and tables, are in most cases, also made with stainless steel, which is non-corrosive, easy to clean, and resistant to chemicals. It also provides a smooth surface that is easy to disinfect. Tempered glass, on the other hand, also provides a signal-blocking surface, especially when laminated or treated with a thin metal layer, so-called E-glass. (See picture 5 of the cleanroom layout with windows and furniture.)

Picture 5. Cleanroom view with PC installation mount on wall and Wi-Fi antenna on roof.

Storage cabinets and shelving are usually made of stainless steel, which is used because it is durable and easy to clean. (See picture 5. above.) Cleanroom chairs and stools are made with non-porous materials like vinyl or polyurethane and designed to minimize particle generation. They need to be easy to clean and resistant to chemicals and mechanical wear without emitting particles, which is the reason for most of the materials chosen.

The choice of materials for cleanrooms is critical to maintaining the necessary cleanliness levels and ensuring that the environment meets the needed standards for contamination control. These materials are selected based on their ability to minimize particle generation, resist chemicals, and facilitate easy cleaning, durability, and ease of maintenance.

Manufacturers do not provide any kind of information about the radio wave or signal passing capabilities of the materials that are used, which makes estimating and simulating the environment difficult.

Static environments in cleanroom areas consist of warehouse- or storage-type areas, although movement of materials can also change the room composition. Non-static environments consist of the production rooms that have moving machinery, materials, and personnel in the room that can change the signal passage.

5 Roaming

Webster´s New World Dictionary defines roaming to be: *“Travelling about, especially in search of adventure: Errant, roving, wondering.”*

In wireless networks, roaming is more commonly defined as extending the connectivity service of a network to a new region. (Greenlaw, Raymond., Goransson, Paul. 2011. 8-9)

It can be seen as mobility between base stations in wireless networks, or in simpler terms, roaming. It is a key element of wireless technology. IEEE standards define ways to roam in Wi-Fi networks. The ideal wireless network has seamless roaming without any major packet drops that are affecting the connection or disconnecting completely. Time-sensitive applications like voice or video roaming this is a critical component. Other applications may not be affected that much by roaming interruptions. That is why it becomes very important to take into consideration, when planning the network coverage, the roaming requirements of devices and applications on the wireless network. (Greenlaw, Raymond., Goransson, Paul. 2011. 29-62)

Wi-Fi roaming allows a device to move seamlessly between different Wi-Fi access points (APs) within the same network or between different networks. The mechanisms used to achieve this include Basic Service Set Transition (BSS Transition) which refers to the movement of a device from one AP to another within the same extended service set (ESS). This has been enhanced in Fast BSS Transition (FT), which is IEEE 802.11r standard that enables faster handoffs between APs by allowing pre-authentication and pre-association. Key technologies and protocols for Wi-Fi roaming also include IEEE 802.11k (Radio Resource Management), which helps devices quickly identify the best AP to connect to by sharing information about neighboring APs. IEEE 802.11v (Wireless Network Management) in turn provides mechanisms for better management of wireless networks, including aiding devices in making better roaming decisions.

Another technique often used is Hotspot 2.0 which is also known as Passpoint. This technology enables seamless and secure roaming between different Wi-Fi networks and is most often used in public Wi-Fi hotspots. (Greenlaw, Raymond., Goransson, Paul. 2011. 29-62)

Wi-Fi roaming is working by scanning. The device scans for available APs and measures signal strength. Then the device authenticates with the new AP and associates with it, often using protocols like 802.1X. There are mechanics like caching and pre-authentication that help speed up the process.

There are also challenges that need to be addressed. Switching between APs can cause brief interruptions and a little additional latency, which might affect applications sensitive to latency, like VoIP or video calls. They may break or have a glitch in them. In addition, ensuring secure transitions between APs without exposing the device to potential attacks is one of the challenges. This means that proper network configuration is required to support seamless roaming securely.

Roaming enables users to stay connected without manual intervention, maintaining ongoing sessions like calls or video streaming. When properly done, users do not need to reconnect manually when moving from one coverage area to another. This mobility is especially beneficial in enterprise environments, allowing employees and devices to move freely without losing connectivity.

