ShadowTrace Positioning Alarm System

Technical Document

A mobile-target satellite positioning, cellular backhaul and near-field proximity alarm system built on a one-way visibility architecture

System Design · Hardware Composition · Communication Protocol · Alarm Mechanism · Deployment and Acceptance

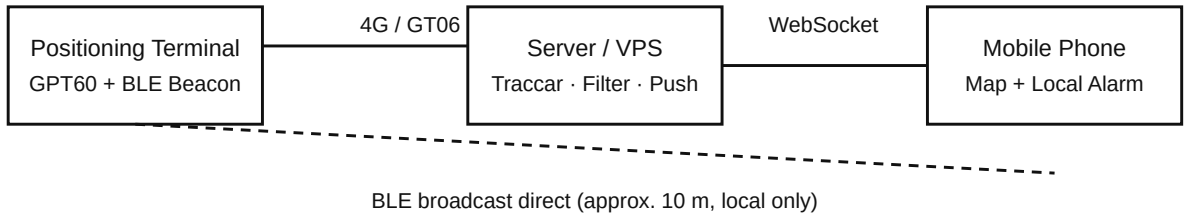


Figure 0-1 System composition line diagram: the positioning terminal and beacon are carried by the monitored target, positions are pushed one-way via the VPS to the phone, and the Bluetooth alarm is delivered locally.

Item	Content
System name	ShadowTrace Positioning Alarm System English full name: ShadowTrace Positioning Alarm System Abbreviation: STAS
Document version	V1.0 (design finalisation edition)
Document nature	System-level technical document for design review, development, deployment calibration and acceptance testing
Scope	Single-target positioning monitoring and short-range proximity alarm within a small enclosed or semi-enclosed area (typical scale 300-500 m)
Core composition	Portable 4G satellite positioning terminal · Low-power Bluetooth beacon · Positioning access and distribution server · Mobile receiving terminal

Device parameters are based on the reference models stated in the text. All alarm thresholds are reference values and must be calibrated in the field in accordance with Chapter 11 before delivery.

Copyright © 人机Cyborg

Contents and Reading Guide

1 System Overview and Design Principles	3
2 Overall System Architecture	4
3 Positioning Terminal Hardware	6
4 Satellite Positioning and Assisted Positioning Principles	9
5 Positioning Data Transmission Link and Protocol	10
6 Short-Range Alarm Subsystem	11
7 Receiving Terminal and Electronic Map	14
8 Server Software Structure and Processing Flow	17
9 Latency, Error and Performance Analysis	20
10 Security, Privacy and Compliance Design	21
11 Deployment, Calibration and Acceptance	21
12 Known Limitations and Evolution Roadmap	22
Appendix A Glossary · Appendix B Alarm Parameter Summary	22

Document Conventions

Monitored target: the mobile target wearing or carrying the positioning terminal and Bluetooth beacon. It is the only party in this system that is positioned and reported. **Guardian:** the party holding the receiving terminal, who only receives the monitored target's position and proximity alarms; the guardian's own position is not collected and not reported. **Platform:** the set of positioning access, parsing, storage and distribution software deployed on the server.

The following measurement conventions apply throughout: positions use the WGS-84 coordinate system (natively consistent with OpenStreetMap data, see Section 7.3); the reporting interval is the period at which the positioning terminal generates and sends a position packet, finalised at 5 s; all distances are horizontal distances; signal strength is in dBm, where a value closer to 0 means a stronger signal.

Abbreviations

Abbr.	Full form and explanation
GNSS	Global Navigation Satellite System, the generic term for GPS, BeiDou and other satellite positioning systems
LBS	Location Based Service via cellular base stations, used as a fallback when satellite positioning fails
A-GPS	Assisted GPS, which downloads ephemeris data over the cellular network to shorten time to first fix
BLE	Bluetooth Low Energy, used in this system for short-range proximity sensing
RSSI	Received Signal Strength Indicator, used to infer approximate distance from signal attenuation
GT06	A widely used binary communication protocol for vehicle and portable positioning terminals
OSM	OpenStreetMap, an openly licensed map data project

 Copyright © 人机Cyborg

1 System Overview and Design Principles

1.1 System Positioning

The ShadowTrace Positioning Alarm System (STAS) is a mobile-target monitoring and proximity sensing system for small-scale areas. The system continuously obtains the real-time position of one monitored target within an area and presents it one-way on the guardian's mobile terminal map. When the physical distance between the monitored target and the guardian enters a preset short-range interval, the system triggers a graded alarm locally on the guardian's terminal.

