NATIONAL TECHNICAL UNIVERSITY OF ATHENS

School of Electrical and Computer Engineering

Division of Communications, Electronics and Information Systems

Design of a Wireless Indoor Tracking System for Multi-Sensor Data Acquisition with BLE Channel Sounding

Diploma Thesis

Vasiloglou Athanasios

Supervisor:

Evangelos V. Christoforou

Professor, N.T.U.A.

Athens, September 2025

NATIONAL TECHNICAL UNIVERSITY OF ATHENS

School of Electrical and Computer Engineering

Division of Communications, Electronics and Information Systems

Design of a Wireless Indoor Tracking System for Multi-Sensor Data Acquisition with BLE Channel Sounding

Diploma Thesis

Vasiloglou Athanasios

Approved by the three-member examination committee on October 17, 2025.

Evangelos Christoforou	Georgios Panagopoulos	Emmanouil Chourdakis
Professor, NTUA	Assistant Professor	Assistant Professor

Vasiloglou Athanasios

Diploma Electrical and Computer Engineer, NTUA

Abstract

This thesis presents the design and development of a **wireless indoor tracking system** that integrates **multi-sensor data acquisition** with **Bluetooth Low Energy (BLE) Channel Sounding** for precise short-range localization. The system combines distance estimation based on *Inverse Fast Fourier Transform (IFFT)* and *Phase-Based Ranging (PBR)* with real-time environmental sensing, enabling both positioning and contextual monitoring in indoor environments.

The thesis is structured into three main parts. The first part introduces the **theoretical background** of radio propagation, BLE technology, and channel sounding principles, emphasizing the advantages of IQ-based phase and delay measurements over traditional RSSI approaches. The second part focuses on the **hardware and software design**, including the development of a custom PCB built around the **nRF54L15 SoC**, integration of environmental and inertial sensors, and implementation of firmware supporting both sensor data transmission and channel sounding procedures. The third part presents an **experimental evaluation** of the system through a series of controlled indoor tests, including stepped-distance measurements, single-link ranging, and local error field visualization.

The results demonstrate that the proposed system achieves **sub-metre accuracy** under realistic indoor conditions, with the **IFFT-based estimator** providing the most stable and accurate distance estimates compared to PBR. The overall performance validates the feasibility of BLE Channel Sounding as a practical ranging method for cost-effective indoor localization and sensor fusion applications. This work establishes a modular foundation for future extensions toward multi-anchor positioning, autonomous mapping, and context-aware tracking in industrial and IoT environments.

Keywords: BLE, Channel Sounding, indoor localization, IFFT, Phase-Based Ranging, IQ sampling, nRF54L15, sensor fusion, embedded systems, wireless tracking.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

The need for precise and accurate supervision of industrial facilities has significantly increased in recent years. Modern industries require continuous monitoring of both operational processes and environmental conditions in order to ensure efficiency, safety, and reliability. While technologies such as GPS and GNSS satellites provide robust solutions for outdoor localization and tracking, their effectiveness is drastically reduced indoors, where satellite signals are often unavailable or unreliable. This limitation creates a persistent challenge for indoor monitoring and supervision.

In this context, the present work aims to develop a stable and easily implementable solution designed specifically for indoor environments. The proposed system provides accurate and fast localization capabilities, complemented by environmental diagnostics such as temperature, pressure, and humidity measurements. Furthermore, the integration of inertial measurement units (IMUs) enables the detection of critical safety-related events, such as free-fall incidents, thereby enhancing system reliability. In addition, it can advance power management through an efficient wake-up/sleep routine that extends battery life and ensures long-term operation.

The technological innovation of this approach lies in its adaptability, simplicity, and low cost. The system is highly configurable, allowing seamless extension from two-dimensional (2D) positioning to full three-dimensional (3D) mapping. This flexibility, combined with its affordability, enables comprehensive remote supervision of indoor spaces, addressing a long-standing gap in facility management and industrial safety.

By combining accurate indoor positioning with environmental monitoring and safety features, the proposed system contributes to the development of intelligent infrastructures.

Such infrastructures can provide significant benefits for industrial applications, occupational safety, and facility management, paving the way for smarter and safer workplaces.

Chapter 2

Theoretical Background

2.1 Indoor Radio Propagation

Indoor radio propagation is a complex phenomenon influenced by building geometry, wall materials, furniture, human mobility, and dynamic environmental conditions. Unlike outdoor propagation, where the free-space path loss (Friis equation) is often sufficient, indoor channels are dominated by multipath reflections, diffraction, and scattering [2][1, 3]. These effects manifest as frequency-selective fading, delay spread, and shadowing, which significantly affect the reliability of wireless communication and localization accuracy.

2.1.1 Channel Parameters

The characterization of indoor radio propagation relies heavily on a set of statistical parameters that describe how multipath propagation affects the temporal and spectral properties of the received signal. These parameters primarily the *root-mean-square (RMS) delay spread*, *coherence bandwidth*, and *coherence time* quantify the channels dispersive nature and determine the extent to which signal components interfere constructively or destructively.

RMS Delay Spread

The **RMS delay spread** (τ_{rms}) is a fundamental parameter that quantifies the temporal dispersion caused by multipath propagation. It measures the second central moment of the *power delay profile (PDP)*, $P(\tau)$, which represents the average received power as a function of excess delay τ:

$$P(\tau) = \mathbb{E}\{|h(t,\tau)|^2\},$$

where $h(t,\tau)$ denotes the time-varying channel impulse response.

The mean excess delay and RMS delay spread are defined respectively as:

$$\bar{\tau} = \frac{\int \tau P(\tau) d\tau}{\int P(\tau) d\tau}, \quad \tau_{\text{rms}} = \sqrt{\frac{\int (\tau - \bar{\tau})^2 P(\tau) d\tau}{\int P(\tau) d\tau}}.$$

Intuitively, τ_{rms} describes how spread out in time the received energy is due to multipath reflections. A small delay spread indicates that most of the received energy arrives within a short time window (typical of line-of-sight or lightly scattered environments), while a large τ_{rms} implies significant temporal dispersion, often leading to *intersymbol interference (ISI)* in digital communication systems. Typical indoor environments exhibit RMS delay spreads ranging from a few tens of nanoseconds (open offices) up to several hundreds of nanoseconds (industrial or dense urban indoor areas) [5, 4].

Coherence Bandwidth

The **coherence bandwidth** (B_c) is a statistical measure of the frequency range over which the channels frequency response is highly correlated. It provides insight into the degree of frequency selectivity that is, whether different parts of the transmitted spectrum experience similar fading.

For a given threshold correlation ρ, the coherence bandwidth can be approximated as:

$$B_c(\rho) = \frac{1}{2\pi\tau_{\text{rms}}}$$

or more commonly in engineering approximations:

$$B_c \approx \frac{1}{5\tau_{\text{rms}}}.$$

If the signal bandwidth $B_s \ll B_c$, the channel can be regarded as *flat fading*, meaning all frequency components experience approximately the same gain and phase shift. Con-

versely, when $B_s > B_c$, the channel exhibits *frequency-selective fading*, and the received spectrum is distorted due to the varying phase and amplitude response across frequency.

In the context of BLE (which typically uses 2 MHz channels), this distinction determines whether simple narrowband models suffice or whether equalization and multipath mitigation techniques are necessary. Channel sounding systems exploit this parameter to ensure the probing signal spans sufficient bandwidth to resolve individual multipath components in the time domain.

Coherence Time and Doppler Spread

The **coherence time** (T_c) characterizes the time duration over which the channel impulse response remains approximately constant. It is inversely related to the **Doppler spread** (f_D), which measures the spectral broadening of the signal caused by relative motion between the transmitter, receiver, and surrounding scatterers:

$$T_c \approx \frac{1}{f_D}.$$

The Doppler spread is given by:

$$f_D = \frac{v f_c}{c},$$

where v is the relative velocity, f_c is the carrier frequency, and c is the speed of light. At BLE frequencies (around 2.4 GHz) and typical indoor mobility (e.g., human walking speed ~ 1 m/s), f_D is on the order of a few Hz, leading to coherence times of several tens to hundreds of milliseconds. Thus, the channel can often be considered *quasi-static* during short BLE packet exchanges, simplifying channel estimation and IQ-based ranging.

Interrelation and Implications

The triplet $(\tau_{\text{rms}}, B_c, T_c)$ succinctly captures the *time-frequency duality* of wireless channels:

- Large $\tau_{\text{rms}} \rightarrow$ small $B_c \rightarrow$ strong frequency selectivity.
- Large $f_D \rightarrow$ small $T_c \rightarrow$ rapid temporal variation.

These relationships are critical when designing and analyzing systems that rely on phase-

coherent processing. For instance:

- The achievable **ranging precision** in phase-based methods is limited by τ_{rms} and B_c, since excessive multipath dispersion introduces phase ambiguities.
- The **channel estimation interval** must be shorter than T_c to ensure valid and consistent IQ measurements across frequency samples.
- In BLE Channel Sounding, where multiple frequency tones are sequentially transmitted, stability within the coherence time is essential for accurate phase differencing.

Overall, the statistical parameters of the indoor radio channel provide the theoretical framework that links the physical environment to the signal characteristics observed in IQ measurements. Accurate estimation of these parameters is indispensable for the design of reliable and high-precision BLE-based localization systems.

Table 2.1: Typical indoor channel parameters at 2.4 GHz [5, 4].

Environment	τ_{rms} [ns]	B_c [MHz]	T_c [ms] (for $v = 1$ m/s)
Open office	3050	46	100150
Residential	50100	24	80120
Industrial hall	100300	0.72	60100
Shopping mall / dense NLOS	200500	0.31	5080

2.2 In-Phase and Quadrature (IQ) Signals

Modern digital communication systems represent radio signals in terms of their *in-phase* (I) and *quadrature* (Q) components. This decomposition is fundamental for capturing both the amplitude and the phase of a signal, enabling advanced modulation schemes, coherent demodulation, and precise channel characterization.

2.2.1 Mathematical Representation

A bandpass signal centered at carrier frequency f_c can be expressed as:

$$r(t) = I(t)\cos(2\pi f_c t) - Q(t)\sin(2\pi f_c t),$$

where $I(t)$ and $Q(t)$ are the time-varying in-phase and quadrature components, respectively. Equivalently, the signal can be represented in complex baseband form as:

$$z(t) = I(t) + jQ(t).$$

This compact representation preserves both magnitude and phase, allowing the use of complex signal processing techniques.

In practice, IQ sampling is performed by downconverting the received RF signal to baseband and digitizing the in-phase and quadrature components using two synchronized analog-to-digital converters (ADCs).

2.2.2 Relevance for Localization

Unlike the Received Signal Strength Indicator (RSSI), which measures only average signal power, IQ samples retain the rich frequency- and phase-domain characteristics of the channel. This enables:

- **Phase-based ranging:** exploiting phase differences across frequencies for sub-meter distance accuracy [7].
- **Angle-of-Arrival/Departure estimation:** comparing IQ samples across antenna arrays to compute signal direction [23].
- **Channel sounding:** reconstructing the channel impulse response (CIR) from IQ samples to isolate line-of-sight paths and mitigate multipath [6].

IQ representation thus forms the theoretical and practical foundation for modern BLE-based localization, particularly with the advent of Bluetooth 5.1 (direction finding) and Bluetooth 6.0 (channel sounding).

2.3 Bluetooth Low Energy (BLE)

Bluetooth Low Energy (BLE) is a wireless communication technology standardized by the Bluetooth Special Interest Group (SIG). It was originally conceived by Nokia in 2006 under the name *Wibree*, a short-range, ultra-low-power technology intended for applications

such as watches and sensors. In 2010, Wibree was merged into the Bluetooth 4.0 Core Specification, marking the official introduction of BLE as a distinct mode alongside Classic Bluetooth [34, 21].

BLE was designed from the ground up to support energy-efficient communication while maintaining sufficient range and interoperability across billions of consumer devices. Its lightweight protocol stack, flexible topologies, and continuous evolution through successive Bluetooth releases have made it a dominant technology in Internet-of-Things (IoT) and indoor localization systems [12, 27].

2.3.1 Historical Evolution of BLE Standards

Each subsequent Bluetooth release extended BLE capabilities significantly:

- **Bluetooth 4.0 (2010):** Introduced BLE as part of the Core Specification, enabling ultra-low-power short-range communication.
- **Bluetooth 5.0 (2016):** Enhanced data rates (2M PHY), range (Coded PHY), and advertising capacity, supporting more robust IoT applications.
- **Bluetooth 5.1 (2019):** Introduced *direction finding* features (Angle-of-Arrival and Angle-of-Departure), enabling centimeter-level localization accuracy with antenna arrays [23].
- **Bluetooth 5.2 (2020):** Added Isochronous Channels, paving the way for LE Audio.
- **Bluetooth 5.4 (2023):** Introduced *Periodic Advertising with Responses (PAwR)*, enabling bidirectional, large-scale broadcasting suitable for sensor networks and electronic shelf labeling [28].
- **Bluetooth 6.0 (2024):** Brought *Channel Sounding*, a fine-ranging feature allowing sub-meter accuracy through phase and delay measurements [29].

This continuous evolution reflects the dual objective of BLE: to remain energy-efficient while enabling advanced features such as high-accuracy indoor positioning.

2.3.2 Roles and Network Topology

BLE defines two fundamental roles: *central* and *peripheral*. A central device initiates and manages connections (e.g., smartphone, gateway), while a peripheral device advertises its presence and responds to connection requests (e.g., sensor node, wearable). In addition, BLE supports the *broadcaster-observer* model, enabling connectionless communication particularly well-suited for scalable localization and tracking systems [14, 15].

2.3.3 Physical Layers (PHYs)

BLE provides multiple physical layers, optimized for different requirements:

- **1M PHY:** Legacy, robust physical layer.
- **2M PHY:** Doubles data throughput at the cost of reduced range.
- **Coded PHY:** Introduced in Bluetooth 5.0, extends communication range using forward error correction with trade-offs in data rate.

This flexibility allows system designers to balance reliability, energy consumption, and coverage according to application needs.

2.3.4 Direction Finding (AoA/AoD)

The introduction of Angle-of-Arrival (AoA) and Angle-of-Departure (AoD) in Bluetooth 5.1 marked a major milestone for BLE-based localization [16, 23]. These features rely on IQ sample collection across antenna arrays and signal processing to compute the direction of signal propagation. Direction finding, combined with multilateration or triangulation, enables sub-meter positioning accuracy, expanding BLEs role in industrial IoT, asset tracking, and navigation.

2.3.5 BLE in Indoor Positioning

BLE has been extensively adopted for indoor localization due to its ubiquity, low energy consumption, and cost efficiency. Common approaches include:

- **RSSI fingerprinting:** Early solutions relied on Received Signal Strength Indicator (RSSI) maps [11], often enhanced with filtering techniques such as Kalman or particle filters [13, 18].
- **Direction finding:** AoA/AoD introduced in BT 5.1 enhanced positioning accuracy in dense multipath environments [16].
- **Channel sounding:** The latest BLE hardware platforms (e.g., Nordic nRF54L15 [35]) allow access to IQ samples and implement Channel Sounding (BT 6.0), enabling robust phase- and delay-based ranging [29].

In summary, BLE has evolved from a low-power communication technology into a comprehensive localization platform. Its trajectory from Wibree to BLE 6.0 illustrates the synergy of energy efficiency, scalability, and high-accuracy positioning features.

2.4 Channel Sounding Concepts

Channel sounding refers to the process of probing the wireless channel in order to characterize its multipath structure in time and frequency. The wireless baseband equivalent channel is often modeled as a linear time-varying system with impulse response:

$$h(t,\tau) = \sum_{k=1}^{L} \alpha_k(t)\,\delta(\tau - \tau_k(t)),$$

where $\alpha_k(t)$ and $\tau_k(t)$ denote the time-varying complex amplitude and excess delay of the k-th multipath component, and L is the number of significant paths [5].

The frequency response is given by the Fourier transform of $h(t,\tau)$:

$$H(t,f) = \int_{-\infty}^{\infty} h(t,\tau)\,e^{-j2\pi f\tau} d\tau,$$

and in practice is estimated over a finite bandwidth by transmitting pilot tones or wideband probing sequences. By applying the inverse Fourier transform, the channel impulse

response (CIR) can be reconstructed, and multipath arrivals can be resolved if the system bandwidth exceeds the channel coherence bandwidth [4, 1].