Roaming on wireless networks in cleanroom areas is going to be one of the issues in planning the coverage. The main reason for difficulties is that in most cases, the access points cannot see each other properly or devices beforehand, so negotiation between the access points is going to be nonexistent. Also, the endpoints can´t “preconnect” to the access points since the metal walls will block the signal efficiently when there is no line-of-sight.
(Greenlaw, Raymond., Goransson, Paul. 2011. 63-99)

Bearing that in mind, while small cell sizes increase the capacity of the network and provide access to fewer devices at a time, they also raise the total cost of ownership (TCO) of the network.

This roaming will also be affected by different chipsets, since roaming capabilities can be tweaked on the devices with separate settings. The issue in cleanrooms also lies with the device itself. The cleanroom requires devices to be encased in easily cleanable materials so they can be cleaned. And of course, this encasing affects the signal strength for the device radio unless the antenna is built separately into the encasing itself, which it rarely is. Material can vary from stainless steel to plastic, which makes calculations difficult.

Wireless roaming is essential for providing a seamless user experience on both cellular and Wi-Fi networks. It requires robust infrastructure, well-defined protocols, and cooperation between network providers to ensure smooth and secure connectivity for users on the move.

6 Measuring and simulating the environment

Network simulation is a technique used to easily create a virtual representation of the network. This virtual representation can then be used for real installation purposes.

The radio environment in cleanrooms is demanding to simulate correctly. The normal simulations only take into consideration the wall structures and drawn static structures. This means that all dynamic environmental changes are left out of the equation. These simulations draw a 2-dimensional picture of the environment, which is sufficient for open environments, but usually the machine structure is dynamically affected along with moving pallets and boxes with their contents in the environment. Also, the wall structure in cleanrooms is non absorbing and either blocking or reflecting the signal, so in most cases, each room is a single-cell area for higher frequencies with low penetration capabilities. (See picture 6 of the example cleanroom physical layout.)

Picture 6. Cleanroom area separation

In Picture 6. above, the green area is for material and personnel flow, and the yellow area is the production area (classified cleanroom area) where wireless is needed.

We did all the simulations ourselves and used in our simulations mostly Aruba Airwave Planner, which provides a good simulation platform that can also be later used in network management and visualizing the network in real time. This later use in the deployment and management phases was one of the main reasons to use it. Other software was also tested and used, but Aruba software was the tool used in implementing the network installations.

The cleanroom structure with metal sheets has faraday cage capabilities, even though they were not intended nor needed in the design, because of the structure of the rooms that require no gas to be leaked.

Faraday cages, also known as Faraday shields or Faraday enclosures, are basically designed to block electromagnetic fields, including radio waves and other signals. They work based on the principles of electromagnetic shielding discovered by Michael Faraday. A Faraday cage is usually made from conductive materials such as metal, copper, or aluminum. In this case, there are two layers of thin metal (steel) sheets. (Lai et al., 2008, 2-5)

