Protection of critical infrastructures in Smart Cities enviroments: risk analysis and resilence strategies

Joan Sala Granyer

Abstract– Smart Cities increasingly rely on connected digital infrastructures to manage essential services such as energy, water, transport, healthcare and emergency response. This digital transformation improves urban efficiency, but it also increases the attack surface and creates new technological dependencies. This work analyses vulnerabilities in critical infrastructures within Smart City environments and focuses on a specific case study: Bluetooth Low Energy (BLE)-based indoor positioning systems in smart hospitals. Based on a literature review, real incident analysis and threat modelling, a multilayer security architecture is proposed to improve the resilience, availability and reliability of these systems.

Keywords– Smart Cities, critical infrastructures, cybersecurity, smart hospitals, indoor positioning, BLE, IoT, resilience.

1 Introduction and work context

Smart Cities represent an evolution of the traditional urban model through the integration of digital technologies in the management of public services. IoT sensors, communication networks, industrial control systems, data platforms and intelligent applications make it possible to optimise processes related to urban mobility, energy, water, transport, healthcare, emergency response and public building management.

This transformation offers clear advantages. A connected city can monitor traffic in real time, optimise energy consumption, detect incidents in water networks and improve the coordination of public services. However, the same connectivity that improves efficiency also introduces new risks. The more systems are connected, the greater the dependence on digital networks and the higher the probability that a technical failure or a cyberattack may have physical consequences.

The problem is particularly relevant when the affected systems are part of critical infrastructures. An interruption in the power grid, water supply, telecommunications network or healthcare system can directly affect public safety and social well-being. In this context, cybersecurity can no longer be considered only an IT issue, but rather a fundamental requirement to ensure the continuity of essential urban services.

• *Contact e-mail:* joansagra@gmail.com
• *Supervised by:* Angeles Vazquez
• *Academic year 2025/26*

Within critical infrastructures, smart hospitals are a particularly sensitive case. These facilities increasingly use connected devices, monitoring systems, management platforms, medical sensors and location-based services. A hospital may use indoor positioning systems to guide patients inside the building, locate healthcare staff, find medical equipment, improve response times and optimise internal workflows. If these systems are manipulated or become unavailable, organisational errors, delays and loss of operational visibility may occur.

For this reason, this work focuses on the vulnerability analysis of BLE-based indoor positioning systems in smart hospitals. The aim is not to perform a real audit of a hospital infrastructure, but to study the most relevant threats, assess their impact and propose a security architecture capable of reducing the identified risks.

The general objective of this work is to analyse the vulnerabilities of BLE-based indoor positioning systems in smart hospitals and to propose a security architecture that improves their resilience and reliability within the context of Smart Cities.

The specific objectives are: to study the role of critical infrastructures in Smart Cities; to identify specific threats such as spoofing, replay, relay, jamming and RSSI manipulation; to evaluate their impact in a hospital environment; and to propose a multilayer security architecture including measures at device, network, data processing, application and monitoring levels.

The paper is organised as follows. First, the technological framework and state of the art are presented. Then, the methodology is described. Next, real incidents affecting critical infrastructures are analysed and the analysis is

applied to the case of indoor positioning in smart hospitals. Finally, a security architecture is proposed, the results are discussed and the main conclusions are presented.

1.1 Scope of the work

The scope of the work is limited to the conceptual and technical analysis of threats affecting indoor positioning systems in smart hospitals. No physical deployment or real audit of a hospital infrastructure is carried out. The work does not attempt to demonstrate the practical exploitation of vulnerabilities, but rather to study how they could affect the system and which measures could reduce their impact.

The work covers four main elements. First, the context of Smart Cities and critical infrastructures. Second, the analysis of real incidents showing how cyberattacks can affect essential services. Third, the threat modelling of a BLE indoor positioning system. Finally, the proposal of a secure architecture that may serve as a reference for a more robust design.

The implementation of a full infrastructure, experimental validation in a real hospital and a quantitative comparison of different positioning technologies are outside the scope of this work. Nevertheless, a scenario-based discussion is included to avoid a purely theoretical approach. This delimitation allows the thesis to focus on a concrete contribution: linking cybersecurity threats with indoor positioning systems in critical healthcare environments.

2 STATE OF THE ART AND TECHNOLOGICAL FRAMEWORK

2.1 Smart Cities and critical infrastructures

Smart Cities are cities that use digital technologies to manage their services more efficiently. However, not all services have the same relevance. Some of them are considered critical infrastructures because their disruption would directly affect the basic functioning of society. These include energy, water, transport, telecommunications, healthcare, emergency response and public safety [1].

In a smart city, critical infrastructures are increasingly interconnected. This interconnection enables real-time data collection and improves decision-making, but it also creates new dependencies. For example, a smart hospital may depend on the power grid, connectivity, databases, management systems and IoT devices. If one of these elements fails, the impact may spread to related services.

Protecting critical infrastructures in Smart Cities requires both technical and organisational measures. It is not enough to deploy sensors or digital platforms; protection mechanisms, continuity plans and incident response procedures are also necessary. Therefore, resilience becomes a central concept. A resilient system is not a system that never fails, but one that can resist, detect, respond to and recover from incidents with minimal impact.

2.2 IT/OT systems

One of the main changes introduced by urban digitalisation is the convergence between IT and OT systems. IT systems are oriented towards information management, servers, databases, applications and communications. OT systems, in contrast, control physical processes such as electricity, water, building climate systems, transport or technical equipment.