2.4.1 Performance Bounds

The accuracy of channel sounding and phase-based ranging can be quantified through the Cramér-Rao Lower Bound (CRLB). For a single-tone phase measurement at frequency f, the variance of any unbiased estimator $\hat{d}$ satisfies:

$$\mathrm{Var}(\hat{d}) \geq \frac{c^2}{8\pi^2 f^2 \cdot \mathrm{SNR}},$$

where SNR is the signal-to-noise ratio [9]. For wideband systems using B Hz of effective bandwidth, the bound improves approximately as $1/B^2$, demonstrating the advantage of large bandwidths (e.g., UWB) over narrowband methods such as BLE [7].

These bounds provide theoretical performance limits against which practical algorithms (e.g., CIR peak detection, multifrequency phase fitting) can be benchmarked. In practice, additional errors arise due to hardware impairments, frequency offset, phase noise, and multipath-induced bias [6].

2.5 Ranging and Positioning Techniques

Several techniques can be employed for estimating distances and positions based on channel sounding measurements.

2.5.1 IFFT (Inverse Fast Fourier Transform) Distance Estimation

In practical channel sounding, the channel frequency response is measured at a finite set of discrete frequencies:

$$\{f_k\}_{k=0}^{N-1}, \qquad \text{with spacing } \Delta f.$$

The measured complex coefficients $H[k] = H(f_k)$ contain both amplitude and phase information of the multipath channel. Applying the inverse discrete Fourier transform

(IFFT) converts these frequency-domain samples into the discrete-time channel impulse response (CIR):

$$h[n] = \frac{1}{N} \sum_{k=0}^{N-1} H[k]\, e^{j2\pi kn/N}, \qquad n = 0, \ldots, N-1.$$

Each time index n corresponds to an excess delay $\tau_n = n\,\Delta\tau$, where the time resolution is

$$\Delta\tau = \frac{1}{N\,\Delta f} = \frac{1}{B},$$

and $B = N\Delta f$ denotes the total sounded bandwidth. The maximum unambiguous delay that can be represented is $\tau_{\max} = 1/\Delta f$.

The magnitude $|h[n]|$ reveals the relative power of multipath components arriving at different delays. The earliest significant peak in the CIR, typically above a noise threshold, is associated with the line-of-sight (LOS) or shortest propagation path. The corresponding distance can be estimated as:

$$\hat{d}_{\mathrm{CIR}} = c \cdot \hat{\tau}_{\min},$$

where $\hat{\tau}_{\min}$ is the delay of the first detectable peak and c is the speed of light.

This method is effective when a clear LOS path is present and separable from multipath components. However, in dense multipath environments, non-line-of-sight (NLOS) propagation can bias the estimated delay and introduce significant ranging errors [3, 5].

Hence, the IFFT serves as the core operation that transforms frequency-domain channel measurements into their time-domain representation, enabling the extraction of the *propagation delay* and consequently, the *distance* from the measured data. This principle forms the foundation for many channel-sounding-based localization techniques.

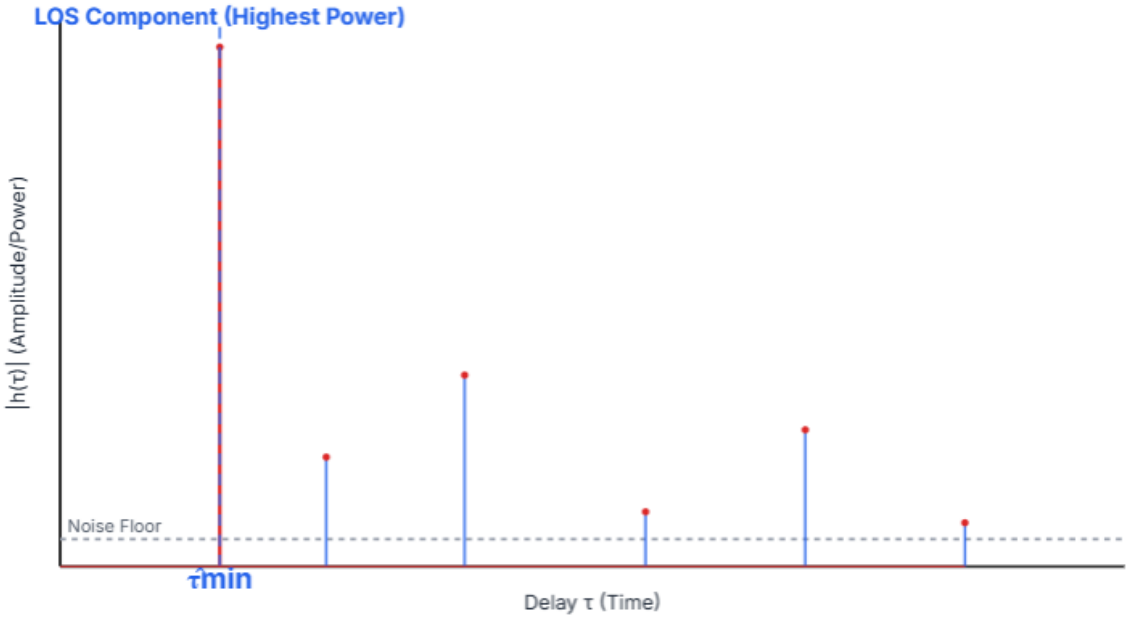

Figure 2.1: Illustration of a typical Channel Impulse Response (CIR) obtained via IFFT, showing multipath components at different delays.

2.5.2 Phase-Based Distance Estimation

The phase response $\phi(f)$ of the channel transfer function $H(f)$ is directly related to the propagation distance d:

$$\phi(f) = \arg\{H(f)\} \approx -\frac{2\pi f d}{c} + \phi_0,$$

where ϕ_0 denotes a frequency-independent hardware phase offset [7]. In practice, the measured phase is wrapped modulo 2π, giving rise to the well-known *phase ambiguity* problem. To mitigate this, measurements across multiple frequencies are used.

For two frequencies f_1 and f_2, the phase difference is

$$\Delta\phi = \phi(f_2) - \phi(f_1) \approx -\frac{2\pi(f_2 - f_1)d}{c},$$

from which the distance can be estimated as

$$d \approx -\frac{c}{2\pi\Delta f}\,\Delta\phi,$$

with $\Delta f = f_2 - f_1$. Extending this to K carrier frequencies allows a least-squares fit:

$$\hat{d} = \arg\min_{d} \sum_{k=1}^{K} \left(\phi(f_k) + \tfrac{2\pi f_k d}{c}\right)^2,$$

which enhances robustness against phase noise and wrapping errors [17].

Alternatively, by considering the continuous phase slope over frequency, the distance can be interpreted as proportional to the negative derivative of the unwrapped phase response:

$$\frac{d\phi(f)}{df} \approx -\frac{2\pi d}{c}.$$

Thus, d can be estimated via linear regression on $\phi(f)$ versus f, achieving sub-wavelength precision even under narrowband conditions.

In practical BLE-based systems, this *multifrequency phase estimation* method is often combined with *CIR peak detection*, forming a hybrid approach that leverages both time- and frequency-domain information for improved robustness in multipath environments [18].

2.5.3 Multilateration and Filtering

Once distances $\hat{d}_i$ to anchors at positions $\mathbf{a}_i = (x_i, y_i)$ are estimated, the tag position $\hat{\mathbf{p}}$ can be obtained by nonlinear least squares:

$$\hat{\mathbf{p}} = \arg\min_{\mathbf{p}} \sum_{i=1}^{N} \left(\|\mathbf{p} - \mathbf{a}_i\| - \hat{d}_i\right)^2.$$

This optimization can be solved iteratively using gradient-based or GaussNewton methods [9]. To mitigate noise and dynamics, state-space filters such as the Extended Kalman Filter (EKF), Unscented Kalman Filter (UKF), or Particle Filter (PF) are applied [8, 18].

2.5.4 Comparison of Techniques

- **RSSI-based ranging** is simple but inaccurate in multipath-rich indoor environments [11].
- **CIR peak detection** provides absolute delay estimates but suffers from NLOS bias.

- **Phase-based methods** enable sub-meter precision but require frequency diversity and phase synchronization.
- **Hybrid methods** combining CIR and phase improve robustness, especially in modern BLE systems with channel sounding support.

Overall, channel sounding approaches bridge the gap between narrowband RSSI methods and wideband UWB solutions, offering a compromise between cost, power, and accuracy.

2.6 Comparison with RSSI-Based Localization

Received Signal Strength Indicator (RSSI) has historically been one of the most widely used features for indoor localization, primarily due to its simplicity and the fact that it is available on almost all wireless transceivers at no additional cost [11]. The principle is based on the log-distance path loss model:

$$PL(d) = PL(d_0) + 10n \log_{10}\left(\frac{d}{d_0}\right) + X_\sigma,$$

where the path loss exponent n and shadowing variable X_σ translate the received signal power into a distance estimate. The estimated distance $\hat{d}$ is then used in trilateration or fingerprinting schemes to infer position.

2.6.1 Limitations of RSSI-Based Methods

Despite its popularity, RSSI-based localization suffers from several limitations:

- **Environmental sensitivity:** Multipath, shadowing, and temporal variations lead to large fluctuations in RSSI values, even when the true distance is constant.
- **Calibration dependency:** The path loss exponent n varies across buildings, rooms, and even different times of day, requiring costly site surveys and recalibration [12].
- **Low spatial resolution:** Small changes in distance often correspond to variations smaller than the intrinsic noise of RSSI measurements, limiting achievable accuracy to the order of meters.

- **Poor robustness in NLOS conditions:** Obstructions attenuate signals in unpredictable ways, producing severe positive biases in range estimates.

These drawbacks make RSSI an unreliable ranging observable in dense multipath environments such as offices, shopping malls, or industrial sites.

2.6.2 Advantages of Channel Sounding

In contrast, channel sounding techniques directly exploit the frequency- and phase-domain information of the received signal, which provides several advantages:

- **Higher resolution:** Phase measurements across multiple frequencies allow sub-wavelength ranging accuracy [7].
- **Reduced bias:** By isolating the first-arrival path in the CIR or using multi-carrier phase difference methods, the effects of multipath and shadowing can be significantly reduced.
- **Theoretical grounding:** Channel sounding performance can be formally analyzed using estimation theory (e.g., CRLB), offering quantifiable guarantees on accuracy limits [9].
- **Compatibility with modern BLE:** The introduction of IQ sampling and channel sounding in BLE 6.0 provides native support for such methods, making them feasible for commodity devices [29].

As a result, channel sounding represents a paradigm shift from empirical, calibration-heavy RSSI methods toward physics-based, measurement-driven ranging techniques.

2.6.3 Summary

This chapter has outlined the theoretical underpinnings of indoor propagation, BLE technology, channel sounding, and ranging methods. In particular, we have contrasted traditional RSSI–based localization,which remains attractive for its simplicity but limited in accuracy,with more advanced channel sounding techniques that exploit the rich information contained in the phase and frequency response of the channel. These concepts

form the foundation for the proposed localization system, which leverages IQ-based BLE measurements to achieve robust and accurate indoor positioning in multipath-rich environments.

Chapter 3

System Design

3.1 System Architecture

3.1.1 Overall System Overview

The proposed system consists of mobile tags(Channel Sounding Reflectors), fixed anchors(Channel Sounding Initiator), and a central gateway. Tags integrate environmental sensors and an inertial measurement unit (IMU) with a BLE radio (nRF54L15). Anchors are deployed at known positions indoors to receive periodic BLE broadcasts containing both sensor data and IQ samples for channel sounding. The gateway aggregates this data, performs multilateration using distance estimates, and provides a real-time view of tag location and sensor measurements.

3.1.2 Data Flow and Communication Model

Two distinct communication paths are implemented in the system: sensor data transmission and channel sounding for ranging.

- **Sensor data:** Each tag periodically transmits environmental measurements (temperature, humidity, pressure) using extended BLE connectionless advertising. These packets are received by multiple anchors and forwarded to the gateway for storage and analysis.

- **Channel sounding data:** BLE channel sounding is executed as a separate procedure, with the anchors acting as channel sounding *initiators* and the mobile tags serving as *reflectors*. The Nordic radio performs the low-level exchange of probe packets and internally processes the IQ samples. As a result, each pair provides a distance estimate derived from IFFT and phase change analysis. These distance values are collected at the anchors and forwarded to the gateway.

The gateway receives all information through the initiators. Each anchor acting as an initiator forwards both the environmental sensor readings it captures from advertisements and the distance measurements obtained from channel sounding. This transfer is performed over a UART interface, which is connected to the gateway through a UART-USB converter and retrieved via the USB Type-C port.

3.2 Hardware Design

3.2.1 SoC and Radio Subsystem

The nRF54L15 system-on-chip was selected due to its support for Bluetooth 6, efficient power consumption, and hardware IQ sampling. The device integrates a high-performance Cortex-M33 processor, a dedicated cryptographic accelerator, and a low-power 2.4 GHz transceiver, making it ideal for embedded localization tasks.

In this work, the nRF54L15 is used within the **ME54BS01** module manufactured by Minewsemi, which provides a compact and production-ready hardware platform with integrated RF design and antenna matching. This choice simplifies hardware development while retaining full access to the advanced channel sounding and BLE features of the nRF54L15.

3.2.2 PCB Design

3.2.2.1 Design Rules

One of the most important steps during PCB layout design is the adaptation of the board to the capabilities and limitations of the subsequent manufacturing process. For this

reason, a detailed study of the technical specifications of the selected manufacturer was performed in order to ensure compliance of the design with the available tools, processes, and production constraints. The correct configuration of the design parameters (design rules) during the early design phase is essential to avoid errors, reduce incompatibility risks, and improve both the quality and the cost-effectiveness of the final product.

The design rules define parameters such as the minimum track width, spacing between tracks, pads, and vias, as well as copper clearances. Adhering to these rules is critical for maintaining signal quality, avoiding electromagnetic interference, and ensuring reliable electrical performance of the circuit. Table 3.1 summarizes the key rules that were established and followed in the design of the present PCB.

Table 3.1: PCB Design Rules

Rule	**Value**
Preferred track widths	0.2 mm / 0.3 mm / 0.4 mm / 0.5 mm
Minimum annular width	0.1 mm
Minimum via diameter	0.5 mm
Preferred via diameter	0.6 mm
Minimum via hole	0.3 mm
Preferred via hole	0.3 mm
Copper to hole clearance	0.1 mm
Copper to edge clearance	0.5 mm
Minimum through hole	0.3 mm
Hole to hole clearance	0.25 mm
Minimum uVia diameter	0.2 mm
Minimum uVia hole	0.1 mm

3.2.2.2 PCB layers and 3D view

The PCB was implemented as a 4-layer stackup with dedicated inner planes for power and ground. This configuration provides low-impedance return paths and stable reference planes for both RF and digital subsystems, ensuring clean signal integrity while keeping the layout compact.

Because the ME54BS01 module integrates the nRF54L15 together with its RF front-end and a matched antenna, no discrete antenna design was required. The layout therefore concentrated on reducing interference, ensuring clean power delivery, and maintaining a solid grounding strategy. High-frequency decoupling capacitors and regulators were placed close to the module, while sensitive analog traces were routed away from high-speed digital

lines to minimize coupling.

Before analyzing the PCB stackup and physical implementation, it is useful to present the complete system schematic. This diagram illustrates the integration of the power supply, MCU, sensors, programming interface, and USB-to-UART bridge, providing the electrical foundation upon which the PCB layout was developed.