The typical working scale is an enclosed or semi-enclosed area 300-500 m on a side, such as a campus, courtyard or building complex. At this scale, the inherent error of satellite positioning (5-10 m) is of the same order of magnitude as the target spacing. This is the fundamental reason this system adopts a dual-layer architecture, detailed in Chapter 6.

5 s	**~6 s**	**10 m**	**0**
Position reporting interval (finalised)	End-to-end presentation latency budget	Short-range alarm distance (BLE decision)	Guardian position data collected

1.2 Three Design Principles

Principle 1: One-way visibility. Position data flows in only one direction in the system: from the monitored target to the guardian. The guardian terminal has no position reporting channel at the protocol level, and the server has no storage structure for the guardian's position. This principle is a data absence at the architecture level, not a permission setting at the interface level: no link anywhere contains data that could be used to track the guardian in reverse.

Principle 2: Division between coarse positioning and precise alarm. Satellite positioning answers "roughly where is the target", for map presentation. The short-range alarm answers "is the target already close enough", decided locally on the receiving terminal by a Bluetooth beacon carried at the same location, without passing through the server and without relying on satellite accuracy. The two links are independent of each other; failure of either does not affect the other function.

Principle 3: Minimised collection and mature components first. The system collects only data required for its function: position, speed, battery level and positioning method identifier. On the platform side, mature open-source components are preferred (see Chapter 8), and self-developed code is concentrated in filtering, push and alarm functions.

1.3 Functional and Non-functional Indicators

Category	Indicator
Positioning	Outdoor open-sky accuracy 5-10 m (GNSS); reporting interval 5 s; time to first fix from a few seconds to 30 s with A-GPS assistance
Presentation	End-to-end latency budget approx. 6 s; continuous track with no abnormal jumps
Alarm	Short-range (approx. 10 m) alarm triggered locally on the receiving terminal, trigger latency under 1 s; with debounce and hysteresis reset mechanisms
Availability	Terminal caches locally during network outage and backfills on recovery; receiving-end map supports offline tiles

2 Overall System Architecture

2.1 Layered Architecture

The system is divided by responsibility into four layers: sensing, transport, platform and application. The sensing layer performs positioning and near-field broadcasting; the transport layer performs cellular backhaul and Internet distribution; the platform layer performs protocol parsing, data filtering, storage and push; the application layer performs map presentation and local alarm. The layers are connected by explicit data interfaces, so replacing the implementation of any layer does not affect the others.

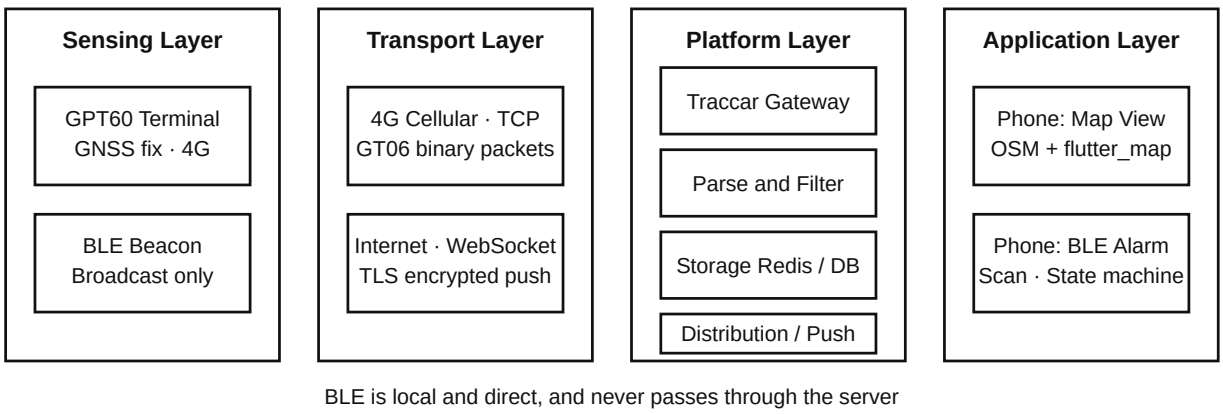


Figure 2-1 Layered architecture. Solid lines are the main position data link; the Bluetooth near-field link never passes through the server at any point.

2.2 Data Flow and One-way Property

The complete path of position data is: positioning terminal → (4G / TCP) → platform access gateway → parsing and filtering → real-time distribution → (WebSocket) → receiving terminal map. The receiving terminal sends only subscription and connection keep-alive packets to the platform, and sends no position field of any kind; the platform database contains only one position table, for the monitored target. The Bluetooth beacon's broadcast is received directly by the receiving terminal only within a physical range of about 10 m, and enters no part of the chain above.