Traditionally, OT systems were more isolated and were not always connected to external networks. However, the need for remote supervision and optimisation has led many OT systems to be integrated with corporate networks and management platforms. This enables more efficient operation, but also increases the attack surface. An intrusion that begins in the IT network may eventually affect physical processes if segmentation and access control are insufficient [4].

In a smart hospital this convergence is very clear. Administrative systems, medical networks, maintenance platforms, connected devices, climate systems and location services may coexist within the same organisation. If they are not properly separated, an incident in an auxiliary system may facilitate access to more critical systems.

2.3 IoT in Smart Cities

The Internet of Things connects physical objects to digital networks so that they can collect, send or process information. In Smart Cities, IoT devices are used to monitor traffic, energy consumption, environmental quality, security, transport and healthcare services. Examples include traffic sensors, cameras, air-quality sensors, beacons, occupancy sensors, connected monitors and medical devices.

These devices provide useful information, but they also create security challenges. Many of them have limited processing capacity, use weak passwords, are difficult to update or rely on exposed wireless communications. In addition, in large environments such as hospitals or cities, the number of devices can be very high, which makes inventory, maintenance and supervision more complex.

In smart hospitals, IoT devices may include medical sensors, monitoring systems, wearable devices, location tags and BLE beacons. If these devices are not properly protected, they can become entry points for attackers or generate incorrect information for hospital management systems.

2.4 Indoor positioning systems

Indoor positioning refers to the set of techniques used to estimate the position of people, devices or objects inside buildings. Unlike outdoor environments, where GPS is usually the main technology, indoor accuracy decreases due to walls, ceilings, obstacles and the lack of direct satellite visibility.

For this reason, alternative technologies such as BLE, WiFi, RFID, UWB and inertial sensors are used. Each technology has advantages and limitations. WiFi can reuse existing infrastructure, RFID is useful for asset identification, UWB provides higher accuracy and BLE stands out for its low cost, low energy consumption and easy deployment. This work focuses on BLE because it is suitable for hospital positioning systems and compatible with mobile devices [11].

2.5 BLE, RSSI and trilateration

In a BLE-based positioning system, the beacons installed in the building periodically transmit signals. Receiver devices, such as smartphones or tablets, detect these signals and record their strength, known as RSSI. Based on the received signal strength, the approximate distance between the receiver and the beacons can be estimated.

When information from several beacons is available, an approximate position can be calculated using trilateration. However, this process has limitations. RSSI varies due to walls, people, interference, furniture and environmental changes. Moreover, since BLE signals are wireless, they can be manipulated, replayed or spoofed. Therefore, security and data validation are key elements for system reliability [9, 10].

2.6 Smart hospitals and RTLS

Smart hospitals are healthcare environments where digital systems support clinical, logistical and administrative processes. Their objective is not only to introduce technology, but to improve patient flow, reduce waiting times, optimise the use of resources and increase the capacity to respond to incidents. In this context, real-time location systems (RTLS) are particularly useful because hospitals are complex buildings with many floors, corridors, rooms, restricted areas and mobile assets.

An RTLS can be used to locate infusion pumps, wheelchairs, beds, defibrillators or portable diagnostic equipment. It can also support staff coordination and guide patients or visitors through the building. These functions are not always directly clinical, but they may influence the quality of service. For example, if a nurse cannot quickly find a required device, the time needed to attend a patient may increase. For this reason, location systems should be considered part of the operational infrastructure of the hospital.

The main challenge is that RTLS data must be reliable. A wrong location may be less visible than a complete system failure, but it can still produce operational consequences. Therefore, an indoor positioning system must be analysed not only from the point of view of accuracy, but also from the point of view of integrity, availability and resilience.

2.7 Comparison of indoor positioning technologies

Although this work focuses on BLE, it is useful to compare it with other common indoor technologies. WiFi can exploit existing infrastructure, but its accuracy depends on the density of access points and signal stability. RFID is useful for identification and asset control, although it does not always provide continuous positioning. UWB provides high accuracy but usually requires a higher deployment cost. Inertial sensors can complement other technologies, but they accumulate error over time.

The choice of BLE is based on a balance between cost, ease of installation and compatibility with mobile devices. However, this choice also determines the security architecture. Since the system depends on wireless signals and RSSI estimations, it requires validation, filtering and anomaly detection mechanisms to prevent manipulated signals from becoming accepted positions.

Table 1: COMPARISON OF INDOOR POSITIONING TECHNOLOGIES

Tech.	Advantage	Limitation
BLE	Low cost and low energy	Unstable RSSI and possible spoofing
WiFi	Existing infrastructure	Variable accuracy
RFID	Useful for assets	Limited range
UWB	High accuracy	Higher cost
Inertial	No fixed radio needed	Accumulated error

3 METHODOLOGY AND DEVELOPMENT PROCESS

The methodology is structured in several phases so that the analysis is not only descriptive. The first phase consists of a bibliographic and technical review of Smart Cities, critical infrastructures, industrial cybersecurity, IoT, BLE, indoor positioning, smart hospitals and real cyberattack cases.

The objective of this phase is to build a theoretical basis for understanding both the operation of intelligent infrastructures and the threats that may affect connected systems. The review includes academic sources, technical reports, institutional documentation and references related to security in industrial and healthcare environments.