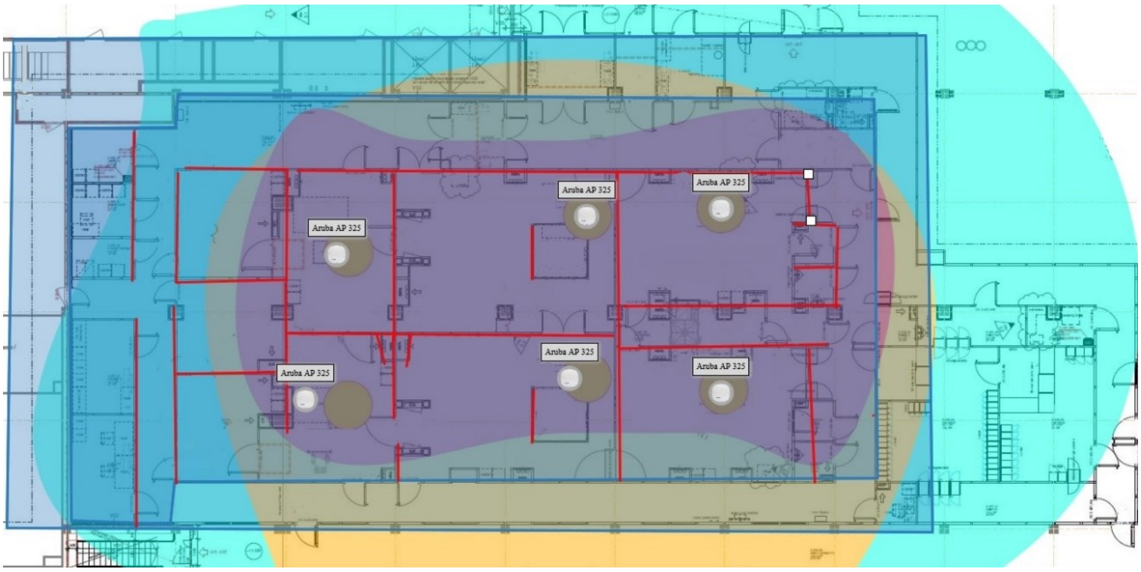
When an external electromagnetic wave, such as a radio wave or microwave signal, encounters the conductive material of the Faraday cage, it induces electric currents within the material. The induced electric currents flow through the conductive material of the cage in response to the incoming electromagnetic wave. These currents generate their own electromagnetic fields that are equal in strength but opposite in direction to the incoming wave. According to the principle of superposition, when two electromagnetic waves with equal strength but opposite directions meet, they cancel each other out. This results in an electromagnetic field of nearly zero inside the Faraday cage. As a result of this cancellation effect, any electromagnetic signals or radio waves that try to enter the Faraday cage are effectively blocked or attenuated, preventing them from reaching inside. (Lai et al., 2008, 2-10)

Faraday cage acts as a shield that isolates the inside from external electromagnetic interference. It is commonly used in various applications where electromagnetic isolation is required.

While Faraday cages are effective at blocking most electromagnetic signals, it is important to note that they are not perfect and have limitations. For example, extremely low-frequency electromagnetic fields (ELF) or very high-frequency signals may require specialized designs or additional measures for effectively blocking them. Additionally, any openings, holes, or gaps in the cage can allow signals to leak through. This means that even though the rooms seem ideal faraday cages, the signal can still penetrate the room and affectively work or disturb devices in the room. (Lai et al., 2008, 9-10)

With simulation, these areas can be planned to be covered with wireless access without the need to access the area physically. Simulation software, such as Aruba Airwave used in this case, allows you to specify wall materials to best fit the existing material attenuation and get a rough estimate for the access point installation plan.

In the physical installation phase, the places for the antennas and access points can move depending on the structure. Since in the simulation phase, ceiling structures cannot always be taken into consideration, since they are not in the blueprint, like lamp covers, fire detectors, sprinkler systems, and so on. Those structures can also affect the placement of the devices above the ceiling since devices in that area need to be accessible and installable as well.



Picture 7. Area in Picture 6. with planned Access points and walls simulated with 30-40dB attenuation.

In the picture above (Picture 7.), the area was installed with antennas that covered the whole area. Wi-Fi in production use was selected to use 5 GHz frequency since other devices use 2,4 GHz band in device networks and office networks. This also limits the signal coverage significantly. N+1 coverage was aimed for. N+1 is a commonly used term for the installation method of using a minimum number of devices and adding one for redundancy. It means that if one access point is down, other access points cover the area, so there are always two or more access points in one area. Full N+1 was not achieved since it would have required multiple access points per room. But with actual device tests, the rooms leaked enough signal to mostly achieve N+1 coverage in areas with reduced speeds. (Raza, Muhammad.; Wickramasinghe, Shanika. 2021)

The same area was covered with a 4G mobile network by a mobile operator with four antennas since a stronger signal and lower frequency were used by them.

In our tests, we found out that the cleanroom materials drop the signal level by 30-50 dB depending on the room structure, windows, doorways, and other unknown factors. So, we used a 30-40 dB attenuation as a baseline in simulations, which we found to be quite accurate in estimating the environmental aspects. This was used as our calibration number for the software that we used, which allowed us to use our own numbers and materials.