> **Design point:** One-way property is guaranteed jointly by three places - the terminal firmware does not implement guardian position collection, the communication protocol defines no guardian position field, and the server provides no write interface for a guardian position. Merely hiding an entry point in the application interface does not constitute one-way property.

2 Overall System Architecture (continued)

2.3 Physical Deployment Topology

System deployment involves four kinds of physical entity: the positioning terminal and Bluetooth beacon are carried by the monitored target; the platform is deployed on a cloud server with a public address (a virtual private server); the receiving terminal is a smartphone held by the guardian. In a small-scale area scenario, the number of monitored targets is one to several, so a single-machine platform deployment satisfies the load with no cluster required.

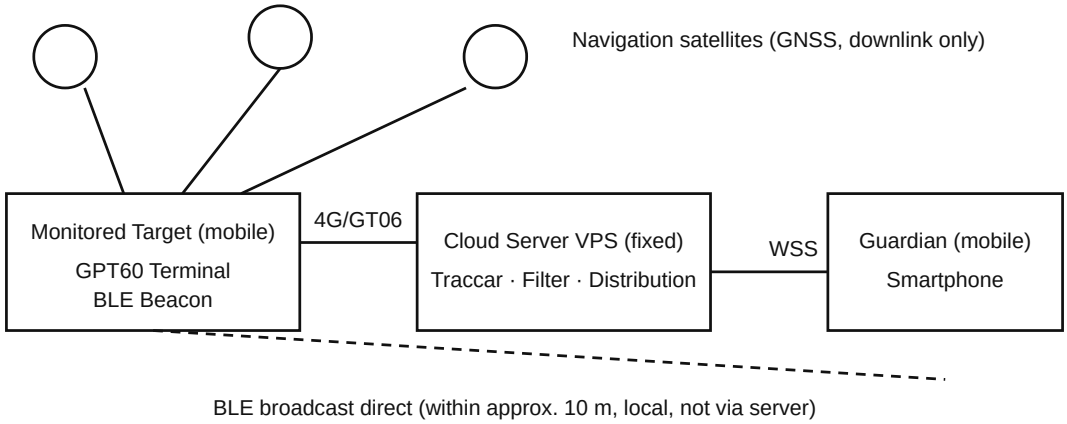


Figure 2-2 Physical deployment topology. Position data reaches the receiving terminal in two hops, over the cellular network and the Internet; near-field sensing is delivered locally by Bluetooth broadcast. Satellite signals travel one-way down from the sky to the positioning terminal and form no data return channel; the guardian's position enters no link.

2.4 Working Sequence Overview

1. **Power-on registration:** after power-on the positioning terminal connects to the platform and sends a login packet containing the device identifier (IMEI); the platform checks the whitelist and establishes a session.
2. **Positioning and reporting:** after a satellite fix, the terminal sends one position packet every 5 s, and a heartbeat every 30 s to maintain the session.
3. **Parsing and distribution:** the platform parses the packet, filters abnormal points, writes to storage, and immediately pushes via WebSocket to subscribed receiving terminals.
4. **Presentation and sensing:** the receiving terminal updates the map marker; at the same time it continuously scans Bluetooth broadcasts, and triggers an alarm locally when signal strength crosses the calibrated threshold.
5. **Offline decision:** if the platform receives no heartbeat from a terminal for over 90 s, it marks it offline; the receiving end greys out the corresponding marker and annotates the last position time.

3 Positioning Terminal Hardware

3.1 Reference Model and Selection Basis

The positioning terminal is a portable 4G positioning device designed to be carried by a person, with the Eelink GPT60 class of product as the reference model. The selection rests on three grounds. First, the overall size and weight allow all-day carrying without a noticeable foreign-body feel. Second, the communication standard is 4G LTE Cat.1 with support for a custom server address, so it can connect to a self-built platform rather than a vendor's closed cloud. Third, the protocol ecosystem is mature: common protocols such as GT06 can be parsed directly by open-source platforms. Vehicle terminals (such as the TK905 class) are about three to four times its size and weight, and some models depend on vehicle power, so they are not suitable for carrying by a person and are not adopted.