The second phase consists of analysing real cases. Incidents affecting critical sectors such as energy, water, fuel transport and healthcare were selected. Each case is analysed according to five elements: affected infrastructure, attacker entry point, exploited vulnerability, impact and lesson applicable to this work.

The third phase defines the system under study. A smart hospital is considered, with BLE beacons installed by zones, patients or staff using mobile devices, a positioning server, a navigation application, the hospital WiFi network and a monitoring system. This model makes it possible to analyse specific threats in a realistic environment without physically deploying the infrastructure.

The fourth phase consists of threat modelling. For each threat, the description, method, exploited vulnerability, impact, risk level and mitigation are analysed. This approach connects technical threats with real operational consequences, such as loss of accuracy, service interruption, incorrect routes or difficulties in locating medical equipment.

The fifth phase is the risk assessment. A qualitative matrix based on probability and impact is used. Probability represents how likely or feasible a threat is, while impact represents the consequences for hospital operation. This assessment helps prioritise the most relevant threats and justifies the proposed architecture.

Finally, a secure multilayer architecture is developed. This architecture is designed according to the identified threats and is organised into physical, network, processing, application and monitoring layers. The result is evaluated by comparing a basic system with a protected system.

In order to make the methodology more transparent, the analysis follows a simple but consistent evaluation criterion. Each identified threat is first described technically, then linked to a specific vulnerability and finally evaluated according to its expected effect on hospital operation. The aim is not to obtain an exact numerical value, because this would require a real deployment and measurements, but to provide a structured comparison between the basic system and the protected system.

The risk score used later in the results is based on the product of probability and impact. Both dimensions are estimated on a scale from 1 to 5. A threat with high probability and high impact receives a higher score, while a threat that is unlikely or has limited consequences receives a lower score. This approach is simple, but it is useful for prioritising threats and for showing the effect of the proposed countermeasures.

4 Analysis of real cases

To better understand the risks associated with critical infrastructures in Smart City environments, it is useful to analyse real incidents that have affected essential services. These cases make it possible to identify common vulnerability patterns, such as lack of network segmentation, insecure remote access, absence of strong authentication, outdated systems or excessive dependence on digital systems.

4.1 Attack on the Ukrainian power grid

The 2015 attack on the Ukrainian power grid is one of the best-known cases of a cyberattack against a critical infrastructure with direct physical consequences. The affected infrastructure was the electricity distribution system, specifically several regional power companies.

The attackers initially gained access to corporate networks through phishing e-mails targeting employees. From this initial access, they moved laterally inside the network until they reached systems related to power grid operation. The attack combined remote access, malware and manipulation of industrial control systems [12].

The main exploited vulnerability was the connection between corporate networks and operational systems. Although industrial systems should be protected and separated, the attack showed that an intrusion into the IT side can end up affecting physical processes. It also revealed insufficient controls to prevent lateral movement and unauthorised remote access.

The main lesson for this work is that digital systems controlling physical infrastructures must be designed with clear network separation, strict access controls and recovery capabilities. In a smart hospital, this is especially important because an apparently secondary system, such as indoor positioning, could become an entry point if not properly protected.

4.2 Oldsmar water treatment incident

The Oldsmar case affected a water treatment plant in Florida. The affected infrastructure was the control system responsible for regulating certain chemical parameters of drinking water.

According to initial reports, the attacker accessed the system through a remote access tool used to manage plant equipment. Once inside, the attacker attempted to modify the sodium hydroxide level, a substance used in water treatment. The change was quickly detected by an operator and reverted before it had real consequences for the population [13].

The main vulnerability was insecure remote access. These tools may be useful for maintenance and supervision, but if they are not properly protected, they can become an entry point for attackers. Common problems in small critical infrastructures were also observed, such as limited resources, weak configurations and absence of advanced controls.

The lesson for this thesis is that any connected system must include robust authentication, access control and monitoring. In a smart hospital, this means that indoor positioning systems should not be directly exposed or managed through insecure remote access tools.

4.3 Colonial Pipeline ransomware attack

The Colonial Pipeline attack affected one of the main fuel transport infrastructures in the United States. Although the attack mainly targeted corporate IT systems, the company temporarily halted pipeline operations as a precaution.

The attackers used ransomware to encrypt organisational systems. The initial access was related to compromised credentials and remote access that lacked sufficient protection. This case is especially relevant because it shows how an attack on IT systems can indirectly affect a physical critical infrastructure [14].

The exploited vulnerability was mainly the lack of multifactor authentication in certain remote accesses, together with high dependence on digital systems. Even if OT systems were not necessarily directly compromised, uncertainty about the scope of the attack forced the operation to stop.

The lesson for this work is that critical infrastructures need continuity plans and clear segmentation between systems. Applied to smart hospitals, an attack on an auxiliary system should not compromise other critical services. For example, a failure in the indoor positioning system should not affect medical networks, administrative systems or clinical equipment.

4.4 WannaCry and healthcare impact

The WannaCry ransomware affected organisations in many countries, but one of the most significant impacts occurred in the British healthcare system. The affected infrastructure was the IT system of hospitals and health centres, especially equipment and services dependent on vulnerable systems.

The attack spread by exploiting a vulnerability in unpatched systems. Once infected, the ransomware encrypted files and blocked normal system operation. This affected the availability of information and digital services needed for daily healthcare activity [15].