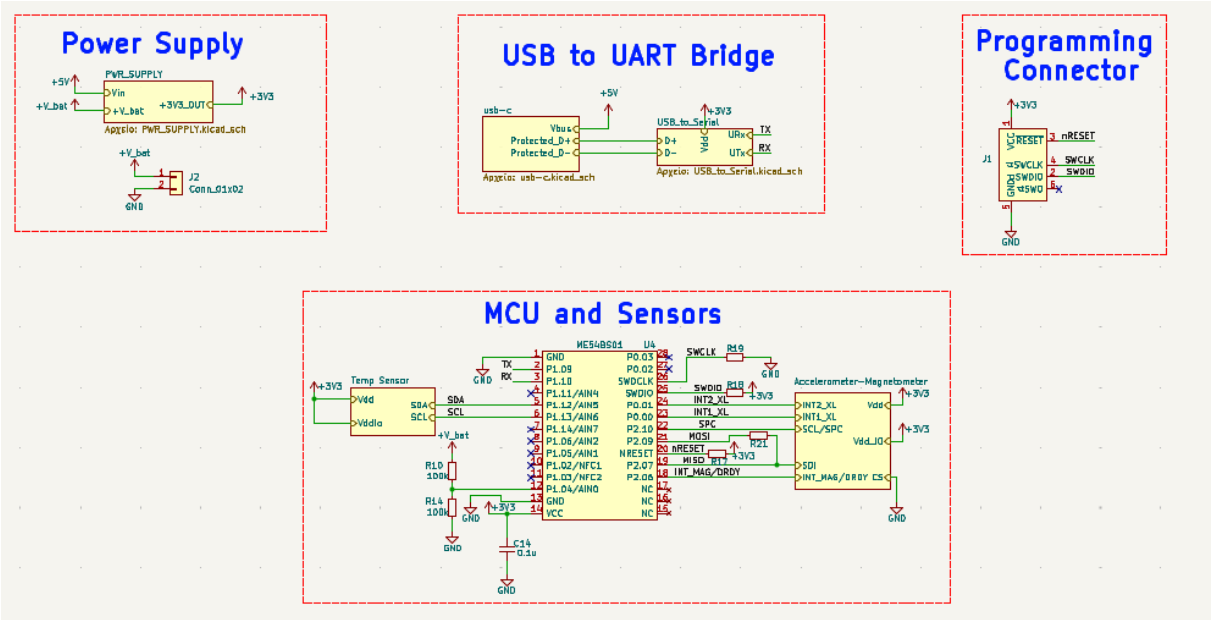

Figure 3.1: Complete schematic diagram of the system, showing the integration of power supply, MCU, sensors, and communication interfaces.

A key design choice was to dedicate the two internal layers to ground (In1) and power (In2), while leaving the outer layers (top and bottom) primarily for component placement and routing. This avoids splitting ground regions on the top and bottom layers, which can complicate return paths and require extensive ground stitching vias. By keeping the ground as a continuous inner plane, the design achieves excellent RF stability and noise reduction without the extra via stitching effort, thereby reducing both layout complexity and manufacturing cost.

The compact arrangement accommodates the ME54BS01 module, USB Type-C connector, charger, buckboost converter, and sensors within a small footprint. The result is a mechanically efficient layout that leverages the inner planes for electrical performance, while leaving the outer copper layers free for optimized routing of power management circuits, differential USB signals, and sensor interfaces.

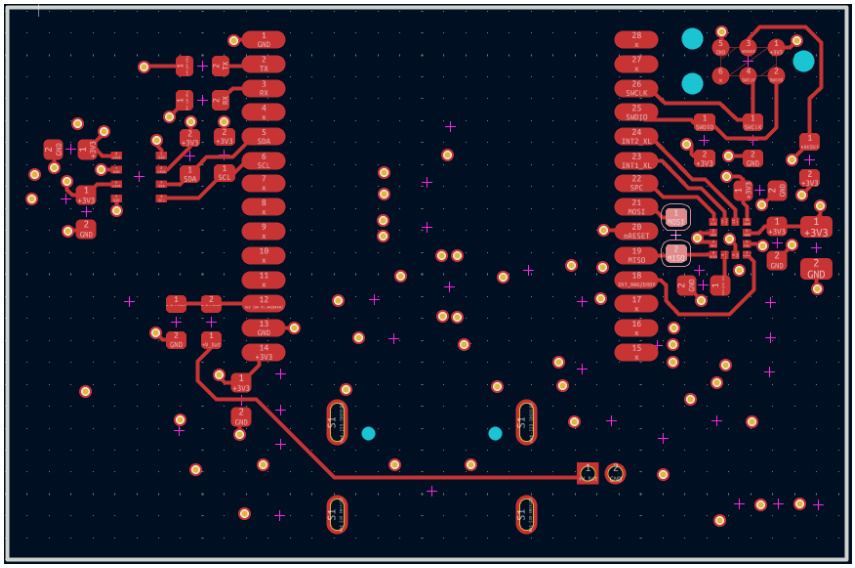

Figure 3.2: Top layer of the 4-layer PCB, showing placement of the ME54BS01 module, USB connector, and sensors.

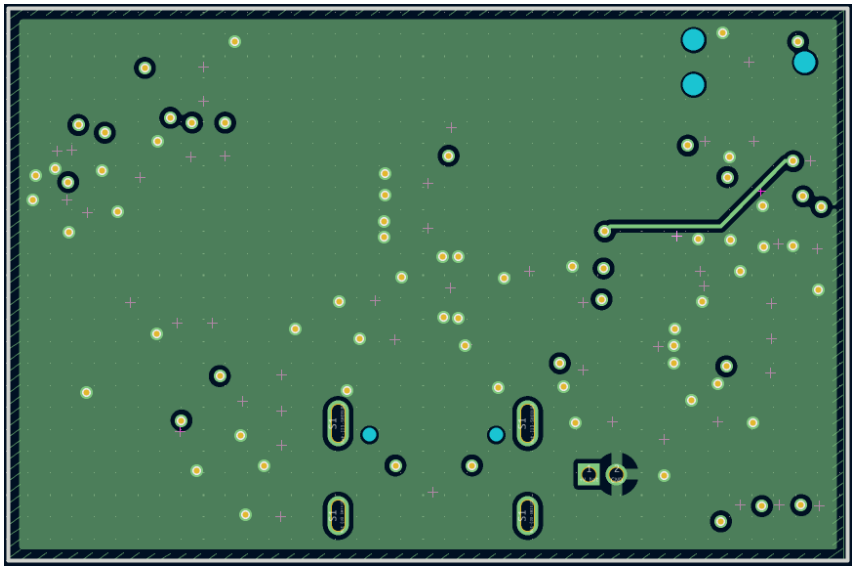

Figure 3.3: First inner layer: continuous ground plane providing RF stability and clean return paths.

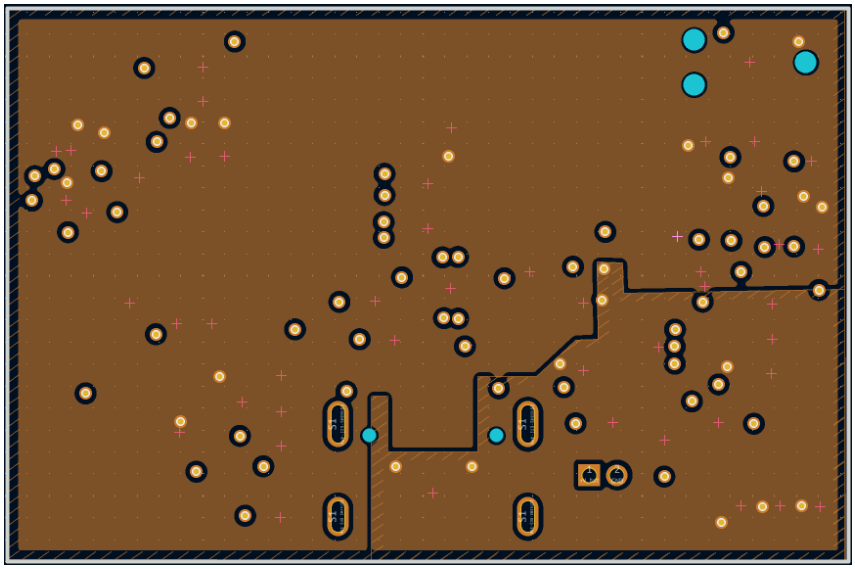

Figure 3.4: Second inner layer: dedicated power plane for 3.3V and 5V distribution.

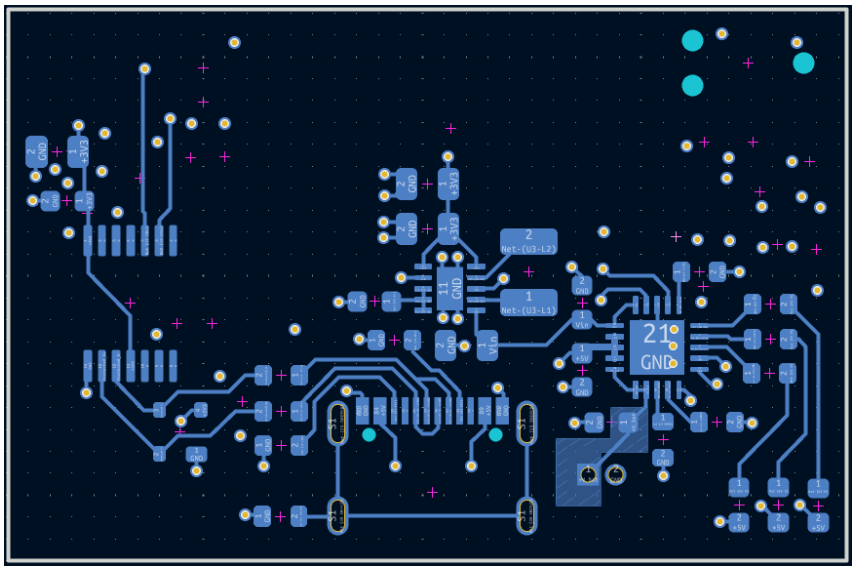

Figure 3.5: Bottom layer of the PCB, including power management circuits, USB differential pairs, and additional routing.

To provide a more intuitive understanding of the final assembly, 3D renderings of the PCB were generated from the KiCad model. These views illustrate the mechanical arrangement of the ME54BS01 module together with the supporting components such as the USB Type-C connector, charger IC, and sensors. The renders also highlight the compact integration achieved with the 4-layer stackup.

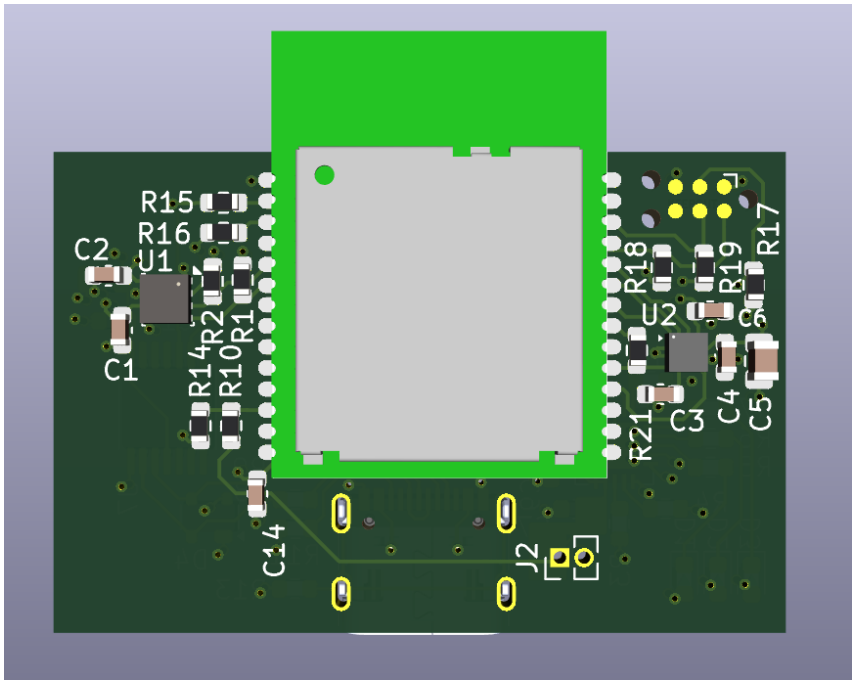

Figure 3.6: 3D render of the PCB (top view) showing placement of the ME54BS01 module and peripheral components.

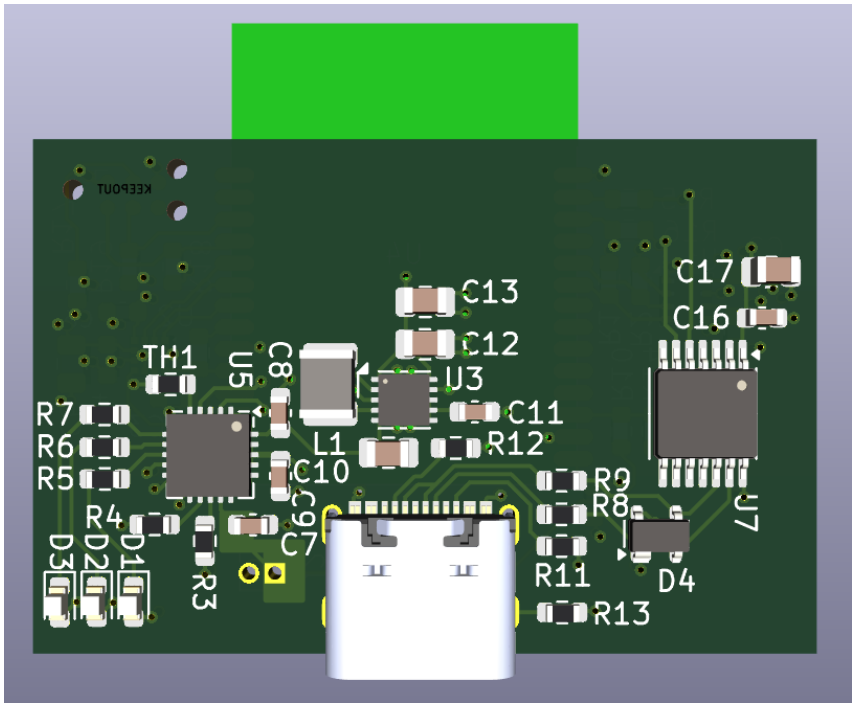

Figure 3.7: 3D render of the assembled PCB (angled perspective) illustrating the mechanical layout and overall compact design.

3.2.2.3 Power Management

The system is designed to operate either from a 5 V USB Type-C supply or from a single-cell lithium-ion battery. A Li-ion cell provides mobile operation when USB power is

unavailable.

3.2.2.3.1 Battery Charging Battery charging and power-path management are implemented using the MCP73871 charger IC. When USB power is connected, the IC charges the Li-ion cell while simultaneously supplying the system load through the `Sys_Load` rail. This ensures uninterrupted operation during charging.

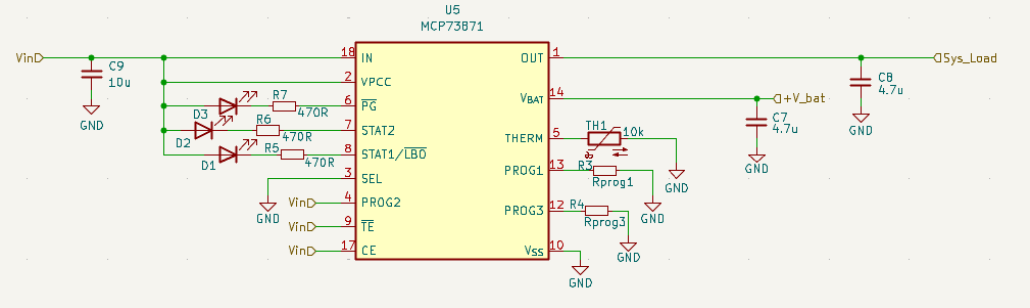

Figure 3.8: Schematic of the Li-ion battery charging stage using the MCP73871.

3.2.2.3.2 Voltage Regulation The regulated supply voltage for the digital and RF subsystems is generated by a TPS63031 buck–boost converter. This device accepts both the Li-ion battery voltage (3.0–4.2 V) and the USB input (5 V), providing a stable 3.3 V output regardless of input fluctuations. The regulated `+3V3_OUT` rail powers the nRF54L15 module (ME54BS01) and all integrated sensors.

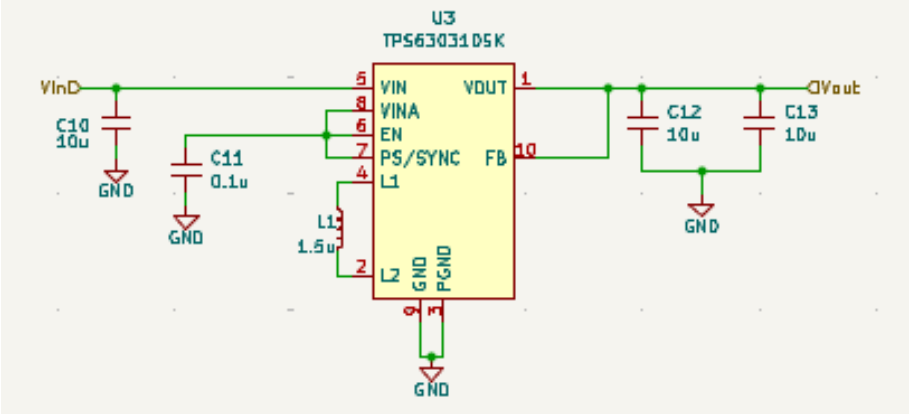

Figure 3.9: Schematic of the buck–boost regulator stage using the TPS63031.