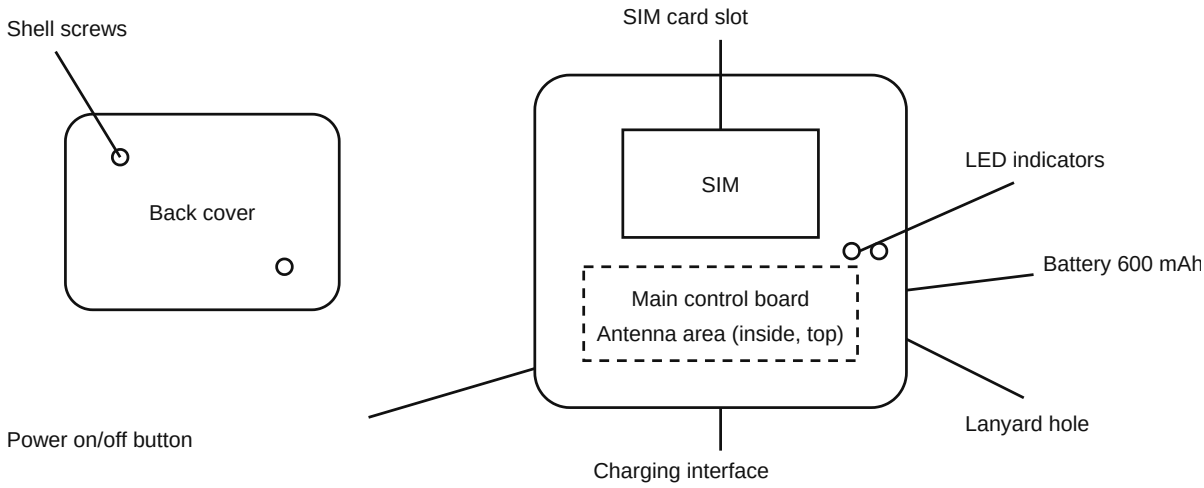


Figure 3-1 Exploded black-line diagram of the GPT60 positioning terminal (back side, back cover open). The leader lines point to the actual parts: back cover, shell screws, SIM card slot, LED indicators, power on/off button, lanyard hole and charging interface, together with the internal main control board, antenna area and lithium battery. Each item is explained in Section 3.2.

How to read the diagram: Figure 3-1 is drawn from the back of the actual device, with the back cover opened to the upper left. Read in this order: first the back cover and shell screws (how it opens), then the SIM card slot and battery (how the card is fitted and how it is powered), and finally the LEDs, power button and lanyard hole (how to judge status, switch it on and off, and fix it in place). What each part is and what it does is explained item by item in Section 3.2 on the next page.

3 Positioning Terminal Hardware (continued)

3.2 Part-by-part Introduction (against Figure 3-1)

Part	What it is	What it does
Back cover and housing	The removable cover on the back of the body, joined to the front shell by clips and screws to form the housing	Protects the internal circuits. The card can only be changed and the battery inspected after opening the cover. Keep it closed in daily use; a poorly closed cover affects dust and water resistance and carrying security.
Shell screws	Small screws fixing the back cover to the body, at the corners of the cover and body (two leader lines in Figure 3-1 point to the cover screw holes and the body screws)	Lock the back cover to the body so walking vibration cannot loosen it and cause poor battery or SIM contact. Use the matching small screwdriver; if a screw is lost the cover relies on clips alone, which is unreliable.
SIM card slot	A card socket on the back of the body, taking a Nano-SIM IoT card, with a hinged metal cover that locks	Only with an IoT card fitted can the terminal join the 4G network and return positions. With no card, no data, or poor contact, the terminal positions but does not report, which appears on the platform as the device being offline.
Antenna area	The area on the upper inside of the body where the GNSS and 4G antennas are placed (dashed box, on the main board)	The GNSS antenna receives satellite signals and the 4G antenna sends and receives cellular signals. When worn, this side should face outward and upward, and must not be fully covered by metal objects or the body, otherwise positioning becomes slower and less accurate.
Main control board	The circuit main board of the device (the dashed area in Figure 3-1), integrating the main MCU, GNSS module and 4G module	The main controller schedules everything: it reads the coordinates computed by GNSS, assembles a GT06 packet every 5 s, and sends it via the 4G module. The GNSS module only measures position and the 4G module only returns data and assists positioning; see Chapter 4 for the division.
Lithium battery	A rechargeable lithium battery below the main board, reference capacity 600 mAh	The only power source. Battery life at a 5 s reporting interval is about 5-8 h (see Section 9.2), so charge it fully before use. The battery percentage is reported with each position packet, so the guardian can judge the remaining endurance.
LED indicators	Two small indicators on the back of the body, corresponding to positioning and network status respectively (per the manufacturer's instructions)	Allow on-site judgement of whether the terminal is normal without a phone: the flashing pattern indicates searching for satellites, fixed, or no network. Before placing the terminal in the carried item, check the lights to confirm a fix and a network connection.
Power on/off button	A physical key on the left side of the body	Long-press to switch on or off. After switch-on the terminal automatically searches for satellites, joins the network and logs in to the platform, with no other operation needed. Accidental switch-off stops reporting, and the platform judges it offline after 90 s.
Lanyard hole	A small hole at the lower corner of the body for threading a cord	With a lanyard threaded, the terminal can be worn around the neck or fixed to a bag or clothing, preventing it from slipping and being lost during activity. When fixing it, take care that the cord or clothing does not cover the antenna area.
Charging interface	Charging contacts / interface on the bottom edge of the body	Connects a charging cable or dock to charge the lithium battery. During charging the LED stays on or changes colour to indicate status (per the manufacturer's instructions); start a complete monitoring task only after a full charge.