The impact was particularly relevant because appointments and procedures had to be cancelled or delayed, and normal hospital operation was disrupted. This case shows

Table 2: COMPARISON OF REAL CASES IN CRITICAL INFRASTRUCTURES

Case	Affected infrastructure	Attacker entry	Exploited vulnerability	Impact	Lesson for the thesis
Ukraine 2015	Power grid	Phishing and remote access	IT/OT connection and insufficient segmentation	Blackouts and affected users	Separate networks and protect operational systems
Oldsmar 2021	Water plant	Remote access	Poorly protected remote control	Risk to water quality	Authentication and access monitoring
Colonial Pipeline 2021	Pipeline	Compromised credentials	Lack of MFA and IT dependence	Operational shutdown and supply problems	Service continuity and segmentation
WannaCry 2017	Hospitals	Malware exploiting vulnerability	Outdated systems	Cancelled appointments and disrupted service	Updates, resilience and response plans

that, in healthcare, system availability is as important as data confidentiality.

The lesson for this thesis is direct: in smart hospitals, cybersecurity must be considered a basic operational requirement. Indoor positioning systems, even if they are not primary clinical systems, may affect internal coordination, asset management and emergency response. Therefore, they must include updates, segmentation, monitoring and recovery mechanisms.

4.5 Lessons learned from the cases

The previous cases show that critical infrastructures can be affected by different types of attacks, but they also reveal common patterns. In all cases, weaknesses related to insecure access, lack of updates, insufficient segmentation or inadequate monitoring are present.

From this comparison, it can be concluded that critical infrastructure security does not depend on a single technology, but on a combination of technical, organisational and operational measures. In the case of indoor positioning systems in smart hospitals, these lessons justify the need for a secure architecture based on defence in depth, segmentation, authentication, data validation and continuous monitoring.

5 SYSTEM UNDER STUDY AND THREATS

The system under study is a smart hospital that uses BLE-based indoor positioning. It is composed of beacons installed by zones, receiver devices used by patients or healthcare staff, a communication network, a positioning server, a navigation application and a monitoring system.

The general operation consists of beacons periodically transmitting signals, receivers detecting these signals and the server calculating an approximate position. Based on this position, the application can generate routes, display locations or help locate medical equipment. This model is useful because it allows specific threats to be analysed without physically deploying the infrastructure.

5.1 Assumptions and protected assets

The proposed analysis assumes a hospital where BLE beacons are installed in corridors, waiting rooms, emergency areas and zones where mobile equipment is frequently used. Patients may use a mobile application for guidance, while healthcare staff may use dashboards or internal applications to locate resources. The positioning server receives the signal information and calculates the approximate location.

The main assets that must be protected are: the identity of the beacons, the integrity of the location data, the availability of the positioning service, the configuration of the server, the application accounts and the logs used for incident investigation. Location data may also be sensitive because it can reveal movement patterns of patients or staff. For this reason, the system must protect both operational reliability and privacy.

Several assumptions are also made. First, the attacker is considered capable of being physically near the hospital or inside public areas, which makes wireless attacks realistic. Second, the attacker may use low-cost BLE hardware or software tools to capture or transmit signals. Third, the attacker does not necessarily need to compromise clinical systems; manipulating the positioning service alone can already reduce operational reliability. These assumptions help focus the threat model on realistic situations.

5.2 Beacon spoofing

Beacon spoofing consists of impersonating a legitimate BLE device by transmitting fake signals. In many BLE systems, beacons transmit identifiers that can be captured by nearby devices. If these identifiers are static or not protected, an attacker may replicate them using programmable BLE hardware.

In a smart hospital, this attack may cause the system to calculate an incorrect position. For instance, a patient could receive incorrect directions to reach a consultation room, or the system could show that a medical device is located in a different area. The main vulnerability is the lack of beacon authentication and the use of static identifiers. Dynamic identifiers, cryptographic authentication and spatial consistency checks can reduce this risk.

This threat is especially relevant because it does not require compromising the central server. A fake beacon located in a corridor or waiting area may be enough to influence the position calculated by a basic system. For this reason, the architecture must be able to verify not only the format of the signal, but also whether the signal is coherent with the known location and expected behaviour of the beacon.

5.3 Replay and relay

A replay attack consists of capturing legitimate signals and retransmitting them later. Unlike spoofing, the attacker does not need to modify the information, but simply reuses valid data at the wrong time. In an indoor positioning system, this may cause the server to accept old signals as current. This type of attack can be mitigated with timestamps, rotating

Table 3: THREAT MODELLING FOR INDOOR POSITIONING SYSTEMS

Threat	Description	Vulnerability	Impact	Risk	Mitigation
Spoofing	Fake beacon	Static identifiers	False position, incorrect routes and localisation errors	High	Dynamic identifiers, authentication and spatial validation
Replay	Reuse of valid signals	Lack of temporal validation	Old signals accepted as current	Medium-high	Timestamps, rotating identifiers and replay detection
Relay	Signal retransmission	Lack of proximity verification	False location of users or devices	High	Temporal consistency, distance analysis and additional technologies
Jamming	Intentional interference	Dependence on BLE	Partial or total service loss	High	Redundancy, signal-loss detection and manual protocols
RSSI	Signal strength manipulation	Signal sensitivity	Low accuracy and wrong positions	Medium-high	Kalman filters, smoothing and beacon comparison
Unauthorised access	Improper system access	Weak credentials or permissions	Configuration manipulation and data access	High	MFA, roles, auditing and segmentation
Availability	Service outage	Lack of redundancy	Inability to locate people or assets	High	Backup systems and continuity plan

identifiers and validation mechanisms that reject repeated signals.