3.2.2.3.3 Design Considerations The separation of the charger and buck–boost stages ensures flexibility and robustness. The system can seamlessly switch between USB and battery operation, with automatic charging of the battery when USB is present. Decoupling capacitors were added at both input and output stages to minimize voltage ripple, improving stability of the 3.3 V rail.

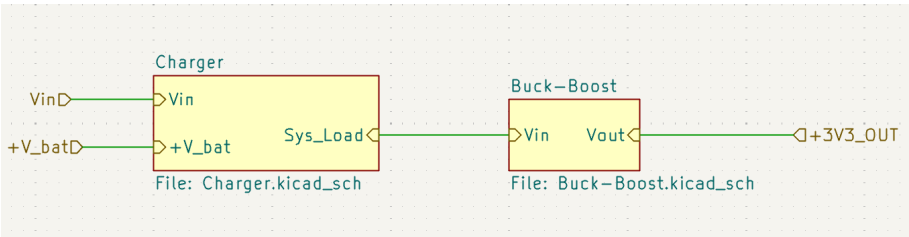

Figure 3.10: Block diagram of the complete power supply subsystem.

3.2.2.4 UART to USB Implementation

To enable communication between the embedded system and a host computer, a USB-to-UART bridge was implemented using a USB Type-C connector and a dedicated USB-to-serial converter IC (MCP2221AxST).

The front end of the design is the USB Type-C receptacle (Figure 3.12). The connector provides VBUS, D+, and D signals, while the CC1 and CC2 pins are biased with pull-down resistors to correctly advertise the board as a downstream device. The USB data lines are routed through series termination resistors and ESD protection diodes to ensure both signal integrity and robustness against transients. VBUS is regulated to +5V and used to power the converter circuit.

The USB-to-serial bridge (Figure 3.13) is implemented with the MCP2221A, which natively translates USB 2.0 data into UART signals. The device is powered from the +3.3V rail and includes local decoupling capacitors for supply stability. The D+ and D- lines from the USB connector are routed directly into the chip, while the Rx and Tx pins provide the UART interface to the ME54BS01 module. Series resistors are added to the UART lines to damp high-frequency edges and reduce EMI.

The complete block-level connection is shown in Figure 3.11, where the protected USB lines are connected from the Type-C receptacle to the USB-to-serial converter, and the translated TX/RX signals are exposed for direct interfacing with the module. This approach provides a reliable and cost-effective solution for debugging and programming, while also ensuring compliance with USB standards and ESD robustness.

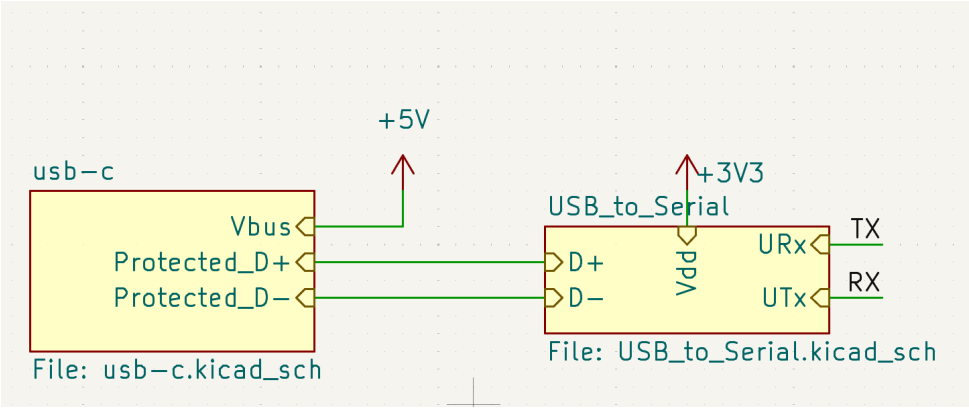

Figure 3.11: Block-level schematic showing USB Type-C to USB-to-Serial bridge connection.

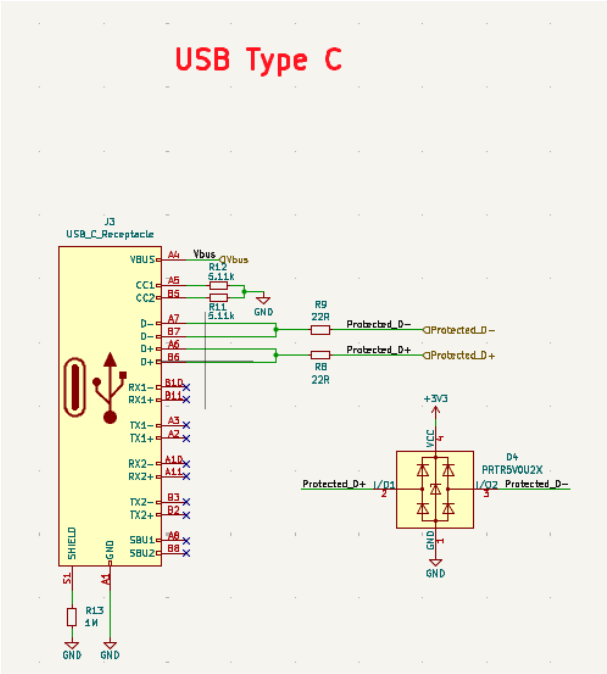

Figure 3.12: USB Type-C receptacle schematic with CC resistors, ESD protection, and data line filtering.

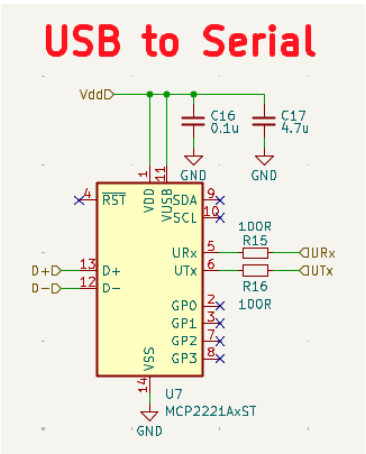

Figure 3.13: USB-to-serial bridge circuit using MCP2221A with UART signal breakout.

3.2.2.5 Temperature and Environmental Sensor Implementation

To monitor environmental conditions, the design integrates a Bosch BME280 sensor, which provides temperature, humidity, and pressure measurements in a compact package. The sensor communicates with the microcontroller over the I^2C interface, minimizing pin usage while ensuring reliable data transfer.

The BME280 is powered from the `VDDIO` and `VDD` rails, both decoupled with 0.1 uF capacitors placed close to the supply pins to suppress noise and stabilize the local power. The I^2C bus is implemented using the SDA and SCL lines, which are pulled up to `VDDIO` using 4.7 k resistors to guarantee valid logic levels and proper open-drain bus operation. The chip select (`CSB`) pin is tied high, fixing the device in I^2C mode instead of SPI.

This implementation ensures that the BME280 operates with high accuracy and minimal interference from the surrounding digital and RF subsystems. By leveraging the dedicated I^2C bus, the sensor can be easily addressed alongside other peripherals while maintaining straightforward integration into the system firmware.

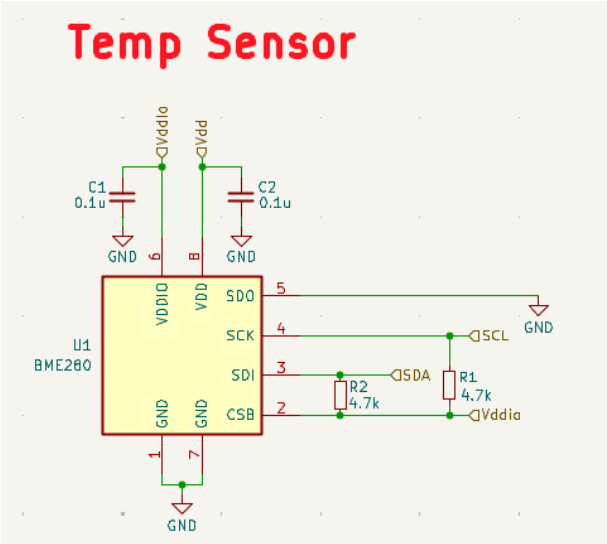

Figure 3.14: Schematic of the BME280 temperature, humidity, and pressure sensor connected via I^2C bus with pull-up resistors.

3.2.2.6 Accelerometer Implementation

To enable motion tracking and orientation sensing, the design integrates the ST LSM303AHTR, a combined 3-axis accelerometer and 3-axis magnetometer. This sensor provides both acceleration and magnetic field data, making it suitable for applications such as tilt detection, step counting, and compass functionality.In this project, the sensor was configured

to generate an interrupt signal to the MCU, enabling the device to wake up from sleep mode and thereby improve power efficiency during battery-powered operation.

The LSM303AHTR supports both I^2C and SPI communication, in this project, it is configured for 3-wire SPI operation to interface with the MCU. For reliable operation, the I/O voltage (`Vdd_IO`) is decoupled with a 0.1 uF capacitor, while the main supply (`Vdd`) is stabilized using a combination of 0.1 uF and 10 uF capacitors placed close to the IC. This arrangement ensures both high-frequency noise suppression and bulk charge storage to meet sudden current demands.

The LSM303AHTR provides multiple interrupt outputs (`INT1_XL`, `INT2_XL`, and `INT_MAG/DRDY`), which can be configured to signal events such as new data availability, free-fall detection, or orientation change. These pins are routed to the controller for flexible use in firmware, allowing low-power event-driven operation instead of constant polling.

This implementation ensures robust sensor performance in noisy environments while maintaining low power consumption.

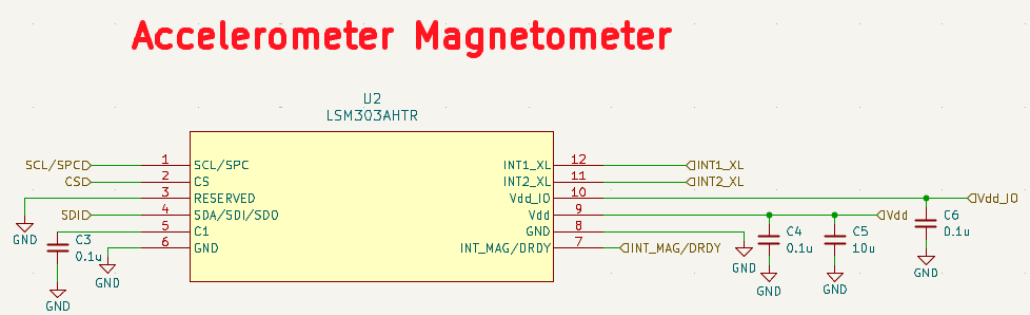

Figure 3.15: Schematic of the LSM303AHTR accelerometer and magnetometer with SPI interface, decoupling capacitors, and interrupt lines.

3.2.3 Microcontroller Unit (MCU)

The MCU is responsible for data acquisition, wireless communication, and the execution of the channel sounding procedures. For this work, the **nRF54L15** from Nordic Semiconductor was selected due to its combination of extremely low power consumption, advanced Bluetooth 6 support, and high computing performance. The SoC integrates an ARM Cortex-M33 core operating at 128 MHz, a FLPR RISC-V co-processor, and multiple hardware accelerators for cryptography and signal processing. This architecture provides sufficient computational resources for real-time localization algorithms, while maintaining very low energy consumption, which is critical for battery-powered tags and anchors.

In addition to the processing core, the nRF54L15 integrates a 2.4 GHz transceiver with hardware IQ sampling, enabling channel sounding for precise indoor ranging. Its rich set of peripherals, AMBA interconnect, and modular power domains allow efficient energy management and peripheral control. These features make the SoC an ideal choice for wireless sensing and tracking applications.

To simplify hardware integration, the **ME54BS01** module from Minewsemi was employed. This compact and cost-effective module incorporates the nRF54L15 SoC together with RF front-end, antenna matching network, and supporting passives, allowing for straightforward PCB design and rapid prototyping. By using the module, RF layout complexity is minimized while maintaining full access to the SoCs advanced BLE and processing features.

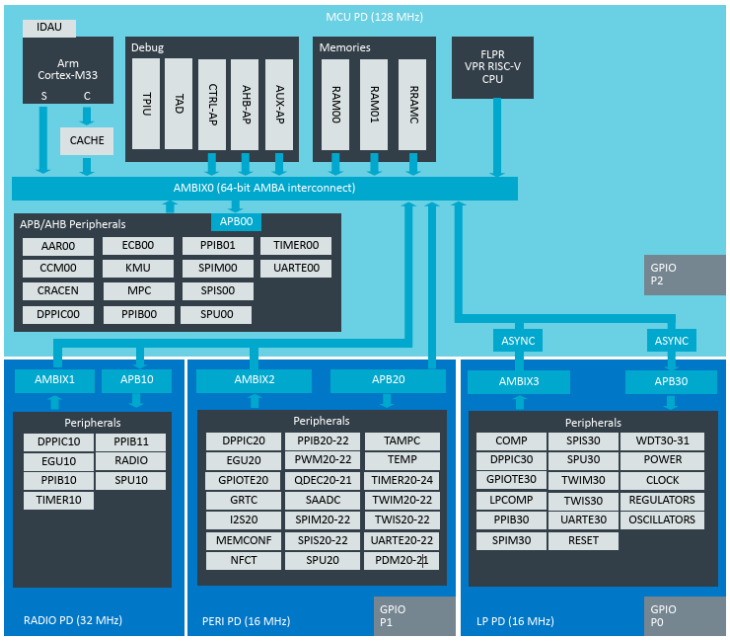

Figure 3.16: Block diagram of the nRF54L15 SoC architecture [35].

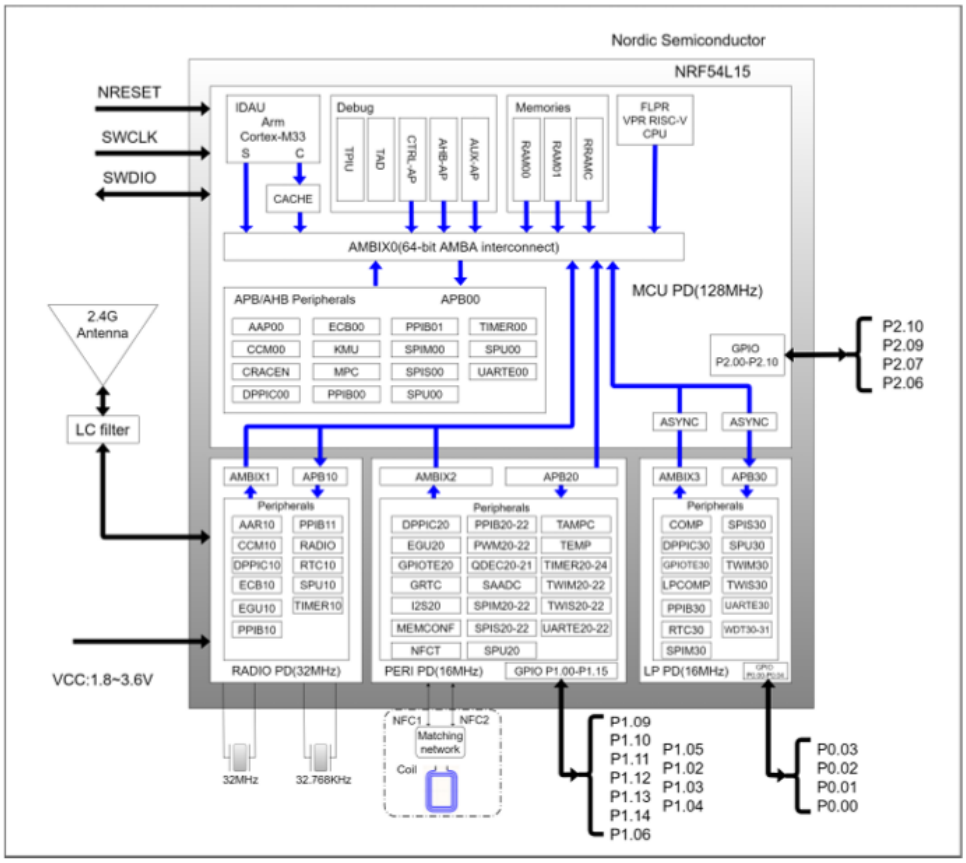

Figure 3.17: Block diagram of the ME54BS01 module integrating the nRF54L15 SoC [37].