Picture 8. Simulation of a new cleanroom area with separate rooms for different production lines.

In simulation and installation, the purpose of the room is also vital to recognize. In the example area in picture 8, there are personnel gowning areas in the left lower corner that require no connectivity, but other areas are vital to cover. In this case, simulation showed that with 18 antennas, the whole area can be covered in most cases with redundancy (N+1).

We also did simulations for various scenarios, such as peak usage times, different device densities, removing access points as a breakage or maintenance effect, and varying levels of interference, to test network robustness.

6.1 Key Metrics in simulation and actual network quality measurements

These metrics are used and combined to create more accurate simulation results to be used when installing the network. Simulation software creates a visual image with the help of an estimation of these metrics within the floor maps to help with locating the best places for the access points. (See pictures 7 and 8.)

The received signal strength indicator (RSSI) measures the power level received from the access point or base station. This is usually measured at the client end, but it can also be measured from the access point or base station. It is easier to move the device and gather signal information on the receiving end. This is usually the case in already-deployed networks. (Rappaport, 2002, 406)

Signal-to-noise ratio (SNR), which means the ratio of the signal power to the noise power, says that the higher the SNR value, the better the signal quality is. This measurement also indicates an outer disturbance in the network. (Rappaport, 2002, 365)

The actual data transfer rate achieved over the network gives a good indication of network quality. This data transfer rate is typically measured in Mbps. There are usually requirements for minimum throughput that need to be met with access point density and quality. These requirements depend on the application.

Latency, or delay in other sources, measures the time it takes for a data packet to travel from its source to its destination. This is measured in milliseconds. Latency is not usually an issue, except if there are specific applications involved. Long latencies in data transfer are usually caused by other network issues, such as low RSSI, low SNR, or other interference.

Packet loss measures the percentage of packets that are lost during transmission, impacting the reliability of the connection. This causes TCP retransmissions or lost UDP connections. This is also commonly related to other network issues. Latency and packet loss often go hand in hand when issues emerge.

Interference measurement means the assessment of other signals or noise in the design area that may affect the performance of the network. Usually, other signals have the same frequency or even the same technology in the area that can be isolated. SNR can also indicate issues in this.

These metrics, in combination, provide comprehensive information in the area to provide heatmaps that can work as baselines in AP installation. Of course, simulation can´t take into consideration all the environmental issues and can only work as a rough guideline for access point amounts and locations.

7 Analysis and results

While the need for wireless coverage in cleanroom areas is growing, there are difficulties in building high-speed and low-latency networks into the areas, or even low-speed sensor data networks. The materials used to build such rooms provide very difficult environments for RF frequencies to be efficiently designed in them.

In most cases, the equipment within the rooms also provides dynamic environments for radio waves to travel in. Equipment is encased in metal structures, and all user equipment (PC, controlling equipment, PLC, logics) is encased in metal structures that effectively prevent radio frequencies from traveling. So, they function as a faraday cage within a faraday cage. To provide access to machines encased in cleanrooms, it will be even more difficult to provide sufficient access.

Wireless coverage in cleanroom environments presents some challenges due to the strict environmental controls and the need to maintain cleanliness in the room. This also limited the usage of certain equipment in the area because the devices did not meet the requirements.

There are ways to mitigate the issues. The materials used in the construction of cleanrooms impact wireless signals, which cannot be changed. Metal materials, painted metals, or coatings, which are best for cleanliness and maintaining the room contaminant-free, can interfere with signal propagation and even block it completely. To avoid this, in building or planning, the materials used inside rooms can be chosen so that they minimize signal absorption and reflection. In most cases, those materials are plastic or glass, which do not have other needed qualities for cleanroom status. This results in other ways to bring the needed signal closer to users.

Measuring and simulating indoor wireless networks involves using specialized tools and software in order to sufficiently assess and optimize performance. A combination of real on-site measurements along with good simulations and designs can be made for reliable wireless connectivity in measured environments. This is really important to tackle the challenges in complex and various cleanroom environments.