A relay attack consists of retransmitting a legitimate signal from one location to another, making the system believe that a device is close to a beacon when it is actually somewhere else. Mitigation is more complex because the original signal may be valid. Therefore, several techniques must be combined, such as temporal verification, distance analysis, detection of impossible movements and comparison with other localisation sources.

The difference between replay and relay is important for the design of the defence. Replay can often be reduced by checking freshness, while relay may require analysing whether the measured proximity is physically plausible. In hospital environments, this means verifying whether the movement of a patient, staff member or asset is compatible with the building layout and with previous known positions.

5.4 Jamming and RSSI manipulation

Jamming consists of generating interference in the frequency band used by Bluetooth, making BLE signal reception difficult or impossible. Unlike other attacks, its main goal is not to alter the calculated position but to affect system availability. In a hospital, loss of the positioning service may hinder patient navigation, delay the location of medical equipment or affect staff coordination during emergencies.

RSSI manipulation directly affects positioning accuracy. In BLE systems, distance is estimated from received signal strength. However, this signal may vary due to walls, furniture, electromagnetic interference or people moving through the environment. Although this attack may be less evident than spoofing or jamming, its impact may be significant if the system does not validate the received data. Smoothing filters, Kalman filters, anomaly detection and comparison among multiple beacons can reduce this risk.

In practice, RSSI errors may be caused by both malicious and non-malicious factors. This makes mitigation more difficult, because the system must distinguish between normal signal variation and suspicious behaviour. A reasonable solution is not to trust a single RSSI measurement, but to combine several readings over time and compare them with historical values and neighbouring beacons.

5.5 Unauthorised access and availability

Unauthorised access occurs when someone enters the management system, server or application without legitimate permissions. This may happen through stolen credentials, weak passwords, misconfiguration or lack of multi-factor authentication. An attacker with unauthorised access could modify settings, alter location data, disable devices or access sensitive information.

Loss of availability refers to the partial or total interruption of the positioning system. It may be caused by attacks, technical failures, network outages, server overload or excessive dependence on a single technology. In smart hospitals, availability is a key requirement. Even if indoor positioning is not a primary clinical system, it may support important processes such as asset management, patient guidance and emergency response.

6 PROPOSED SECURE ARCHITECTURE

The proposed architecture is based on security by design. This means that security is not added at the end, but incorporated from the initial system definition. Defence in depth is also applied, using several protection layers so that if one measure fails, other controls can reduce the impact.

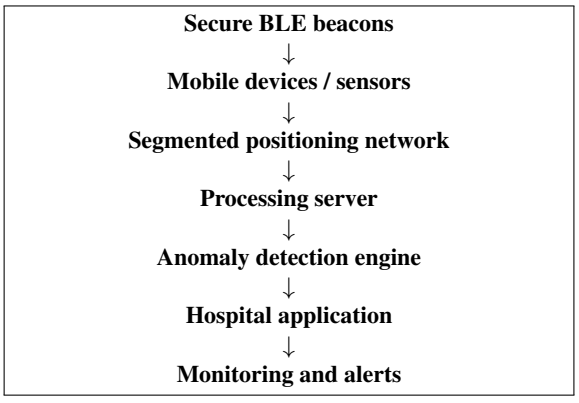

Fig. 1: Secure architecture for indoor positioning in smart hospitals.

6.1 Physical layer: BLE beacons

The physical layer is composed of the BLE beacons installed in the hospital. These devices are essential for the

positioning system and must be protected against spoofing, manipulation and physical replacement. A first measure is to avoid static identifiers. Instead, dynamic or rotating identifiers can be used so that an attacker cannot easily copy the identity of a legitimate beacon.

It is also necessary to maintain an updated inventory of devices, control their physical location and apply firmware updates when needed. Periodic checks of transmission power and detection of unauthorised beacons inside the hospital environment are also recommended.

6.2 Network layer

The network layer transports information between devices, servers and applications. In a hospital, this network should not be mixed with other critical systems without any separation. A specific VLAN or separated network for the positioning system is proposed. This network should be isolated from the administrative network and from critical medical systems.

Thus, if an attacker compromises a positioning device, the possibility of propagating the attack to other hospital systems is reduced. Encrypted communications, access control, internal firewall rules and traffic supervision are also recommended.

6.3 Processing layer

The processing layer calculates the position of users or devices from received signals. This layer is especially important because it allows errors or manipulations to be detected before they reach the final application. Data validation, anomaly detection, comparison among different beacons and temporal and spatial consistency analysis should be incorporated.

For example, if a user appears in two distant areas within a few seconds, the system should treat the position as suspicious. Similarly, if a beacon appears with signal strength inconsistent with its location, an alert should be generated. Kalman filters can help smooth RSSI measurements and reduce errors caused by environmental noise.

6.4 Application layer

The application layer is the visible part for users and healthcare staff. It may include mobile applications for patients, control panels for medical staff or management tools for administrators. Authentication and access control are important in this layer. Not all users should have access to the same information. A patient only needs general route guidance, whereas authorised staff may access information about equipment or internal resources.