3.2.4 Sensor Integration and Peripheral Communication

The tag integrates several sensors and peripheral interfaces, including:

- **Inertial Measurement Unit (IMU):** Provides motion and fall detection, interfaced through 3-wire SPI.
- **Environmental Sensors:** Measure temperature, pressure, and humidity for environmental monitoring via the I^2C bus.
- **USB–UART Bridge:** Enables debugging and provides a data communication channel.
- **Analog-to-Digital Converter (ADC):** Monitors the battery voltage level.
- **Bluetooth Low Energy (BLE):** Handles wireless connectivity and data transmission.

All sensors communicate with the SoC using either I^2C or SPI buses. Sampling synchronization is employed to align motion events with BLE transmissions, ensuring consistent

and time-coherent data transfer.

3.2.4.1 SPI Interface

The Serial Peripheral Interface (SPI) is a synchronous serial communication protocol originally introduced by Motorola, and has since become one of the most widely adopted standards for short-range digital interconnects in embedded systems. Unlike asynchronous interfaces such as UART, SPI relies on a dedicated clock signal generated by the master device to synchronize the data exchange with one or more slave devices.

The interface typically consists of four signals:

- **SCLK (Serial Clock):** Generated by the master to provide timing for all data transfers.
- **MOSI (Master Out, Slave In):** Unidirectional data line carrying information from the master to the slave.
- **MISO (Master In, Slave Out):** Unidirectional data line carrying information from the slave back to the master.
- **SS/CS (Slave Select or Chip Select):** Control line used by the master to activate a specific slave device during communication.

SPI supports full-duplex operation, as data can be shifted in and out simultaneously on the MOSI and MISO lines. Its main advantages are simplicity, very high throughput (tens of MHz are common in modern microcontrollers), and low protocol overhead, which makes it particularly well suited for fast sensor interfacing, ADC/DAC data acquisition, and memory device access.

In addition to the standard four-wire implementation, a half-duplex variant known as *three-wire SPI* is also used in certain systems. In this configuration, the MOSI and MISO pins are tied together into a single bidirectional data line. To reduce the risk of bus contention, a small series resistor (typically in the range of 100 Ω to 1 kΩ) is placed between the two pins. While this approach simplifies routing and reduces pin count, it restricts the interface to half-duplex communication, as simultaneous transmission and reception are no longer possible.

SPI does not implement intrinsic addressing. Each slave device requires a dedicated `CS` line, which can limit scalability in systems with a large number of peripherals. In practice, system designers must balance speed and wiring complexity when deciding to use SPI.

In the present design, SPI is employed for interfacing high-speed peripheral components, where deterministic timing and low-latency data transfer are essential for synchronizing sensor readings with the wireless subsystem.

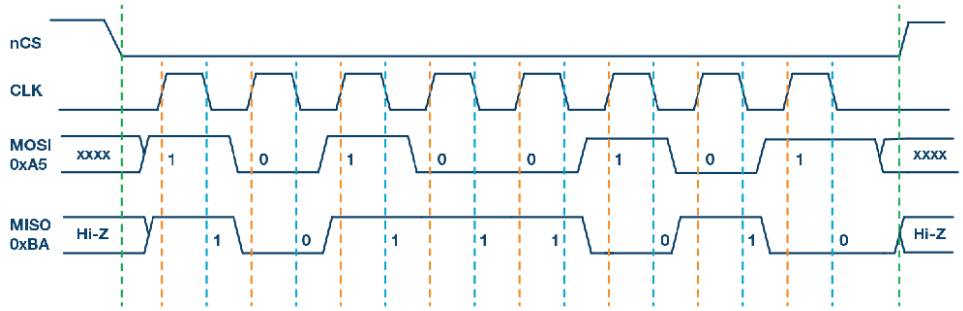

Figure 3.18: SPI timing diagram showing full-duplex data exchange between master and slave

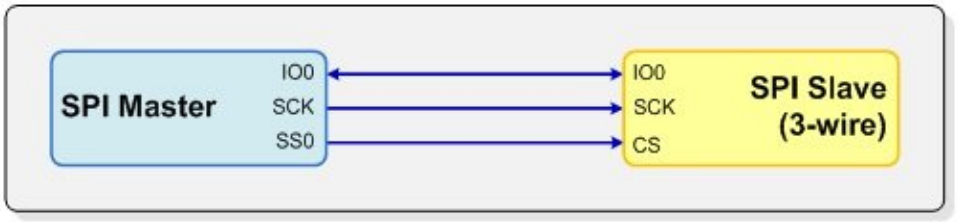

Figure 3.19: Three-wire SPI configuration. MOSI and MISO are combined into a single bidirectional data line

I^{2}C Interface

The Inter-Integrated Circuit (I^{2}C) bus is a synchronous, serial communication protocol originally developed by Philips (now NXP) and widely adopted in embedded systems. In contrast to SPI, which primarily follows a master-slave architecture with dedicated chip select lines, I^{2}C was designed for multi-master, multi-slave communication over a shared two-wire bus. Its main advantage lies in simplicity of wiring: only two signals are required regardless of the number of devices connected.

The two lines are:

- **SCL (Serial Clock Line):** Provides the clock signal, always generated by the master during communication.

- **SDA (Serial Data Line):** A bidirectional line used to transmit or receive data bits between master and slave devices.

Each device on the bus has a unique 7-bit or 10-bit address, allowing multiple peripherals to coexist without the need for separate chip select pins. Communication is organized into data frames, which typically consist of:

1. A **Start condition**, where the master pulls SDA low while SCL is high.
2. A 7- or 10-bit **slave address** followed by a read/write bit.
3. An **acknowledge bit**, driven by the addressed slave to confirm reception.
4. One or more **8-bit data bytes**, each followed by an acknowledgment.
5. A **Stop condition**, where SDA is released high while SCL is high.

The effective data rate of I^2C communication can vary depending on configuration and bus conditions. In the present implementation, the bus was configured to operate at **250 kbps**, which provides a good balance between robustness and throughput for periodic acquisition of environmental sensor data in the indoor tracking system. Because I^2C relies on open-drain signaling, external pull-up resistors are included on both SDA and SCL lines to ensure reliable logic-level recovery.

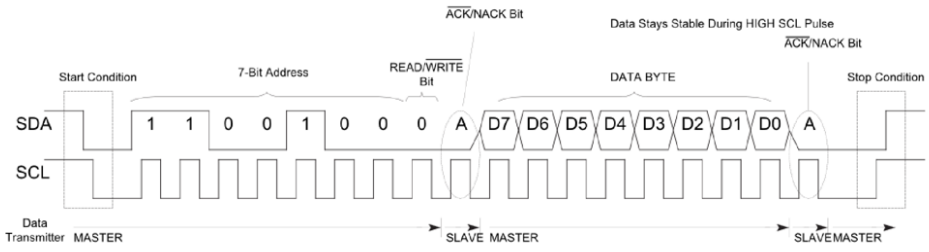

Figure 3.20: I^2C data transfer sequence

Analog-to-Digital Converter (ADC) Interface

An Analog-to-Digital Converter (ADC) is a fundamental building block in embedded systems, responsible for converting continuous analog signals into discrete digital values that can be processed by the microcontroller. Most modern ADCs are based on the Successive Approximation Register (SAR) principle, which iteratively compares the input voltage against reference levels using a comparator and an internal DAC until the closest

digital representation is found. The resulting digital code is expressed with a finite resolution, commonly 8 to 16 bits, which determines the smallest voltage step that can be distinguished. In addition, performance metrics such as sampling rate, reference voltage, and input configuration (single-ended or differential) influence the ADCs precision and suitability for different applications.

The ME54BS01s nRF54L15 SoC integrates a **Successive Approximation Register ADC (SAADC)** with configurable resolution, gain, and input modes, offering flexibility and precision for analog measurements [36]. In this design, the SAADC is dedicated to monitoring battery voltage to ensure safe and reliable device operation.

Key Features and Configuration

- **Channel:** The `AIN0` input, mapped to pin `P1.04`, is configured in single-ended mode.
- **Resolution:** Operated at 12-bit resolution, providing 4096 discrete levels sufficient for precise battery monitoring without excessive conversion latency.
- **Reference voltage and gain:** Configured to match the maximum expected battery voltage, maximizing dynamic range and reducing quantization error.
- **Sampling and oversampling:** Battery voltage is periodically sampled; optional oversampling can be used to reduce noise and improve effective resolution.
- **Buffering and events:** The SAADC leverages EasyDMA to store conversion results in memory buffers. Events are triggered when buffers are filled, allowing efficient processing or BLE transmission.
- **Calibration:** Internal calibration is supported to correct for offset and gain errors, ensuring stable accuracy across temperature and supply variations.

Role and Integration

- Periodic ADC sampling allows continuous tracking of the battery voltage while minimizing energy consumption.
- Converted values are processed in firmware to estimate charge status and detect undervoltage conditions, which can then be reported over BLE.

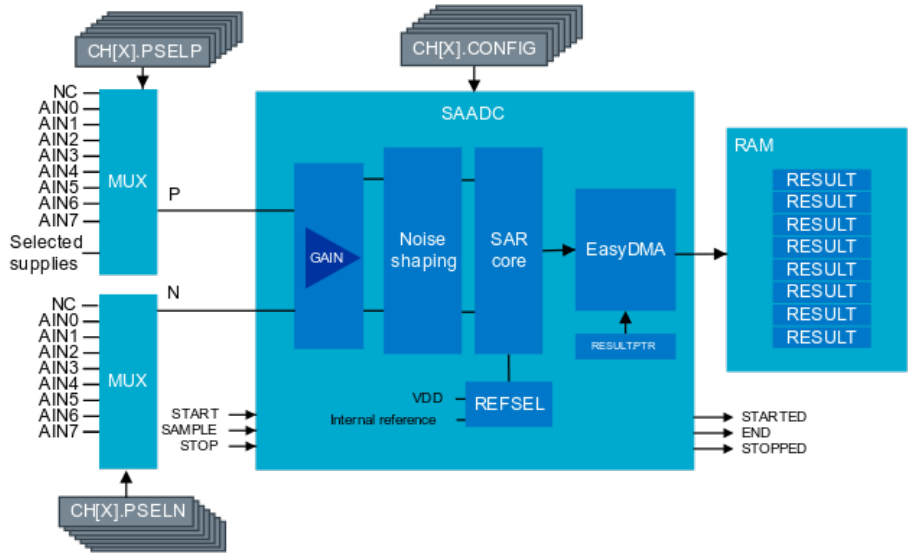

Figure 3.21: Block diagram of the nRF54L15 SAADC architecture [36].

UART Interface

UART is one of the most widely used asynchronous serial communication protocols in embedded systems. It enables full-duplex data exchange between two devices using only two signal lines: TX (transmit) and RX (receive). Unlike synchronous interfaces such as SPI or I^2C, UART does not rely on a shared clock signal. Instead, both transmitter and receiver must agree in advance on the transmission parameters, typically including baud rate, word length, parity bit, and stop bits.Data is transmitted in discrete *frames*, each consisting of:

- a **start bit**, indicating the beginning of the frame,
- a configurable number of **data bits** (commonly 8),
- an optional **parity bit** for error detection, and
- one or more **stop bits** to signal the end of the frame.

The absence of a clock makes UART simple to implement in hardware and highly robust for point-to-point communication over short distances. Error detection is provided through parity and framing checks, while buffering and flow control mechanisms (hardware CTS/RTS or software XON/XOFF) can be added if required.

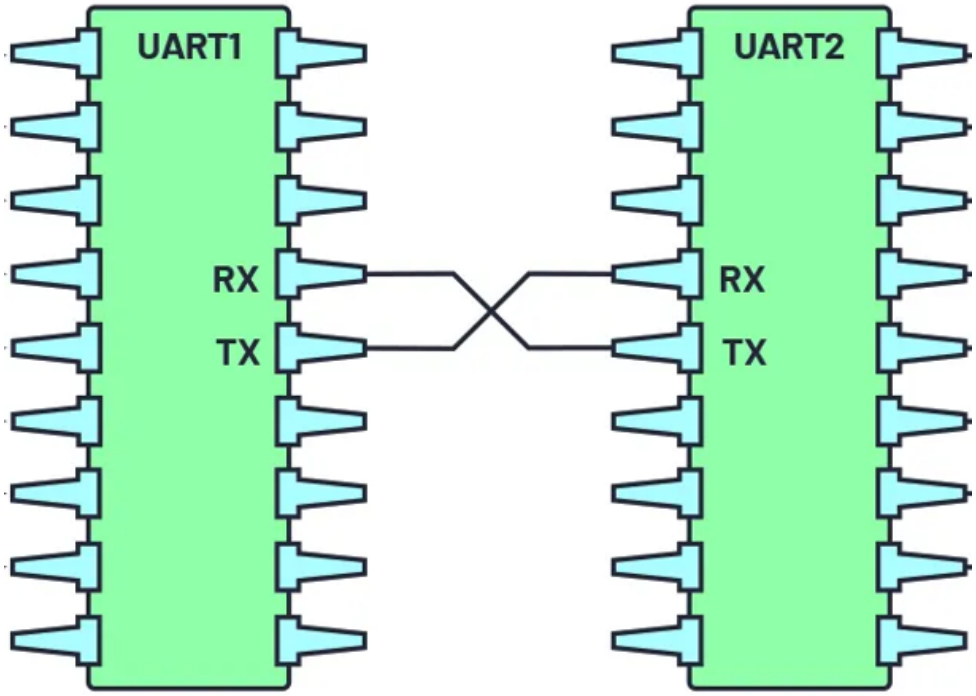

Figure 3.22: Example of Direct UART connection between two devices

USB (Universal Serial Bus)

USB (Universal Serial Bus) constitutes the dominant standard for interconnection between computers and peripheral devices, enabling both data exchange and power delivery through a single unified channel. Its communication model is based on a *host-device* architecture, where the host (e.g. a personal computer) maintains full control of the bus, while the connected devices respond to host requests. The USB specification defines both the physical layer (cables, connectors, electrical signaling) and a multi-layer communication protocol that regulates the flow of information through well-defined channels with specific roles and directions.

At the physical level, USB employs differential signaling over the D+ and D- lines. This approach reduces common-mode noise and improves robustness in electrically noisy environments. Advanced timing, synchronization, and error-detection mechanisms, such as NRZI (Non-Return-to-Zero Inverted) encoding and CRC (Cyclic Redundancy Check), ensure reliable data transmission. The protocol supports four fundamental transfer types:

- **Control transfers**, used for configuration and commands,
- **Bulk transfers**, providing reliable transport of large volumes of data,

- **Interrupt transfers**, intended for periodic and latency-sensitive data,
- **Isochronous transfers**, guaranteeing timing for real-time applications such as audio and video.