3.3 Main Parameters and Procurement Checks

Parameter	Reference model value	Significance for this system
Size / weight	Approx. 60 x 45 x 19 mm / approx. 40 g	Can be placed in a pocket or worn, without affecting normal activity
Battery	600 mAh lithium battery	Supports one working period at a 5 s reporting interval; must be fully charged before use
Cellular standard	4G LTE Cat.1, Nano-SIM	Balances coverage and power consumption; an IoT card is sufficient
Positioning method	GNSS (GPS + BeiDou) + LBS fallback	Outdoor accuracy 5-15 m; degrades automatically indoors (see Section 4.4)
Server configuration	Supports changing the server IP and port by SMS / application	A precondition for connecting to a self-built platform; must be confirmed at purchase

> **Procurement checklist:** before ordering, confirm with the supplier item by item - (1) it is the 4G version, not the 2G version; (2) it supports a custom server address and port; (3) it supports domestic 4G bands and Nano-SIM. If any one of the three is missing, the terminal cannot connect to this system's platform.

3.4 Form and Wearing Method

The terminal measures about 60 x 45 x 19 mm and weighs about 40 g. It can be placed in a pocket, worn around the neck, or fixed to a carried item such as a bag, without affecting normal activity. When fixing it, the antenna area on the upper part of the body should face outward and upward, and must not be fully covered by metal objects or the body; threading the lanyard hole prevents slipping (see Figure 3-1). Its fixed position should be as close as possible to the beacon's: carrying the two at the same location is the precondition for the near-field alarm to hold (see Section 6.3). Before starting a monitoring task, confirm in order: the back cover is closed and the screws are tightened, the IoT card is fitted, the battery is fully charged, and the LEDs show a fix and a network connection.

 Copyright © 人机Cyborg

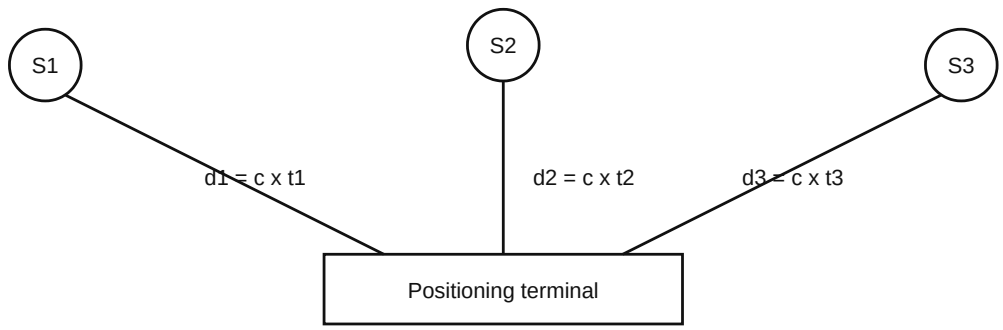
4 Satellite Positioning and Assisted Positioning Principles

4.1 Division: Measuring Position and Returning Data Are Two Different Things

It is commonly misunderstood that "4G positioning" means the 4G network performs the positioning. In the ShadowTrace Positioning Alarm System (STAS), the three radio systems have a clear division: GNSS is responsible for computing the position - it only receives the weak downlink signals from satellites and sends no data outward; the 4G cellular network is responsible for delivering the computed position to the server, and also undertakes assisted positioning and fallback positioning; Bluetooth is responsible for near-field sensing at the 10 m level. None of the three can replace another.