Relevant accesses and changes should also be recorded using logs, because this allows incidents to be reviewed and anomalous behaviour to be detected. The principle of least privilege is essential to limit damage if an account is compromised.

6.5 Monitoring layer

As an additional layer, a monitoring system is proposed to supervise system behaviour in real time. This layer would detect anomalous patterns such as unknown beacons, sudden signal loss, repeated identifiers or impossible movements.

Monitoring can rely on log analysis tools, intrusion detection systems, security dashboards and automatic alerts. Although this layer cannot prevent all attacks, it improves response capacity and allows action before the problem seriously affects the service.

6.6 Relationship between threats and security controls

The proposed architecture is designed so that each relevant threat is addressed by more than one control. This is important because no single measure is sufficient in a critical environment. For example, beacon authentication can reduce spoofing, but it does not solve jamming. Similarly, network segmentation limits lateral movement, but it does not correct inaccurate RSSI values. Therefore, the architecture combines preventive, detective and corrective measures.

Table 4 summarises how the security proposal is linked to the threat analysis. This table is useful because it shows that the architecture is not a generic list of good practices, but a response to the specific risks identified in the hospital positioning system.

7 Results and Discussion

The results are presented through a qualitative-quantitative risk assessment. Each threat is assigned a score by combining probability and impact on a scale from 1 to 5. The final score is interpreted as an approximation of risk, where higher values indicate more critical threats for the indoor positioning system.

This assessment is not intended to replace a professional audit or a real experimental test, but it makes it possible to compare the behaviour of a basic system with the proposed security architecture. It also helps visualise the contribution of this work: moving from a descriptive threat analysis to an original risk-reduction evaluation.

Table 5 shows that the threats with the highest initial risk are spoofing and jamming, both with a score of 20. In the case of spoofing, the risk is due to the possibility of impersonating beacons when static identifiers are used. In the case of jamming, the risk is related to service unavailability, which is especially critical in a hospital environment. Relay and RSSI manipulation also present relevant values because they affect location integrity and accuracy.

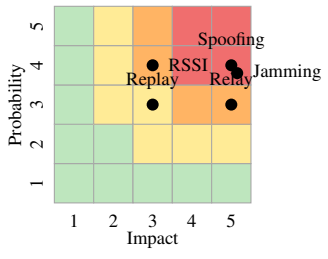

Fig. 2: Visual risk matrix for the basic system. Threats in red areas require priority measures.

Table 4: MAPPING BETWEEN THREATS AND PROPOSED SECURITY CONTROLS

Threat	Preventive controls	Detection controls	Response controls	Expected effect
Spoofing	Dynamic identifiers and beacon authentication	Unknown beacon detection and spatial validation	Ignore suspicious signals and generate alerts	Lower probability of accepting fake beacons
Replay	Timestamps and rotating identifiers	Repeated-signal detection	Reject old packets	Better signal freshness
Relay	Proximity checks and multi-source positioning	Impossible movement detection	Request confirmation or use backup location source	Lower risk of false proximity
Jamming	Redundant technologies and robust deployment	Sudden signal-loss alerts	Manual procedure and fail-safe mode	Improved availability
RSSI manipulation	Filtering and multiple beacon comparison	Anomaly detection	Discard outliers and recalculate position	Improved accuracy and integrity
Unauthorised access	MFA, roles and least privilege	Log review and access alerts	Account blocking and incident response	Reduced risk of configuration abuse

Table 5: RISK COMPARISON BEFORE AND AFTER APPLYING THE PROPOSED ARCHITECTURE

Threat	Basic system	Protected system
Spoofing	20	8
Replay	9	4
Relay	15	6
Jamming	20	10
RSSI	12	5

Figure 2 visually represents the criticality of threats in the basic system. Spoofing and jamming appear in the highest-risk zone because they combine high probability or ease of occurrence with a significant impact on system operation. Relay is also placed in a high-risk area, since it can alter the perceived location of users or devices. Replay and RSSI remain relevant because they degrade positioning reliability.

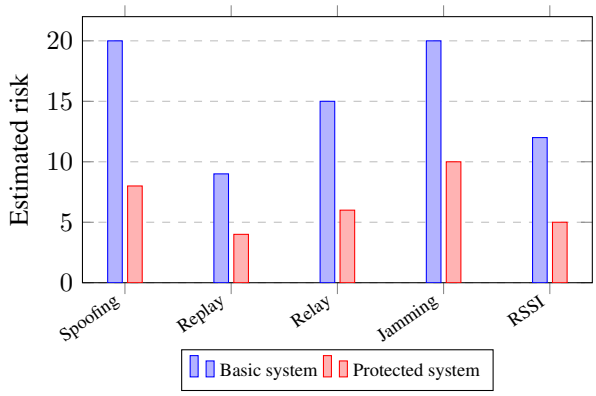

Fig. 3: Residual risk comparison before and after applying the proposed architecture.

Figure 3 shows the reduction of residual risk after applying the proposed architecture. Spoofing decreases from 20 to 8 thanks to dynamic identifiers, beacon authentication and spatial validation. Replay is reduced from 9 to 4 through timestamps and replay detection. Relay decreases from 15 to 6 due to temporal and spatial consistency controls. Jamming remains relevant, but its residual risk decreases from 20 to 10 thanks to redundancy and signal-loss detection mechanisms. Finally, RSSI manipulation decreases from 12 to 5 through filtering, anomaly rejection and comparison among multiple beacons.