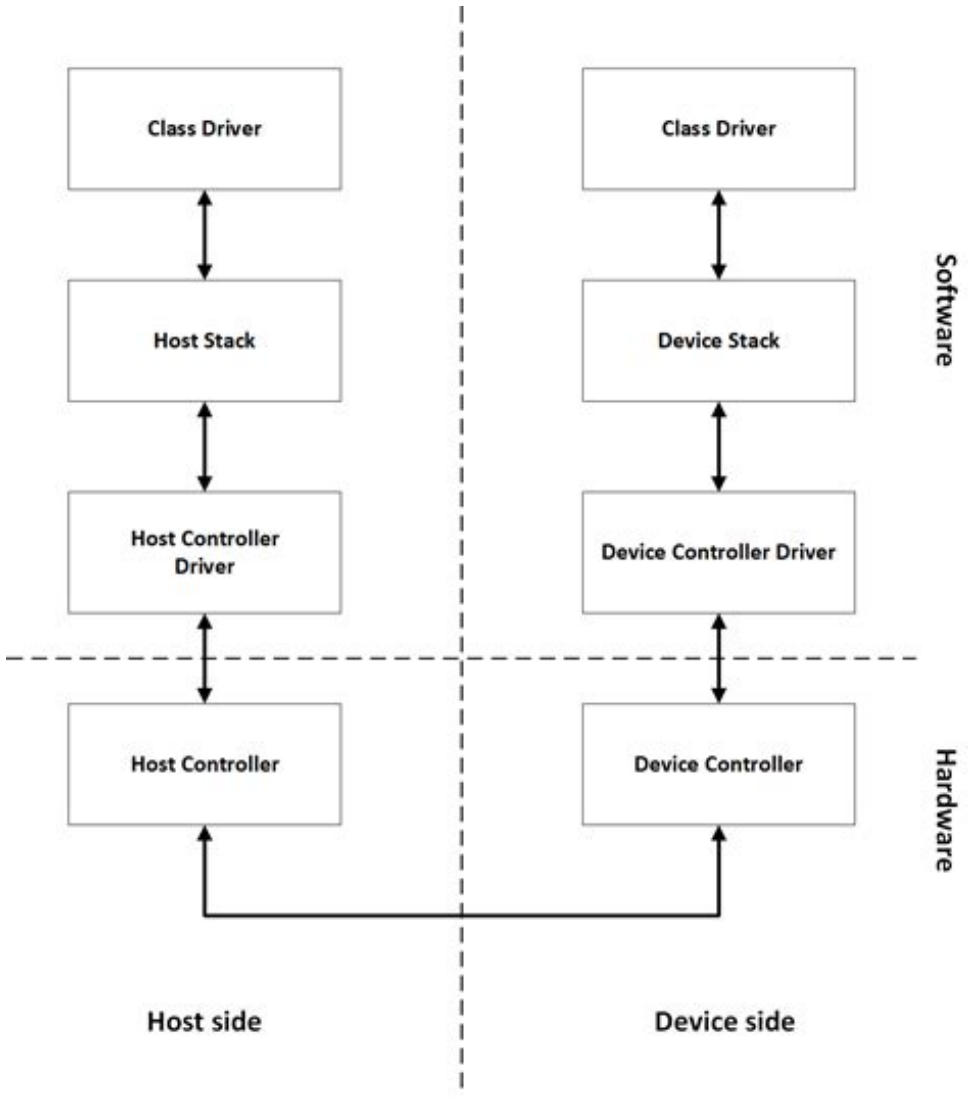

Figure 3.23: USB 2.0 protocol stack architecture illustrating the layered separation between Host and Device.

In the present system, the USB functionality is not implemented natively by the MCU (nRF54L15), but rather delegated to an external **MCP2221A** bridge manufactured by Microchip. This device translates the asynchronous UART byte stream from the SoC into USB frames, presenting itself to the host as a *CDC-ACM* (Communication Device Class Abstract Control Model) device. As a result, the system enumerates as a Virtual COM Port on the host computer, which allows transparent serial communication without requiring additional drivers on most operating systems.

The chosen implementation follows the USB 2.0 Full-Speed specification, supporting data rates up to 12 Mb/s[42]. Through this architecture, the simplicity and low-power oper-

ation of UART are preserved within the embedded device, while the host benefits from the universality and wide adoption of USB. The Type-C connector used in the hardware design further provides mechanical robustness and reversibility, while also supplying 5 V power to the charging and regulation subsystem.

Implementation in the Present System

In this system, the nRF54L15 communicates over UART at a fixed baud rate with an external **MCP2221A** bridge from Microchip. The MCP2221A translates the asynchronous UART stream into USB CDC-ACM, presenting the device to the host computer as a virtual COM port accessible via the USB Type-C connector. This setup combines the simplicity and low power consumption of UART with the universality of USB connectivity, ensuring compatibility with standard PCs and gateways.

All environmental sensor readings (temperature, humidity, pressure, and acceleration data) as well as distance estimates derived from BLE channel sounding are forwarded through this interface. The separation of wireless communication (BLE) and wired communication (UART-to-USB) improves modularity: BLE is reserved for indoor localization and sensing tasks, while the UART provides a reliable and low-latency data pipeline to the gateway or host system.

Bluetooth Low Energy (BLE)

Bluetooth Low Energy (BLE) is a wireless communication standard introduced in Bluetooth 4.0, engineered for ultra-low-power, short-range applications. Unlike Bluetooth Classic, which emphasizes high-throughput continuous connections, BLE enables intermittent or event-driven transmissions with minimal energy consumptionmaking it well suited for IoT, wearable, and sensing devices [59].

At the firmware and protocol level, BLE is organized into a **Controller-Host architecture**. The Controller encompasses the **Physical Layer (PHY)** and the **Link Layer (LL)**, which are responsible for radio signaling, channel access, and packet framing. The Host layer, on the other hand, includes higher-level protocols such as the **Logical Link Control and Adaptation Protocol (L2CAP)**, the **Attribute Protocol (ATT)**, and the **Generic Attribute Profile (GATT)**. Together, these manage logical channels, attribute storage and access, and application data formatting respectively [52]. The **Generic Access Profile (GAP)** defines how devices discover each other, advertise their

presence, and establish connections, whereas the GATT layer organizes system data into **Services** and **Characteristics** using the ATT as transport-allowing application-level services to read, write, or notify sensor values through structured attributes [53, 60].

Nordic Semiconductor has significantly advanced BLEs capabilities through early adoption of features like Bluetooth 5.0s high-speed 2 Mbit/s PHY and direction-finding from Bluetooth 5.1, culminating in Bluetooth 5.4 and Core 6.0 support for **Channel Sounding** [49]. Channel Sounding leverages **Phase-Based Ranging (PBR)** and **Inverse Fast Fourier Transform (IFFT)** to derive accurate and secure distance estimates: PBR computes phase differences across multiple frequencies, while IFFT provides cryptographic distance bounding to resist relay attacks, achieving centimeter-level accuracy [29, 26]. In this system, BLE is used not only for wireless transport but also as the foundation for **precise indoor localization** via channel sounding. This method outperforms traditional RSSI-based approaches in accuracy and robustness, without the need for complex hardware such as multi-antenna AoA setups.

Furthermore, BLEs modular design enables dissemination of sensor data via a **connectionless GATT service**, implemented at the firmware level using BLE advertising packets. Sensors like temperature and environmental monitors are encapsulated as GATT Services and Characteristics, rather than forming a bonded connection, the firmware periodically broadcasts short, structured advertisement payloads containing sensor readingsthereby conserving power, reducing latency, and supporting scalable multi-receiver reception in dense IoT deployments.

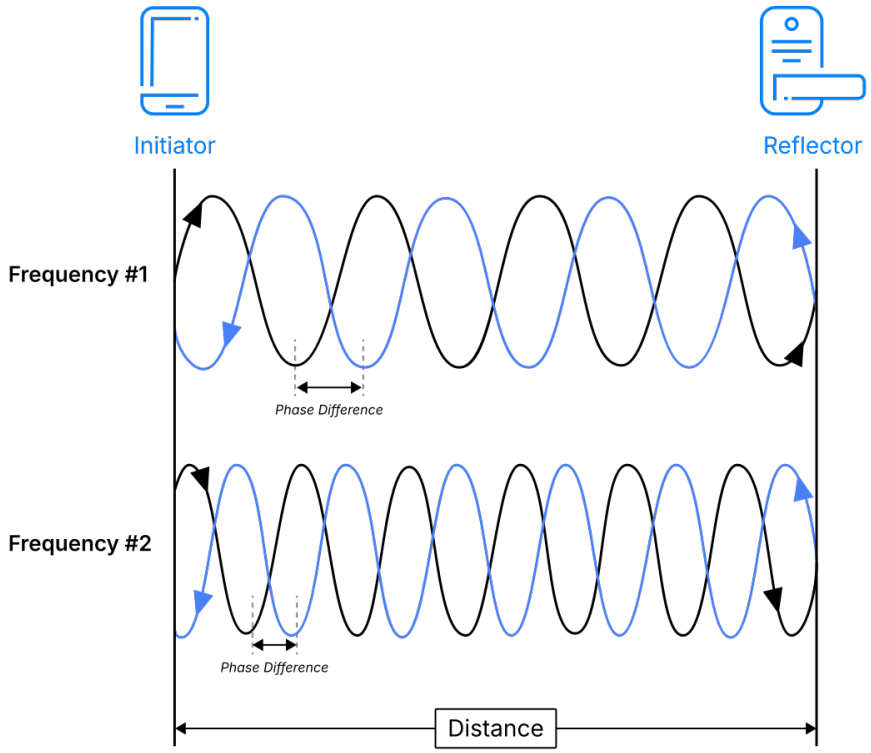

Figure 3.24: Illustration of Phase-Based Ranging (PBR), where distance is estimated from phase differences across multiple carrier frequencies.

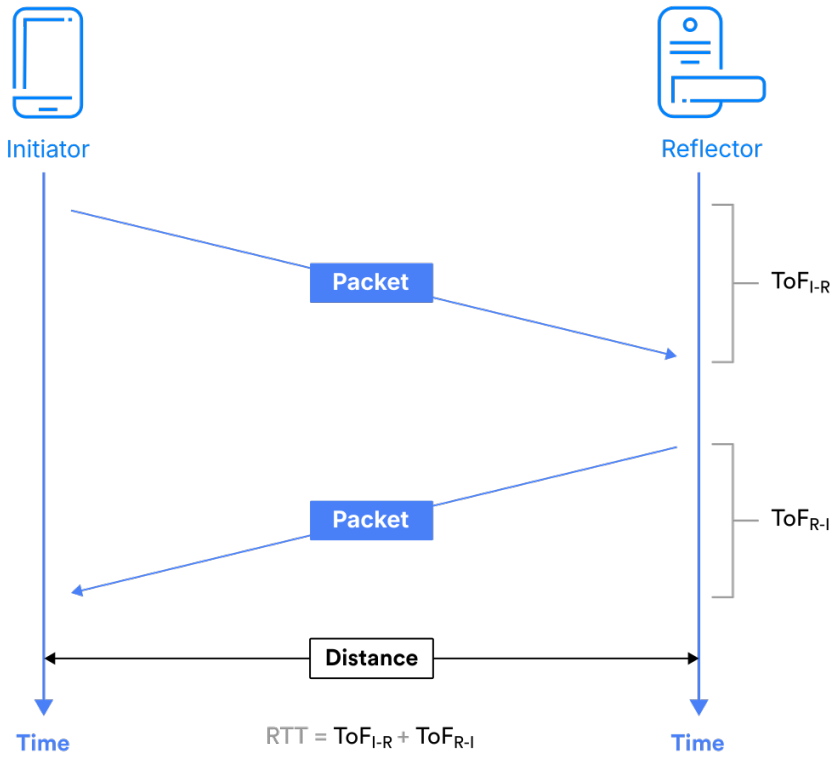

Figure 3.25: Illustration of Round-Trip Time (RTT), where distance is derived from the measured time it takes for signals to travel to the peer device and back.

3.3 Software Design

3.3.1 Firmware Architecture

The firmware has been designed to achieve two primary goals:

- Support reliable **channel sounding** procedures, enabling precise ranging between devices.
- Collect and transmit **environmental data** from the BME280 sensor (temperature, pressure, humidity) along with device battery voltage and a wake-up/sleep schedule optimizing power performance.

To meet these goals, the firmware is organized into independent but cooperating tasks: sensor acquisition, BLE advertising, and channel sounding. A cooperative scheduler ensures deterministic execution of these tasks while keeping the system lightweight and power efficient. Furthermore, the modular design allows individual subsystems to be updated or replaced without affecting the rest of the system. This flexibility is important for supporting different experimental setups or extending the solution to additional sensors and protocols.

Since the implementation is based on the **nRF54L15** platform, the **Zephyr RTOS** was used to provide kernel services such as `kthreads`, synchronization primitives, and event handling. This enables a clean separation of concerns between concurrent tasks, ensures predictable timing behavior, and simplifies the integration of power management mechanisms, sensor drivers, and BLE stack operations.

3.3.1.1 Initiator Firmware

The initiator device is responsible for discovering peers, establishing secure connections, and running the channel sounding procedures. It begins with performing a passive scan to identify devices offering the ranging service, sets up security and service discovery, and then configures the channel sounding parameters. During operation, the initiator collects ranging data, processes it to derive distance estimates, and fuses the results using IFFT and phase calculations. In parallel, it can subscribe to connectionless GATT notifications to log environmental sensor data received from the reflector.Then, every two seconds,

it logs the distance estimates via the UART-USB subsystem and, when available, the environmental data, thus allowing a completely separate data acquisition process.

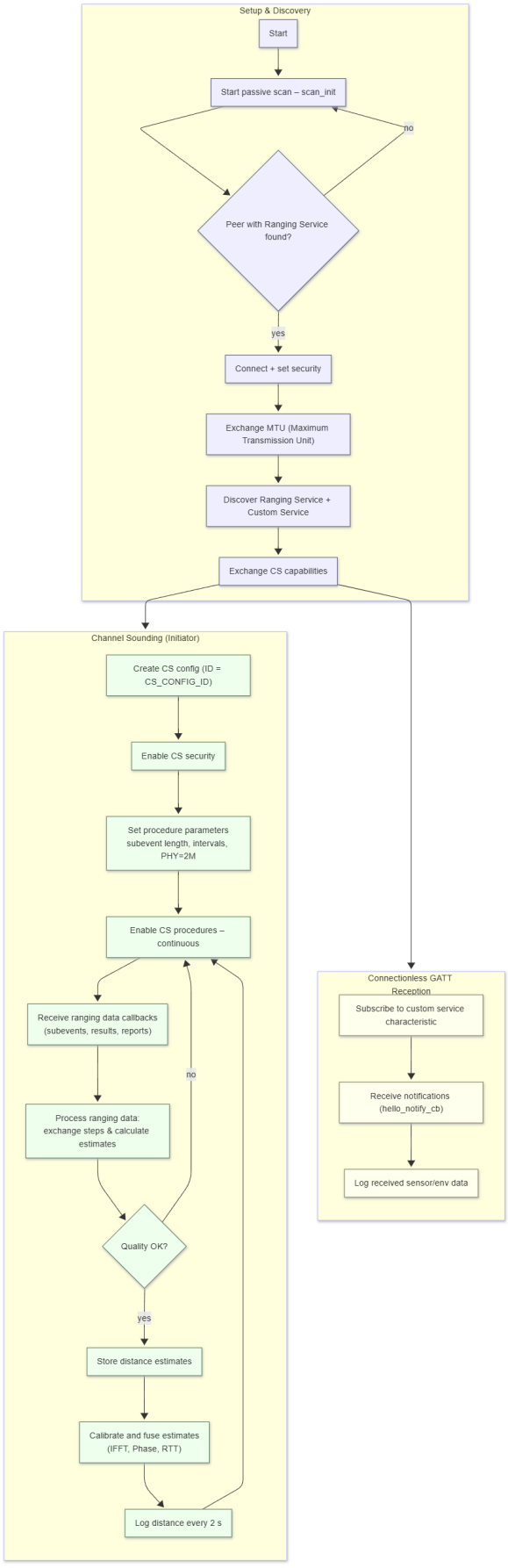

Figure 3.26: Flowchart of the firmware architecture for the initiator device.

3.3.1.2 Reflector Firmware

The reflector device is responsible for providing environmental data ,acting as the counterpart in the channel sounding procedure and controlling the state of the device form the accelerometer interrupts. It initializes the BME280 sensor and the accelerometer, creates BLE advertising sets, and periodically updates the advertising payload with fresh sensor data and battery status. When a channel sounding connection is established, the reflector assumes the role of a responder (reflector role), ensuring synchronization with the initiator. Additionally, a power management routine is implemented to optimize energy consumption, where the accelerometer detects motion events and triggers wake-ups from sleep mode.