Good consideration and planning should be given to the placement of wireless transmitters, access points, and antennas. Depending on the cleanroom design, installation of access points outside the cleanroom and directional antennas can be used. This, of course, helps in contamination prevention, but also presents issues if walls prevent signal. One way to use antennas is to install the access point or RF source outside of the room and only present the antenna in the room. This, of course, requires special antennas and need a hole to cleanroom structure, which is always a bad thing to do, and installation into the rooms.

This is the way that we have chosen to bring the Wi-Fi signal in the Turku facility to cleanroom areas. It is necessary to conduct a site survey to determine the optimal placement of access points and ensure adequate signal strength throughout the cleanroom areas.

In some cleanroom devices, electronic equipment may be used that emits electromagnetic interference (EMI) or that uses RF within the manufacturing devices. It needs to be ensured that the wireless equipment operates on “free” frequencies that are not interfering with other devices within the cleanroom. This is something that can be mitigated with measurements and specific RF plans for the environment.

Cleanrooms are categorized based on the required level of cleanliness. The classification affects the types of materials and equipment that can be used. It is a requirement for any wireless equipment that it meets the standards for the specific cleanroom classification. This often means enclosing wireless equipment in protective enclosures to prevent contamination, provide a cleanable surface, and meet required standards.

It is important to regularly inspect and maintain the wireless infrastructure to ensure that it meets cleanroom requirements. All maintenance, service, or replacement should be done so that it minimizes the risk of introducing contaminants. In most cases. equipment that is installed on walls or ceilings and is removed from the room or replaced, causes the room to lose its status, and the room needs to be cleaned and measured for air tightness and bacterial growth tests to be conducted.

Also, security is a critical concern; all wireless networks need to be secured to prevent unauthorized access, especially in cleanroom environments where sensitive processes or data is handled. It is important to work closely with cleanroom design and maintenance experts, as well as wireless network specialists, to create a solution that meets both cleanliness and connectivity requirements. Additionally, adherence to industry and local standards and regulations is crucial to ensuring a successful wireless implementation in cleanroom environments.

In addition to the above, hardware used for installation in cleanrooms needs to be able to handle the cleaning of them with different chemicals, in most cases alcohol-based solvents. Many manufacturers declare that their equipment is cleanroom certified and can withstand the cleaning, but they also need to withstand the chemicals in liquid form to be wiped around them. And in addition, they cannot produce surfaces that cannot be wiped easily (below ceiling installation) that may gather dust or other materials and drop as bigger particles onto production machines or directly to the product.

7.1 Case: Bayer Finland implementations

At Bayer, we have implemented and tested two different techniques for cleanroom areas. Wi-Fi and 4G. Wi-Fi has been implemented with an antenna solution for production, and a 4G mobile network has been tested in demo production areas. Wi-Fi was chosen because it could be installed and implemented in existing structures with minor changes, and there was a lot of existing equipment available and already tested. Especially in warehouse operations, it was already used with handheld scanners, which were the initial expansion needs that were a running factor in the project.

These two technologies were chosen because they provide a wide selection of endpoint devices that are easily available from most manufacturers and have proven to have a long lifetime expectancy and easy upgradeability for future technologies. The requirement for low latency and speed was ruling out other IOT network solutions.

The Wi-Fi implementation was installed for production use after testing it in the IT department and getting approvals for the antenna installation procedure and the antenna itself from the validation department.

Devices and antennas were also chosen according to company policies and according to cleanroom specifications and requirements. The antenna itself can be used with multiple devices since it uses standard connectors. So even if the device manufacturer changes, antennas can be re-used with them. Also, other manufacturers provide similar solutions that can be used with them. Antennas can also be ATEX-compliant because they are gastight, passive equipment and can be installed in areas that require ATEX compliant installation. “ATEX” derives from the ATEX Directive and is short for “Atmospheres Explosibles.” It consists of European Union regulations that are designed to ensure the safety of products being used in environments that contain explosive materials or gases. (EU Directive 94/9/EC, 1994).