Overall, these results show that the proposed security architecture does not completely eliminate threats, but it does reduce their impact and improves detection and response capability. This is the main difference between a functional system and a resilient system: the former may work under normal conditions, while the latter includes mechanisms to preserve reliability under manipulated signals, failures or anomalous behaviour.

From an engineering perspective, the proposal is feasible because it does not depend on a single protection measure. The combination of controls at device, network, processing, application and monitoring levels implements defence in depth. However, it also has limitations: it may increase management complexity, require additional investment and depend on correct initial configuration. Therefore, any real deployment should be accompanied by testing, audits and maintenance procedures.

The most relevant result is the reduction of residual risk in the threats that directly affect the integrity and availability of the positioning service. Spoofing and relay are reduced because the system no longer accepts signals only based on their identifier or apparent proximity. Jamming remains with a higher residual value because interference cannot be completely prevented by software controls. Nevertheless, redundancy and alerting mechanisms can reduce the operational impact. RSSI manipulation also remains relevant because indoor radio propagation is naturally unstable, but filtering and consistency checks make the final position more robust.

It is also important to note that the proposed measures have different costs. Some controls, such as access control, log review or segmentation, are common in secure network design and can be integrated without modifying the positioning algorithm. Others, such as dynamic beacon identifiers or anomaly detection, require additional configuration and maintenance. Therefore, in a real hospital, the implementation should be gradual and prioritised according to risk.

8 LIMITATIONS AND FUTURE VALIDATION

The proposal developed in this work should be understood as a conceptual design aimed at improving the security of indoor positioning systems in smart hospitals. Its main value is to connect technical threats with operational consequences and to propose specific controls to reduce risk. However, several limitations must be considered.

The first limitation is that no physical deployment has been carried out in a real hospital. Therefore, parameters such as positioning accuracy, latency, packet loss, energy consumption and real anomaly detection time have not been

measured. These factors may vary depending on the building, beacon distribution, wall materials, people density and network configuration.

The second limitation is related to the nature of RSSI. BLE signal strength is unstable indoors and may change for non-malicious reasons. This means that anomaly detection must be carefully configured to avoid false positives. If the system is too strict, it may discard valid signals; if it is too flexible, it may accept manipulated signals.

The third limitation is organisational. A secure architecture does not depend only on technology. It also requires maintenance processes, trained staff, updated inventories, log review and incident response procedures. If these processes are not maintained over time, initial security may gradually degrade.

To validate the proposal in the future, quantitative metrics could be defined. Possible metrics include average positioning error, percentage of discarded signals, time required to detect a fake signal, service availability under partial beacon loss and number of false alarms generated by the system. These metrics would make it possible to compare a basic system with the proposed architecture in a more objective way.

A simple simulation could also be implemented using a hospital floor plan, several beacons and different attack scenarios. A first scenario would analyse normal system behaviour. A second one would introduce a fake beacon. A third one would apply the secure architecture with temporal and spatial validation. Such a simulation would visually show how estimated positions change and what each protection measure contributes.

9 Conclusions

This work has analysed the protection of critical infrastructures in Smart City environments, paying special attention to indoor positioning systems in smart hospitals. The study shows that urban digitalisation offers important advantages, but also introduces new vulnerabilities that must be considered from the design stage.

The analysis of real cases shows that many threats share common patterns: insecure access, lack of segmentation, outdated systems and insufficient monitoring. These lessons are applicable to the hospital context, where connected systems may affect operational continuity.

The threat model shows that BLE-based systems may be affected by spoofing, replay, relay, jamming, RSSI manipulation, unauthorised access and loss of availability. In a hospital environment, these attacks can affect patient navigation, medical equipment location and healthcare staff coordination.

As the main contribution, a multilayer security architecture has been proposed. It includes measures at the device, network, processing, application and monitoring levels. This architecture does not completely eliminate risks, but it reduces their impact and improves detection and response capability.

As future work, it would be interesting to implement a more detailed simulation, compare BLE with technologies such as UWB or WiFi, and validate the proposal in a real or simulated hospital environment. Machine learning techniques could also be studied to detect anomalous patterns in location signals.

Another future line would be to define quantitative metrics to evaluate the improvement provided by each security measure. For example, average positioning errors before and after applying Kalman filters, anomaly detection times or system behaviour under partial beacon loss could be compared. This would make it possible to transform the conceptual proposal into a more complete experimental evaluation.

Finally, the work could be extended by incorporating privacy factors. Indoor positioning systems may handle sensitive information about the movements of patients, healthcare staff or equipment. Therefore, in addition to availability and data integrity, data minimisation, access control and anonymisation or pseudonymisation mechanisms should be studied whenever location information is not strictly necessary.

Acknowledgements

I would like to thank the guidance received during the development of this thesis, especially in defining the focus of the work and improving the final structure. I also appreciate the support received during the review, planning and writing process.

References

[1] L. Cotino et al., *Guía de ciberseguridad para ciudades inteligentes*. Inter-American Development Bank, 2021. Available at: https://publications.iadb.org/publications/spanish/document/Guia-de-ciberseguridad-para-ciudades-intelige pdf

[2] M. Kalinin, V. Krundyshev and P. Zegzhda, "Cybersecurity Risk Assessment in Smart City Infrastructures," *Machines*, vol. 9, no. 4, 2021.