4.2 GNSS Positioning Principle

The positioning terminal simultaneously receives signals broadcast by multiple navigation satellites, and each satellite states its own position and transmission time in the signal. The terminal multiplies the speed of light by the signal propagation delay to obtain its distance from each satellite (the pseudorange), and solving four or more distance equations together yields the terminal's three-dimensional coordinates and clock bias. The more satellites participate and the more dispersed their geometry, the more stable the result. Building obstruction and reflection (the multipath effect) are the main sources of error in urban and campus environments.



Three spheres intersect at a point (an actual solution needs 4+ satellites to also correct the terminal clock bias)

Figure 4-1 Schematic of GNSS pseudorange positioning. Distance comes from signal propagation delay, not from signal strength.

4.3 A-GPS Assistance and Cold Start

When the terminal is switched on with no prior information at all (a cold start), it must first demodulate the ephemeris from the satellite signal itself, and the time to first fix can exceed 30 s. A-GPS downloads the ephemeris and an approximate position in advance over the 4G network, so the terminal skips the demodulation step and can complete its first fix within seconds. This system's terminal relies on this mechanism to shorten readiness time at the power-on and entry stage.

4.4 LBS Fallback and Degradation Rules

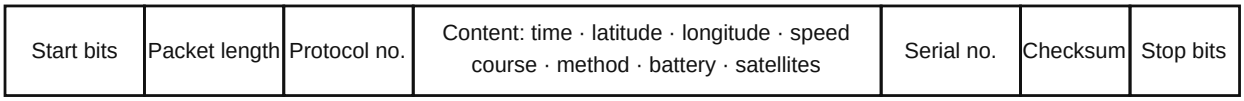
When the terminal enters a building interior, an underground space or a gap between tall buildings, the satellite signal attenuates to unusable levels and the terminal automatically switches to LBS: it estimates position from the connected base station and neighbouring cell signals, and the error rises sharply to 100-500 m. The platform marks LBS-sourced points separately and does not use them for any distance decision (see the filtering rules in Section 8.4). When the map end receives an LBS point or no new point for a long time, it should present a "weak signal / last known position" state rather than connecting the jumping point directly, so as not to mislead the guardian.

5 Positioning Data Transmission Link and Protocol

5.1 Link Composition

The backhaul link uses "TCP long connection + binary protocol" rather than HTTP polling: the terminal and the platform gateway establish one long-lived TCP connection, position packets are sent directly as binary frames, and both connection overhead and packet size are minimal, suiting a high-frequency small-packet scenario of once every 5 s. The platform-to-receiving-terminal segment uses a WebSocket long connection, so the server actively delivers each new position, avoiding the latency and battery cost of client polling.

5.2 GT06 Frame Structure



Protocol number distinguishes packet types: login / position / heartbeat / alarm; receiver must handle sticky and half packets. Start / stop bits and checksum are framing and error-checking fields; the content area is the payload (schematic).

Figure 5-1 Black-line sketch of a GT06-class protocol position packet frame structure (schematic, not a byte-by-byte specification; implementation follows the protocol manual).

5.3 Session Life Cycle

Stage	Behaviour
Login	The terminal sends a login packet containing the IMEI; the gateway checks the whitelist, and on a match replies and registers the session "device identifier → connection".
Position reporting	One position packet every 5 s; after parsing, the gateway passes it to the filtering module, and a qualified point immediately enters the distribution channel.
Heartbeat	One heartbeat packet every 30 s; no heartbeat for over 90 s is judged offline, and the receiving end greys out the marker.
Offline caching	With no cellular signal, the terminal caches position frames locally and backfills them in timestamp order on recovery; backfilled points are only stored and drawn as a track, and do not trigger real-time presentation jumps.
Reconnection	After a connection interruption the terminal automatically redials and logs in again; the gateway registers idempotently by device identifier to avoid duplicate sessions.

5.4 Platform-side Push Format

The platform pushes structured JSON to the receiving terminal, one message per position point. The receiving terminal updates the map marker from this message alone, with no second coordinate conversion (see Section 7.3).

```
{"deviceId":"stas-001","lat":38.04231,"lng":114.51482,
 "time":1731480000,"speed":1.4,"course":86,
 "source":"GNSS","battery":78}
```

Field notes: *source* identifies the positioning source (GNSS / LBS), and LBS points must be presented distinctly in the interface; *battery* is the terminal's remaining battery percentage, for the guardian to judge the remaining endurance.