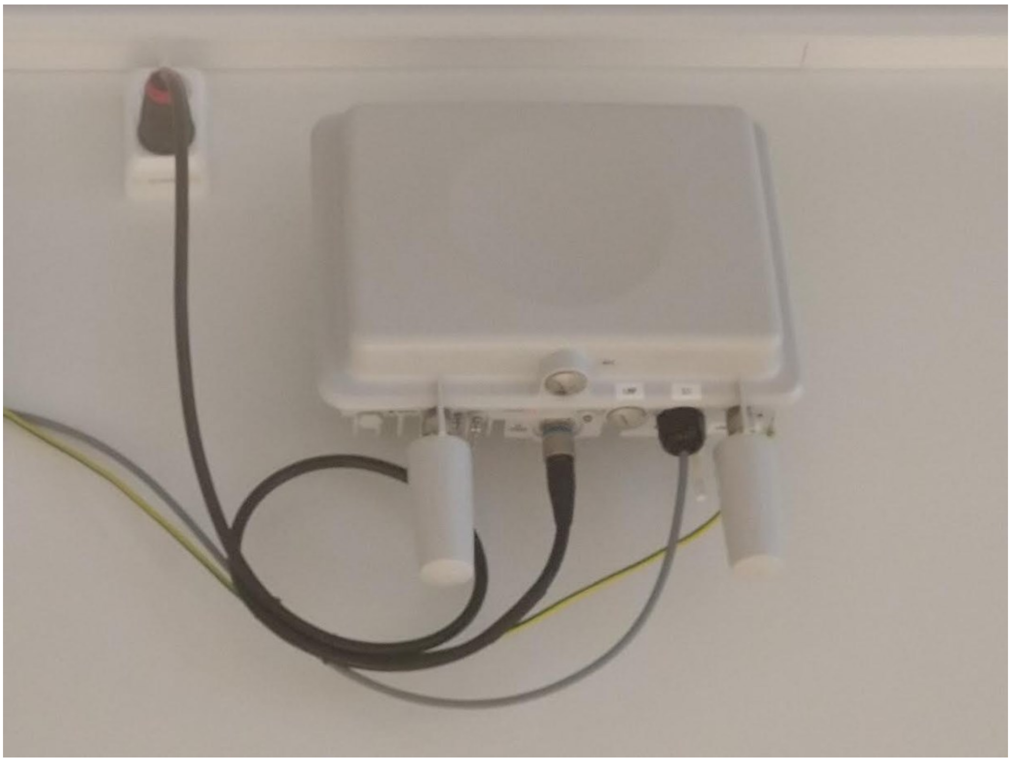
The simulations proved to be quite accurate with the antenna solution chosen (see picture 9.). After initial installations, we were able to do tests on the first installation areas during the maintenance break, when we were able to go to the cleanroom area with limited equipment.

Picture 9. Aruba AP-ANT-40

Our tests of wall structure attenuation in simulation use proved to be rather accurate, and due to windows, doorways, and other structural leaks, the signal levels were almost identical to simulations in adjoining rooms as well. Of course, this maintenance break was lacking the actual materials, movement, and personnel in the rooms, which was taken into consideration. This test phase was sufficient to do full coverage installations according to simulations and to trust the simulation as a source for antenna location documentation for the installation phase.

This comparison between simulation and actual results was done with a handheld device and a measurement laptop. It was done in a few locations only due to cleanroom access limitations and only documented as a note to installation documents internally at Bayer.

The 4G network was also tested, measured, and installed in selected test locations with Nokia and Verizon technicians. (See picture 10. of the example installation.) The frequency range was requested and reserved from Traficom to 2300-2320 MHz range for indoor use. 4G proved in tests to limit the speed according to the frequency (20 MHz) to the maximum speeds of 20-60 Mbps, which was enough for most applications, but proved slow for larger documents, files, and especially picture handling.



Picture 10. Nokia 4G outdoor AP

As in the example above in picture 10, the device itself is IP65 and even outdoor compliant, so it is suitable for cleanrooms from a chemical perspective, but it provides surfaces and cabling that are extremely hard to keep particle-free, which reduces its usability unless the AP itself can be installed outside and antennas brought to the area needed. This method has been used at the Bayer factory to bring normal mobile network coverage to cleanrooms for emergency phone usage at the Bayer facility in Turku.