[3] National Institute of Standards and Technology, *Cybersecurity Framework*. Available at: https://www.nist.gov/cyberframework

[4] K. Stouffer et al., *Guide to Operational Technology (OT) Security*, NIST Special Publication 800-82 Rev. 3, 2023.

[5] International Society of Automation, *ISA/IEC 62443 Series of Standards*. Available at: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standar

[6] European Parliament and Council, *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union*, 2022.

[7] ENISA, *Cyber Security and Resilience for Smart Hospitals*, 2016.

[8] ENISA, *ENISA Threat Landscape: Health Sector*, 2023.

[9] V. Cantón Paterna et al., "A Bluetooth Low Energy Indoor Positioning System with Channel Diversity, Weighted Trilateration and Kalman Filtering," *Sensors*, vol. 17, no. 12, 2017.

[10] T. Shi et al., "A Survey of Bluetooth Indoor Localization," arXiv, 2024.

[11] D. Barba et al., "Uso de Bluetooth de Baja Energía en Aplicaciones de Localización Indoor," Universidad de Valladolid, 2017.

[12] CISA, *Cyber-Attack Against Ukrainian Critical Infrastructure*, 2016. Available at: https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01

[13] University of Hawai'i West O'ahu Cyber, *Oldsmar Water Treatment Facility Attack*, 2021. Available at: https://westoahu.hawaii.edu/cyber/ics-cybersecurity/ics-weekly-summaries/oldsmar-water-treatment-facility-attack/

[14] CISA, *The Attack on Colonial Pipeline: What We Have Learned*, 2023. Available at: https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

[15] Information Commissioner's Office, *NHS cyber attack*. Available at: https://ico.org.uk/for-the-public/ico-40/nhs-cyber-attack/

[16] Oficina de Coordinación de Ciberseguridad, *Guía sobre Seguridad en Dispositivos IoT*. Available at: https://occ.ses.mir.es/publico/occ/dam/jcr:a97a3ac9-1a92-4af0-a5c0-3ac8557244ba/Guia-sobre-Seguridad-en-Dispositivos-IoT.pdf

[17] W. P. Moya Velasco, *Implementación de un algoritmo de localización basado en trilateración y tecnología Bluetooth Low Energy*, Escuela Politécnica Nacional, 2019.

[18] Z. Wang, "Securing Bluetooth Low Energy: A Literature Review," arXiv, 2024.

[19] J. Leng, X. Yan and Z. Lin, "Design of an Internet of Things System for Smart Hospitals," arXiv, 2022.

[20] H. Agarwal, N. Sanghvi, V. Roy and K. Kitani, "DeepBLE: Generalizing RSSI-based Localization Across Different Devices," arXiv, 2021.

APPENDIX

A.1 Complete threat table

The complete threat table has been integrated into the main body of the work to make reading easier and to directly relate each threat to its mitigation. In an extended version, quantitative probability and impact metrics could be added.

A.2 Practical scenario

The practical scenario compares three situations: normal system, system under attack and protected system. This example shows that the proposed architecture mainly adds value in the detection and response to anomalous signals.

In the normal scenario, a patient enters the hospital and uses the navigation application to find a consultation room. The system receives signals from several beacons, estimates the position through RSSI and generates a route. Although some precision error may exist, the service is sufficient to guide the user.

In the attack scenario, a fake beacon appears with an identifier similar to a legitimate device. The basic system accepts the signal and calculates an incorrect position. As a result, the route may deviate and the user may receive wrong indications.

In the protected scenario, the server compares the received signal with the beacon inventory, verifies temporal consistency and analyses whether the position change is possible. If an inconsistency is detected, the system discards the signal or generates an alert. Thus, the system does not necessarily prevent the attacker from transmitting the signal, but it reduces its impact on the final application.

A.3 Priority measures summary

The priority measures for a real deployment would be: beacon inventory, dynamic identifiers, network segmentation, multi-factor authentication for administrators, signal validation, anomaly detection and contingency planning. These measures are considered priorities because they directly address the highest risks identified in the threat model.

A.4 Implementation checklist

As a practical support for the proposal, a short checklist could be used before deploying an indoor positioning system in a smart hospital. First, all installed beacons should be inventoried, have a known location and avoid permanent identifiers that are easy to copy. Second, the positioning network should be separated from clinical and administrative networks through logical segmentation.

Third, the processing server should apply validations before accepting a position as valid. These validations should include temporal coherence, spatial coherence, comparison among several beacons and rejection of clearly anomalous RSSI values. Fourth, the application should use permissions according to user roles. A patient does not need the same information as a technician or system administrator.

Finally, the system should generate activity logs and alerts for unusual behaviours. For example, the appearance of an unknown beacon, the simultaneous loss of several signals or an impossible user movement should be considered relevant events. This checklist does not replace a full audit, but it helps translate the proposed architecture into practical measures.

A.5 Relation with the objectives of the work

The work fulfils the objectives established at the beginning. The first objective is addressed by studying Smart Cities, critical infrastructures, IoT and IT/OT systems. The second objective is fulfilled through the analysis of specific threats affecting BLE and indoor positioning. The third objective is developed by studying the impact of these threats in smart hospitals. Finally, the fourth objective is materialised in the proposed multilayer security architecture.

The main contribution of the work is to connect a general urban cybersecurity problem with a specific and current case: indoor positioning in hospitals. This connection avoids an overly broad analysis and focuses the proposal on a specific system, with clearly identified threats and solutions.