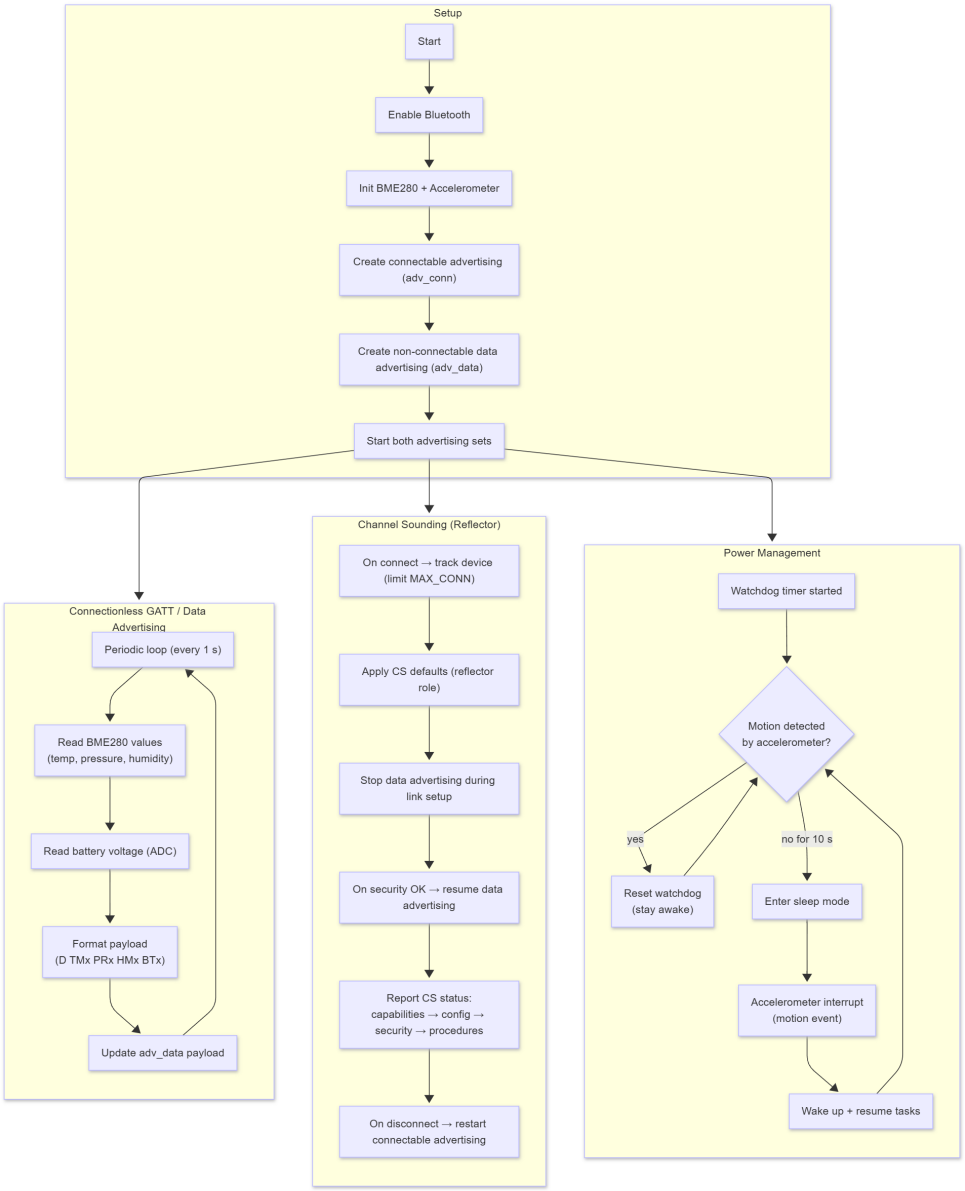

Figure 3.27: Flowchart of the firmware architecture for the reflector device.

3.3.2 Debugging and Logging Tools

For day-to-day observation and dataset collection, the system used a simple **UART–USB** console. Logs were viewed with **PuTTY** for quick inspection, while a small **Python** script (based on `pyserial`) recorded timestamped lines to files (CSV/JSON) for later analysis. This path carried sensor readings (BME280), battery voltage, and ranging outputs (IFFT/PBR summaries) at a modest baud rate, keeping the setup reproducible and lightweight.

For firmware flashing and debugging, a **SEGGER J-Link** probe was employed through the **SWD (Serial Wire Debug)** interface provided on the PCB. No full JTAG header was included in the designonly the compact two-wire SWD connection was implemented, as it provides equivalent functionality for ARM Cortex-M devices while reducing pin count and board space. This setup enabled reliable firmware programming, breakpoint-based debugging, and register inspection without interfering with the UART logging interface. When high-speed, pinless tracing was required, **SEGGER RTT** was used over the same SWD interface to stream logs directly to the host.

Summary: UART with PuTTY/Python was used for experimental logging and data acquisition, while J-Link over SWD provided efficient firmware flashing and non-intrusive debugging.

Chapter 4

Experimental Evaluation

4.1 Evaluation Subsystem Design

In the current implementation, no real-time floor plan plotting software has been developed. Instead, the evaluation was carried out using **Python** together with custom scripts tailored for each test scenario. These scripts were responsible for gathering the logged data and plotting the results in different formats, depending on the requirements of each experiment.

4.2 Stepped–Distance Error Characterisation

To quantify ranging accuracy across a set of discrete ground-truth distances and to evaluate which of the two estimators (**IFFT** and **Phase-Based Ranging**) provides higher accuracy, a stepped-distance experiment was performed. The reflector was positioned at five known ranges, $d_{\text{true}} \in \{1, 2, 3, 4, 5\}$ m, and at each step **60 sequential measurements** were collected from the same initiator/reflector pair. For each measurement, the combined distance estimate (`Dist`) was obtained as the arithmetic mean of the *IFFT* and *PBR* results, while both metrics were also logged individually to assess their independent performance.

Error definition and processing: For every sample k we compute instantaneous errors

for the three estimators:

$$e_{\text{IFFT}}[k] = d_{\text{IFFT}}[k] - d_{\text{true}}, \quad e_{\text{Phase}}[k] = d_{\text{Phase}}[k] - d_{\text{true}}.$$

Timestamps are not used for the plot. Instead, samples are shown on a *uniform index axis* ($k = 1, \ldots, N$) so each capture appears as a continuous sequence. Segment boundaries (where d_{true} changes) are indicated by vertical dashed lines and alternating shaded bands. Within each band we report the **per-segment averages** (Avg IFFT ,Avg Phase and Avg Dist), corresponding to the mean error of each estimator over the 60 samples at that true distance.

Visualisation: Figure 4.1 shows the two error series versus sample index. The shaded regions mark the five groundtruth distances (1–5 m), and the text boxes inside each region summarize the average errors for that segment. This view makes it easy to compare estimator bias and variability at each range while ignoring timing.

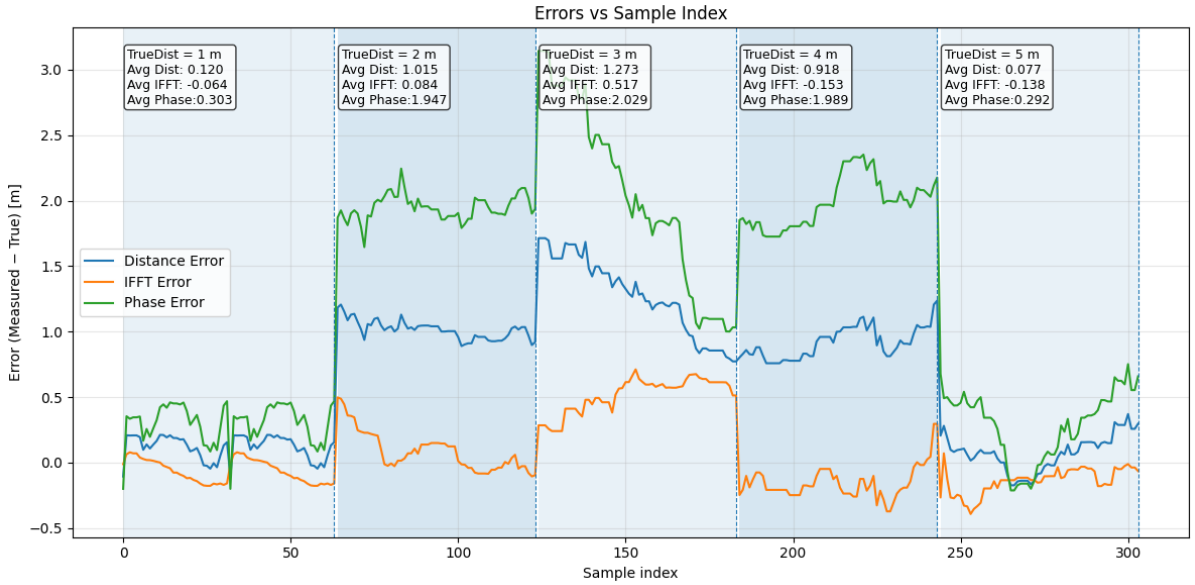

Figure 4.1: Errors vs. sample index for the stepped-distance experiment.

True Distance [m]	Avg Dist [m]	Avg IFFT [m]	Avg Phase [m]
1	0.120	-0.064	0.303
2	1.015	0.084	1.947
3	1.273	0.517	2.029
4	0.918	-0.153	1.989
5	-0.077	-0.138	0.292
Average	**0.650**	**0.049**	**1.312**

Table 4.1: Average errors per true distance (from plot annotations).

Results: From Figure 4.1 , it can be observed that the ranging system maintains consistent behaviour across all measured distances, with only moderate bias variations between

the estimators. The **average absolute distance error** over all ranges is approximately **0.65 m**, confirming that the distance estimation pipeline remains stable even in the presence of multipath reflections and environmental noise.

The **IFFT-based estimator** shows the lowest mean bias (**0.049 m**), demonstrating that the coarse range estimation obtained in the frequency domain is both robust and well-centered around the true values. In contrast, the **Phase-based estimator** exhibits higher variability, with a mean deviation of about **1.31 m**, indicating that while phase unwrapping provides fine-grained resolution at short distances, its accuracy degrades significantly for longer ranges due to ambiguity and phase wrapping effects.

Overall, the stepped-distance evaluation shows that the implemented ranging method achieves sub–metre performance in near-field conditions and maintains consistent error behaviour. Based on the obtained results, it is evident that the **IFFT-based ranging** approach provides superior stability and accuracy compared to the Phase-based estimator, and should therefore be preferred for reliable distance estimation in practical indoor localisation scenarios.

4.3 One Initiator One Reflector Case

The evaluation was conducted using a minimal configuration consisting of a single **initiator** and a single **reflector** device. The devices were positioned across a busy hallway, with a separation distance of approximately 2.7 m. This setup was selected in order to test the robustness of the system under realistic indoor conditions, where multipath effects and interference are present due to human movement and surrounding infrastructure.

Figure 4.2: Test setup with one initiator and one reflector device placed 2.7 m apart across a hallway for BLE channel sounding distance estimation.

Figure 4.3 shows the measured distance over time for the experimental setup with one initiator and one reflector device separated by 2.7 m. The measured distance closely follows the real value, indicated by the dashed orange line. Despite small fluctuations caused by multipath and interference in the hallway environment, the system demonstrates stable performance with an **average error of** 0.18 **m** across 740 samples. This result validates the effectiveness of the channel sounding approach for short-range indoor scenarios.

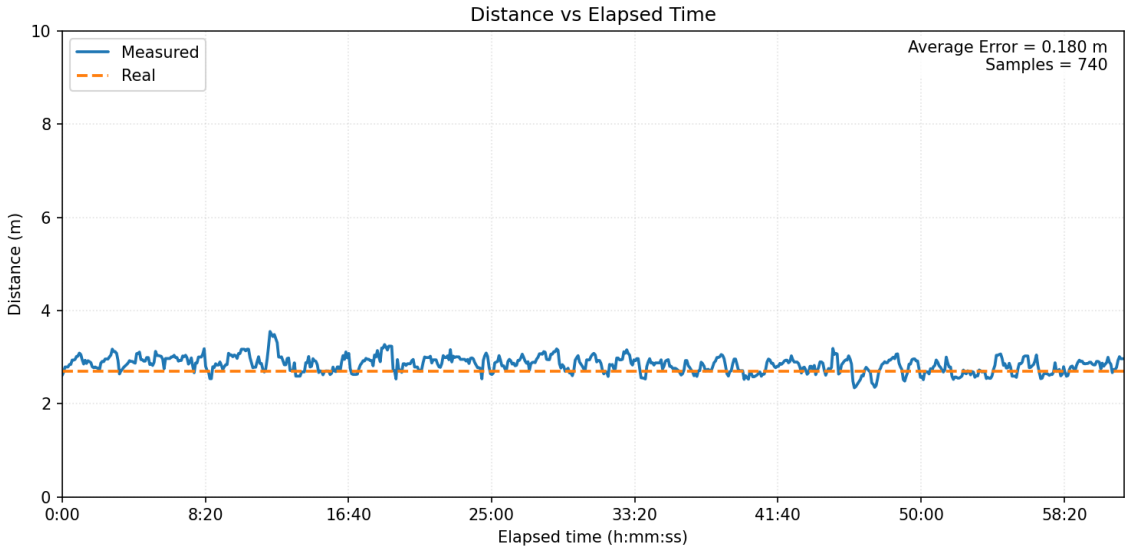

Figure 4.3: Measured vs. real distance for the 2.7 m one-initiator/one-reflector test case. The graph was generated using Python from logged UART-USB data.

4.4 Local Error Field Around a Fixed Target

For the third experiment we visualised the *local ranging error* around a fixed target, using the same logging pipeline (UART–USB) but a different visualisation approach. Three static anchors were deployed in an orthogonal layout on the walls to provide stable references during the session. The target position was fixed on top of a central table and used only as the plotting centre. Unlike the second experiment, here we do not show the full floor plan or anchor layout, instead, we focus on a compact $1\,\text{m} \times 1\,\text{m}$ window centred at the target to highlight centimetre-scale behaviour.

Initiator	**Distance to target (m)**
Initiator 1	4.0
Initiator 2	4.5
Initiator 3	3.0

Table 4.2: Distances between the fixed target and each initiator.

Figure 4.4: Experimental setup of the local error field measurement. Three initiators (black cubes) were mounted on the walls, forming an orthogonal reference geometry, while a single reflector (target) was placed on the table at the centre of the test area. This configuration provided stable ranging anchors for characterising local error growth around the target.

From the log we computed the per-anchor instantaneous errors

$$e_i(t) = \text{Position}_i(t) - \text{RealDist}_i \quad (i \in \{1, 2, 3\}),$$

and their per-anchor mean absolute values over the whole capture:

Anchor	**Average error (m)**
Average 1	0.142
Average 2	0.177
Average 3	0.193
Overall mean	**0.171**

Table 4.3: Per-anchor mean absolute error and overall mean.

Visualisation model: To provide an intuitive view of how error evolves around a stable reflector, we map the local error field as a heat map depicting the positions estimated by our implementation over the course of one hour. The average error of each initiator is also shown, giving insight into how the anchor geometry influences the ranging estimation error.

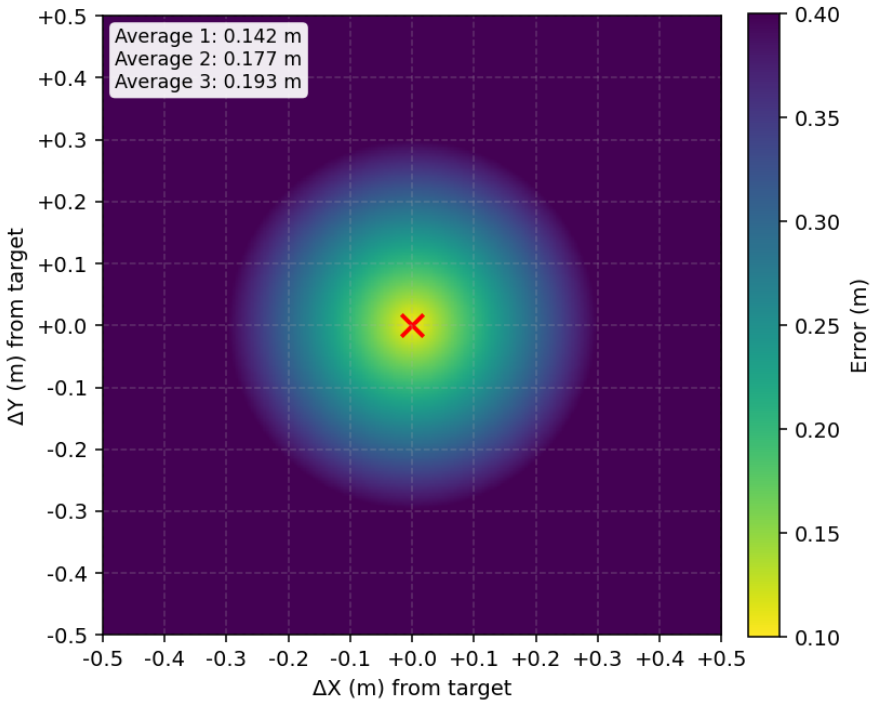

Figure 4.5: Local error heatmap in a 1×1 m window centred at the target (Reflector).

Results: Figure 4.5 illustrates that the local error distribution agrees with the expected accuracy levels, confirming sub-metre precision close to the target. These results provide a stable and interpretable basis for understanding how ranging data can be retrieved and analysed in the context of two-dimensional location estimation.

Chapter 5

Conclusions

This thesis demonstrated the feasibility and reliability of developing a **Bluetooth Low Energy (BLE) Channel Sounding** system for shortrange distance estimation and indoor localization. The complete system integrates both hardware and software components, including a custom **nRF54L15**-based PCB with environmental and inertial sensors, a communication layer for data exchange, and a software framework for acquisition, logging, and visualization of ranging data.