6 Short-Range Alarm Subsystem

6.1 Why Satellite Positioning Is Not Used to Judge Short Range

Within a small-scale area, the GNSS error of 5-10 m is of the same order as the 10 m alarm distance: judging proximity by the satellite-position distance between two points produces both missed alarms (the target is actually close but the measured distance is too large) and false alarms (position drift makes the measured distance momentarily smaller). STAS therefore decouples the short-range decision completely from satellite positioning and assigns it to a Bluetooth signal that is physically effective only at short range: the signal itself cannot reach far away, and that physical constraint is the most reliable basis for the decision.

6.2 BLE Beacon and RSSI Ranging Principle

The BLE beacon, carried at the same location as the positioning terminal, broadcasts packets containing a fixed identifier at a fixed interval (typically 350-1000 ms), without establishing a connection. The receiving terminal scans periodically in the background and measures the RSSI of each broadcast packet. In free space, RSSI attenuates logarithmically with distance - the closer the distance, the smaller the attenuation - so an approximate distance can be inferred from an RSSI threshold. Body obstruction, walls and wearing orientation cause the RSSI at the same distance to fluctuate by about +/-6-10 dB, so a threshold can only give a judgement of "entered the approx. 10 m interval" and cannot give a precise distance reading.

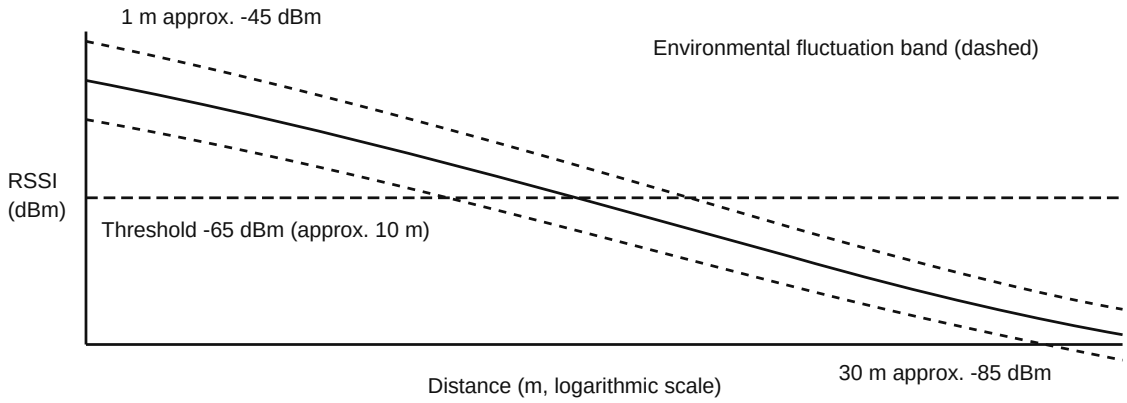


Figure 6-1 Schematic of the RSSI-distance attenuation relationship. The middle curve is the typical value and the upper and lower dashed lines are the environmental fluctuation band; the intersection of the threshold line and the curve is the alarm distance.

6.3 Beacon Selection

The beacon is a button-type BLE broadcaster: about 30 mm in diameter, powered by a coin cell, with a battery life on the order of months, and configurable transmit power and broadcast interval. It is independent of the positioning terminal in function and power supply, so even if the positioning terminal's battery is exhausted, the near-field alarm can still work within the beacon's endurance - this is the availability benefit of the separated dual-device design.

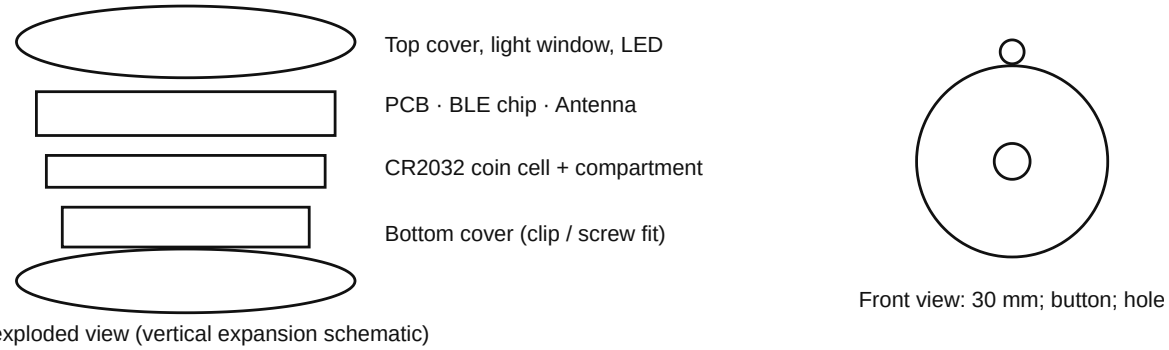


Figure 6-2 Exploded black-line diagram (left) and front view (right) of the BLE Bluetooth beacon. The beacon only broadcasts and does not connect to a network. What each part is and what it does is introduced item by item below.