8 Conclusion

This thesis handled Bayer decisions made to eventually build a Wi-Fi network into both factories to cover the needs as a result of tests and studies of usage.

The results of the technology decision were made based on equipment availability and costs. Wi-Fi was chosen since it is most widely supported by all manufacturers, and antenna solutions for a cleanroom environment were available.

4G and, to some degree, 5G technologies were also tested, but the total cost of ownership for full factory coverage would have risen too high. In addition, the limitation on private frequencies to only one reasonably usable band allowed in Finland limited the use cases so much that it was ruled out of full coverage installation. The network is still under testing for other applications.

In the installation phase, we discovered that the actual places for the antennas and access points needed to move depending on the structure. In the simulation phase, all structures cannot always be taken into consideration since they are not in the blueprint. Examples were lamp covers, fire detectors, sprinkler systems, and other structures in rooms. Other structures can also affect the placement of the devices above the ceiling since devices in that area need to be accessible and installable as well. This caused the places specified for installation to be flexible, and instructions were given by us to subcontractors and our own electricians to use best practices in installation and to find the best possible location within a few square meters for devices.

This resulted in additional documentation and simulations with actual installation places to be done after the revised blueprints of the places was available. Despite this, all access points and antennas were successfully installed in places, and this caused no harmful effects on the network coverage.

As a result, we successfully had full coverage of all necessary areas in the old factory without significant issues. In the new factory, where the use of the network is still pending in some areas, we have the network infrastructure already installed and approved for use according to experiences gained from other site.

These results of planning and installation can be applied to any cleanroom wireless network planning and implementation as-is. This thesis will be presented to the Bayer organization as a reference on how to plan and build a wireless network in cleanroom areas successfully.

This thesis could serve as a background for further study on how other techniques could be implemented in similar environments. Since there were no similar studies made, this could benefit other future technology implementations for such applications.

References

British FibreOptic Industry Association. Optical Fibers Explained. https://www.fia-online.co.uk/media/d4bjmhhb/ufo.pdf. Retrieved 13.11.2023.

Clark, Kristen.; Nordrum, Amy. 27.1.2017). Everything you need to know about 5G. IEEE Spectrum magazine. Institute of Electrical and Electronic Engineers. https://spectrum.ieee.org/everything-you-need-to-know-about-5g. Retrieved 17.1.2024.

Cleanroom and Controlled Environment Attire - ANSI Blog. 2015. The ANSI Blog. 2015-07-15. https://blog.ansi.org/cleanroom-and-controlled-environment/. Retrieved 24.5.2024.

Dahlman, Erik.; Parkvall, Stefan.; Sköld, Johan.; Beming, Per. 2007. 3G Evolution HSPA and LTE for Mobile Broadband, Elsevier, 2007

Didcott, Paul G. 6.6.2004. Bluetooth: Global Certification Requirements. https://blueradios.com/Bluetooth_Global_Certification_Requirements.pdf. Retrieved 14.11.2022.

Elliott, Barry J. 2000. Cable engineering for local area networks, Woodhead publishing Ltd. England

Elliot, Barry J. 2018. Designing a Structured Cabling System to ISO 11801. CRC Press, USA

Ethernet Media Standards and Distances, https://kb.wisc.edu/ns/page.php?id=7829. Retrieved 16.11.2023.

EU Directive 94/9/EC. 1994. https://www.ipu.co.uk/wp-content/uploads/2014/07/ATEX-EU-Directive-94-9-EC.pdf. Retrieved 14.5.2024

Frenzel, Lou. 29.3.2012. What's The Difference Between ZigBee And Z-Wave? Electronic Design. https://www.electronicdesign.com/technologies/communications/article/21796052/whats-the-difference-between-zigbee-and-z-wave. Retrieved 14.11.2023

Generational Wi-Fi User Guide. https://www.wi-fi.org/system/files/Generational_Wi-Fi_User_Guide_202304.pdf. Retrieved 12.4.2024.