Through a progressive design and validation process, the implemented platform enabled accurate acquisition and processing of channelsounding metrics, supporting both **Inverse Fast Fourier Transform (IFFT)** and **Phase-Based Ranging (PBR)** estimators. The experimental evaluation confirmed that the system can achieve **submetre accuracy** under realistic indoor conditions, with the IFFT-based estimator consistently outperforming the PBR method in terms of stability and overall accuracy. The stepped-distance experiments, single-link ranging tests, and local error-field visualizations validated the robustness of the proposed approach in the presence of multipath and interference.

The communication between initiator and reflector was successfully implemented using the BLE Channel Sounding protocol, enabling reliable data exchange without requiring additional synchronization mechanisms. Data acquisition and visualization scripts were developed in **Python**, providing flexibility for offline processing and experimental analysis.

In summary, this work resulted in the development of a fully functional and modular **BLE ranging platform**, which can serve as a foundation for future research in the areas of **indoor localization**, **sensor fusion**, and **wireless distance estimation**. The

system offers scalability at both the hardware and software levels, enabling extensions toward multi-anchor localization, map generation, and realtime tracking in complex indoor environments.

Chapter 6

Future Work

The present thesis successfully completed the design and implementation of a portable BLE-based ranging and localization platform that supports both wireless communication and integrated environmental sensing. The developed system establishes a strong foundation for further research and development, which can be pursued along two main directions: (a) the enhancement of software and visualization capabilities toward real-time supervision, and (b) the optimization of hardware architecture for improved energy efficiency and scalability.

The first direction concerns the creation of a complete real-time acquisition and visualization framework, capable of providing a continuous overview of the operating area on a digital floor plan. Such a system would allow users to monitor in real time the position and status of multiple moving tags, display distance errors, and visualize estimated trajectories across the mapped environment. A dedicated software suite could be developed to handle live data acquisition, filtering, and plotting, enabling seamless integration between the ranging firmware and a desktop or web-based monitoring interface. In this context, the implementation of safety-related features could be particularly valuable for industrial environments. For instance, the accelerometer integrated into each mobile tag could be used for **fall detection** and sudden-motion alerts, while the floor-plan software could define **danger zones** or restricted areas, automatically generating notifications when a worker approaches or enters them. The combination of these features would transform the current ranging prototype into a complete real-time supervision platform for indoor safety and operational monitoring.

The second direction focuses on the optimization of power consumption and hardware efficiency, particularly for the mobile tags. One of the most straightforward improvements

would involve the removal or disabling of non-essential components, such as user LEDs or the UART-USB bridge, which consume power without contributing to normal operation. Parallel to these optimizations, a dedicated **anchor variant** could be designed, omitting the onboard sensors and USB interface, while integrating a higher-gain antenna or front-end amplifier to extend communication range and improve signal quality. Such an anchor would be optimized for fixed deployment, offering stronger connectivity and increased coverage for larger industrial spaces.

Overall, the proposed extensions would advance the current prototype from a proof-of-concept ranging system to a fully functional, scalable, and energy-efficient localization platform. The integration of real-time visualization, safety supervision, and optimized hardware would significantly expand the potential of the system, paving the way for applications in industrial monitoring, worker safety, and context-aware indoor tracking.

Bibliography

[1] A. A. M. Saleh and R. A. Valenzuela, "A statistical model for indoor multipath propagation," *IEEE Journal on Selected Areas in Communications*, vol. 5, no. 2, pp. 128–137, Feb. 1987.

[2] H. T. Friis, "A note on a simple transmission formula," *Proceedings of the IRE*, vol. 34, no. 5, pp. 254–256, May 1946.

[3] H. Hashemi, "The indoor radio propagation channel," *Proceedings of the IEEE*, vol. 81, no. 7, pp. 943–968, Jul. 1993.

[4] T. S. Rappaport, *Wireless Communications: Principles and Practice*, 2nd ed., Prentice Hall, 2002.

[5] A. F. Molisch, *Wireless Communications*, 2nd ed., Wiley, 2011.

[6] M. Z. Win and R. A. Scholtz, "Characterization of ultra-wide bandwidth wireless indoor channels: A communication-theoretic view," *IEEE Journal on Selected Areas in Communications*, vol. 20, no. 9, pp. 1613–1627, Dec. 2002.

[7] D. Dardari, A. Conti, U. Ferner, A. Giorgetti, and M. Z. Win, "Ranging with ultrawide bandwidth signals in multipath environments," *Proceedings of the IEEE*, vol. 97, no. 2, pp. 404–426, 2009.

[8] H. Wymeersch, J. Lien, and M. Z. Win, "Cooperative localization in wireless networks," *Proceedings of the IEEE*, vol. 97, no. 2, pp. 427–450, 2009.

[9] N. Patwari, J. N. Ash, S. Kyperountas, A. O. Hero, R. L. Moses, and N. S. Correal, "Locating the nodes: Cooperative localization in wireless sensor networks," *IEEE Signal Processing Magazine*, vol. 22, no. 4, pp. 54–69, Jul. 2005.

[10] E. Kaplan and C. Hegarty, *Understanding GPS: Principles and Applications*, 2nd ed., Artech House, 2005.

[11] R. Faragher and R. Harle, "Location fingerprinting with Bluetooth Low Energy beacons," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 11, pp. 2418–2428, Nov. 2015.

[12] F. Zafari, A. Gkelias, and K. K. Leung, "A survey of indoor localization systems and technologies," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2568–2599, 2019.

[13] V. Cantón Paterna, A. Calveras Augé, J. Paradells Aspas, and M. A. Pérez Bullones, "A Bluetooth Low Energy indoor positioning system with channel diversity, weighted trilateration and Kalman filtering," *Sensors*, vol. 17, no. 12, Art. 2927, 2017.

[14] M. Nikodem and M. Bawiec, "Experimental evaluation of advertisement-based Bluetooth Low Energy communication," *Sensors*, vol. 20, no. 1, Art. 107, 2020.

[15] G. Shan and B. Roh, "A slotted random request scheme for connectionless data transmission in Bluetooth Low Energy 5.0," *Journal of Network and Computer Applications*, vol. 207, Art. 103493, 2022.

[16] K. Xiao, F. Hao, W. Zhang, N. Li, and Y. Wang, "Research and implementation of indoor positioning algorithm based on Bluetooth 5.1 AoA and AoD," *Sensors*, vol. 24, no. 14, Art. 4579, 2024.

[17] M. Nikodem, G. Trajnowicz, G. S. de Blasio, and A. Quesada-Arencibia, "Experimental evaluation of multi-carrier phase difference localization in Bluetooth Low Energy," *IEEE Sensors Journal*, Nov. 2024.

[18] O. Dyhdalovych, A. Yaroshevych, O. Kapshii, I. Kravets, and O. Farenyuk, "Particle filter-based BLE and IMU fusion algorithm for indoor localization," *Telecommunication Systems*, vol. 88, Art. 9, 2025.

[19] E. Skýpalová, M. Boro, T. Loveek, and A. Veas, "Innovative indoor positioning: BLE beacons for healthcare tracking," *Electronics*, vol. 14, no. 10, Art. 2018, 2025.

[20] ISO/IEC 18305:2016, *Information technologyReal-time locating systemsTest and evaluation of localization and tracking systems*, International Organization for Standardization, 2016.

[21] Bluetooth Special Interest Group (SIG), *Bluetooth Core Specification Version 4.0*, Kirkland, WA, USA, 2010.

[22] Bluetooth SIG, "Bluetooth Core Specification v5.0: Feature overview," Kirkland, WA, USA, 2016. [Online]. Available: `https://www.bluetooth.com/wp-content/uploads/2019/03/Bluetooth_5-FINAL.pdf`

[23] Bluetooth SIG, "Bluetooth Core Specification v5.1: Feature Overview (Direction Finding)," Kirkland, WA, USA, 2019. [Online]. Available: `https://www.bluetooth.com/bluetooth-resources/bluetooth-core-5-1-feature-overview/`

[24] Bluetooth SIG, "Bluetooth Core Specification v5.2: Feature Overview (Isochronous Channels / LE Audio)," Kirkland, WA, USA, 2020. [Online]. Available:

https://www.bluetooth.com/wp-content/uploads/2020/01/Bluetooth_5.2_Feature_Overview.pdf

[25] Bluetooth SIG, "New Bluetooth Core v5.3 Feature Enhancements," Kirkland, WA, USA, 2021. [Online]. Available: https://www.bluetooth.com/bluetooth-resources/bluetooth-core-5-3-feature-enhancements/

[26] Bluetooth SIG, "Bluetooth Channel Sounding," Bluetooth feature enhancements page, 2024. [Online]. Available: https://www.bluetooth.com/learn-about-bluetooth/feature-enhancements/channel-sounding/

[27] Bluetooth SIG, *Specification of the Bluetooth System, Covered Core Package*, Version 5.4, Kirkland, WA, USA, 2023.

[28] Bluetooth SIG, "Bluetooth Core 5.4 Technical Overview (PAwR)," February 2023. [Online]. Available: https://www.bluetooth.com/bluetooth-resources/bluetooth-5-4-technical-overview/

[29] Bluetooth SIG, "Bluetooth Core Specification v6.0: Channel Sounding overview," Kirkland, WA, USA, 2024. [Online]. Available: https://www.bluetooth.com/learn-about-bluetooth/feature-enhancements/channel-sounding/

[30] Bluetooth SIG, "Bluetooth Direction Finding (AoA/AoD) overview," Kirkland, WA, USA, 2019. [Online]. Available: https://www.bluetooth.com/learn-about-bluetooth/feature-enhancements/direction-finding/

[31] Bluetooth SIG, "Bluetooth Direction Finding Technical Overview," [Online]. Available: https://www.bluetooth.com/wp-content/uploads/Files/developer/RDF_Technical_Overview.pdf

[32] ETSI TR 103 546, *Short Range Devices (SRD) in the UHF band; Technical characteristics and methods of measurement*, ETSI, 2020.

[33] ETSI EN 300 328, *Wideband transmission systems; Data transmission equipment operating in the 2.4 GHz ISM band and using wide band modulation techniques*, v2.2.2, 2019.

[34] Nokia, "Wibree: Ultra low power wireless technology," Nokia Press Release, Oct. 2006. [Online]. Available: https://www.wibree.com/wp-content/uploads/Wibree_pressrelease_final_1206.pdf

[35] Nordic Semiconductor, *nRF54L15 Preliminary Datasheet*, Nordic Semiconductor ASA, 2023.

[36] Nordic Semiconductor, "SAADCElectrical specifications, channels, gain, and functionality of the nRF54L15 SoC," *Product Specification, nRF54L15*, 2025. [Online]. Available: https://docs.nordicsemi.com/bundle/ps_nrf54L15/page/saadc.html Accessed: Sep. 13, 2025.

[37] Minewsemi, *ME54BS01 Module Datasheet (nRF54L15-based)*, 2024. [Online]. Available: https://en.minewsemi.com/bluetooth-module/nrf54l15-me54bs01#pro-detail

[38] Bosch Sensortec, *BME280 Combined Humidity and Pressure Sensor Datasheet*, Document No. BST-BME280-DS001, 2024. [Online]. Available: https://www.bosch-sensortec.com/media/boschsensortec/downloads/datasheets/bst-bme280-ds002.pdf

[39] STMicroelectronics, *LSM303AH Ultra-compact high-performance eCompass module (3D accel + 3D magnetometer) Datasheet*, Rev. 6, 2018. [Online]. Available: https://www.st.com/resource/en/datasheet/lsm303ah.pdf

[40] Microchip Technology Inc., *MCP73871 Li-Ion/Li-Polymer Charge Management Controller Datasheet*, DS20002090E, 2019. [Online]. Available: https://ww1.microchip.com/downloads/en/DeviceDoc/MCP73871-Data-Sheet-20002090E.pdf

[41] Texas Instruments, *TPS63031 High Efficiency Buck-Boost Converter Datasheet*, SLVS707, 2015. [Online]. Available: https://www.ti.com/product/TPS63031

[42] Microchip Technology Inc., *MCP2221A USB-to-UART Serial Converter, Datasheet*, Document No. 20005565E, 2023. [Online]. Available: https://ww1.microchip.com/downloads/aemDocuments/documents/APID/ProductDocuments/DataSheets/MCP2221A-Data-Sheet-20005565E.pdf

[43] Texas Instruments, *TPD4E05U06: 4-Channel ESD Protection for USB Datasheet*, Rev. C, 2020. [Online]. Available: https://www.ti.com/lit/ds/symlink/tpd4e05u06.pdf

[44] Amphenol ICC, *USB Type-C Receptacle Product Specification*, 2022. [Online]. Available: https://cdn.amphenol-cs.com/media/wysiwyg/files/documentation/usb_type_c_receptacle_product_specification_a.pdf

[45] The Zephyr Project, "Zephyr RTOS Documentation," Version 3.6.0, 2025. [Online]. Available: https://docs.zephyrproject.org/latest/

[46] Nordic Semiconductor, "nRF Connect SDK (NCS) Documentation," Version 2.6.0, 2025. [Online]. Available: https://developer.nordicsemi.com/nRF_Connect_SDK/doc/latest/nrf/

[47] SEGGER, "J-Link Debug ProbesUser Guide," Rev. J-Link V7.94a, 2024. [Online]. Available: https://www.segger.com/doc/UM08001_JLink.pdf

[48] Python Software Foundation, "pySerialPython Serial Port Access Library Documentation," Version 3.5, 2025. [Online]. Available: https://pyserial.readthedocs.io/en/latest/

[49] Nordic Semiconductor, "Bluetooth Low Energy Channel SoundingnRF54 Series," Nordic Semiconductor Infocenter Documentation, 2024. [Online]. Available: https://docs.nordicsemi.com/bundle/ncs-latest/page/nrf/protocols/bt/channel_sounding.html

[50] u-blox, "Introduction to Bluetooth Channel Sounding," u-blox White Paper, May 2025. [Online]. Available: https://www.u-blox.com/en/docs/UBX-23030002

[51] Analog Devices, "Understanding architecture of the Bluetooth Low Energy stack," Technical Article, 2021. [Online]. Available: https://www.analog.com/en/resources/technical-articles/understanding-architecture-bluetooth-low-energy-stack.html

[52] M. Afaneh, "Bluetooth LE ATT and GATT explained," NovelBits Blog, 2017. [Online]. Available: https://novelbits.io/bluetooth-le-att-gatt-explained-connection-oriented-communication/

[53] Punch Through, "How GAP and GATT work," Developer Blog, Nov. 2019. [Online]. Available: https://punchthrough.com/how-gap-and-gatt-work/

[54] M. Afaneh, "Periodic Advertising with Responses (PAwR): Bidirectional BLE advertising," NovelBits Blog, Dec. 2024. [Online]. Available: https://www.novelbits.io/periodic-advertising-with-responses-pawr/

[55] M. Afaneh, "Bluetooth Channel Sounding: Secure fine ranging using Bluetooth LE," NovelBits Blog, Dec. 2024. [Online]. Available: https://www.novelbits.io/bluetooth-channel-sounding/

[56] S. Gezici, Z. Tian, G. B. Giannakis, H. Kobayashi, A. F. Molisch, H. V. Poor, and Z. Sahinoglu, "Localization via ultra-wideband radios: A look at positioning aspects for future sensor networks," *IEEE Signal Processing Magazine*, vol. 22, no. 4, pp. 70–84, Jul. 2005.

[57] F. Gustafsson and F. Gunnarsson, "Mobile positioning using wireless networks: Possibilities and fundamental limitations," *IEEE Signal Processing Magazine*, vol. 22, no. 4, pp. 41–53, Jul. 2005.

[58] S. Gezici and H. V. Poor, "Position estimation via ultra-wideband signals," *Proceedings of the IEEE*, vol. 97, no. 2, pp. 386–403, 2009.

[59] J. Yang, C. Poellabauer, P. Mitra, and C. Neubecker, "Beyond beaconing: Emerging applications and challenges of BLE," *arXiv preprint* arXiv:1909.11737, 2019

[60] Bluetooth SIG, "Part A: Architecture, mixing, and conventions," Bluetooth Core Specification v5.4 site, 2023. [Online]. Available: https://www.bluetooth.com/wp-content/uploads/Files/Specification/HTML/Core-54/out/en/architecture,-mixing,-and-conventions/architecture.html .