Greenlaw, Raymond.; Goransson, Paul. 2011. Secure Roaming in 802.11 Networks. England. Elsevier Science.

Gupta, Naresh. 2016. Inside Bluetooth Low Energy, Second Edition. Boston, USA. Artech House

Information Technology--Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks--Specific Requirements Part 11: Wireless LAN Medium

Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Std 802.11-2020. https://doi.org/10.1109/ieeestd.2012.6361248. Retrieved 10.11.2023.

ISO 14644-1:2015. - Cleanrooms and associated controlled environments -- Part 1: Classification of air cleanliness by particle concentration. 2015-2021. https://doi.org/10.3403/30152866. Retrieved 21.2.2024.

Kadia, Hema. 2024. 5G Networks: Everything you need to know about 5G. TeckNexus. https://tecknexus.com/5g-network/5g-networks-know-about-5g/. Retrieved 17.6.2024

Kallioniemi, Tapio. (10. 11 2009). Zigbee Standardin Toiminta ja Periaatteet. https://urn.fi/URN:NBN:fi:amk-201005078375

Kozicki, Michael.; Hoenig, Stuart.; Robinson, Patrick. 2012. Cleanrooms: Facilities and Practices. Netherlands: Springer Netherlands

Lai, Andrea.; Lam, Sandra.; Navara, Rachita. 2006. A Faraday Cage Exploration: Final Report and Project Assessment. https://wiki.laptop.org/mediawiki/images/3/3f/Faraday_Cage_Activity.pdf. Retrieved 19.6.2024.

LoRa Alliance. 2021. What is LoRaWAN® Specification. 2021. https://lora-alliance.org/about-lorawan/. Retrieved 18.11.2022.

Nokia. 2021. 5G Spectrum bands explained. https://www.nokia.com/networks/insights/spectrum-bands-5g-world/. Retrieved 13.11.2022.

Park, Ju-Min.; Li, Kenneth. 5.4.2019. South Korean, U.S. telcos roll out 5G services early as race heats up. https://www.reuters.com/article/idUSKCN1RF0KH/. Retrieved 14.1.2024.

Ramstorp, Matts. 2008. Introduction to Contamination Control and Cleanroom Technology. Weinheim, Germany. Wiley-VCH

Raza, Muhammad.; Wickramasinghe, Shanika. 30.8.2021. N-Modular Redundancy Explained: N, N+1, N+2, 2N, 2N+1, 2N+2, 3N/2. https://www.bmc.com/blogs/n-n1-n2-2n-3n-redundancy/. Retrieved 12.5.2024.

Rappaport, Theodore. 2002. Wireless Communications: Principles and Practice. Hoboken, USA: Prentice Hall

Sheriff, Robert E. 1996. Understanding the Fresnel Zone. Explorer, Geophysical corner. https://www.searchanddiscovery.com/documents/geophysical/sheriff/images/sheriff.pdf. Retrieved 10.2.2024.

Technical Air Products. 2021. What are the benefits of modular cleanrooms?. https://www.technicalairproducts.com/2021/02/13/benefits-modular-cleanrooms/. Retrieved 16.6.2024.

Traficom. 2023. Local 4G/5G networks. https://www.traficom.fi/en/communications/communications-networks/local-4g5g-networks. Retrieved 18.6.2024.

Vilches, Jose. 29.4.2010. Everything You Need To Know About 4G Wireless Technology, TechSpot. https://www.techspot.com/guides/272-everything-about-4g/. Retrieved 16.10.2022.

Woolley, Martin. 2019. Bluetooth 5 / Go Faster. Go Further. https://www.bluetooth.com/wp-content/uploads/2019/03/Bluetooth_5-FINAL.pdf. retrieved 11.11.2023.

What is SigFox? LinkLabs. 12.2.2015, https://www.link-labs.com/blog/what-is-sigfox. Retrieved 15.11.2022.

Whyte, William. 2001. Cleanroom Technology: Fundamentals of Design, Testing and Operation. England. John Wiley & Sons.

Wi-Fi Generation Numbering. ElectronicNotes. https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/wifi-alliance-generations-designations-numbers.php. Retrieved 10.11.2021.