Beacon Parts, Item by Item

Top cover and light window: the upper half of the beacon housing, with a small translucent area at the top. It protects the internal circuits and lets the LED light through. The housing is mostly plastic, with no external antenna.

LED indicator: a small indicator under the top cover. It flashes to indicate broadcasting, pairing or low battery, and can normally be dimmed or switched off to save power - it is only a status indication and takes no part in ranging.

PCB main board and BLE chip: the beacon's circuit board, whose core is one low-power Bluetooth chip. At a fixed interval (typically 350-1000 ms) it sends out a broadcast packet containing a fixed identifier, without establishing a connection with any device.

Antenna: a board-mounted antenna at the edge of the main board, which radiates the broadcast signal. Metal objects pressed against the beacon noticeably reduce the signal, so the beacon should be exposed when fixed.

Coin cell and battery compartment: one CR2032 coin cell pressed into the compartment supplies power. Because broadcast power consumption is extremely low, one cell can work for months. When the battery is low the broadcast weakens and the effective distance shortens, so check it before a whole session.

Bottom cover and hanging hole: the lower half of the housing, press-fitted to the top cover by clips or a screw thread, and opened here to change the battery. A small ear extending from the bottom cover carries a hanging hole, so it can be fixed to a carried item with a cord, a pin or adhesive, and carried together with the positioning terminal.

Button: a small button on the front, used for power on/off, broadcast mode switching, or factory reset. At deployment, press it to confirm broadcasting has started, then fix the beacon in place and do not operate it again.

6 Short-Range Alarm Subsystem (continued)

6.4 Alarm State Machine and Debounce Design

A single RSSI sample crossing the threshold does not raise an alarm directly. The receiving terminal first applies a moving average to the scan results, then decides through a three-state state machine: only when several consecutive samples stably cross the threshold does it enter the alarm state; after entering the alarm state, the RSSI must fall continuously below the reset line before it exits. The hysteresis interval between the trigger line and the reset line eliminates repeated triggering when the target hovers at the edge of the alarm distance.

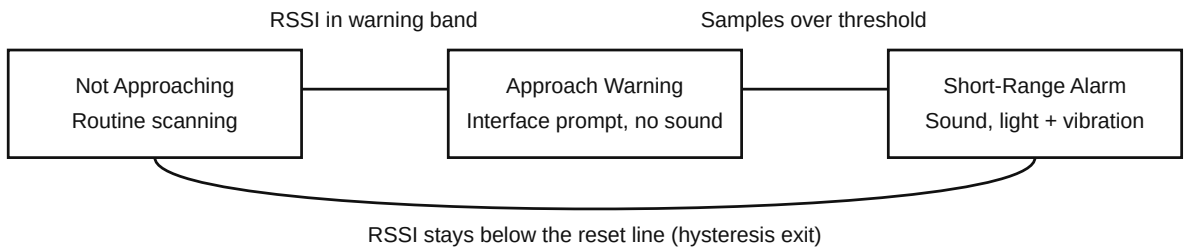


Figure 6-3 Short-range alarm state machine. All decisions are completed locally on the receiving terminal and do not depend on the server or network connectivity.

Parameter	Reference value	Explanation
Warning band	From approx. -75 dBm	Corresponds to approx. 15-25 m; interface weak prompt only
Alarm threshold	Approx. -65 dBm	Corresponds to approx. 10 m; the field calibration result prevails (Chapter 11)
Trigger confirmation	3 consecutive samples meeting the standard	Suppresses false alarms caused by single-point spikes
Reset condition	8 dB below threshold, sustained 5 s	Hysteresis exit, preventing repeated alarms from edge jitter
Alarm latency	Under 1 s (local decision)	Complements the approx. 6 s presentation latency of the map link

> **Permission note:** mainstream mobile operating systems require an application to hold location permission before it can perform Bluetooth scanning; this is a system-level interface constraint. The STAS receiving terminal holds that permission only to enable the scanning function, and does not use it to collect the guardian's position (see Option 1 in Section 7.4). The purpose of the permission should be stated to the user inside the application.

7 Receiving Terminal and Electronic Map

7.1 Terminal Form and Technology Stack

The receiving terminal is a cross-platform application running on a smartphone, built for both Android and iOS from a single Flutter code base. The application consists of three parts: the map view (presenting the monitored target's position), the push client (maintaining the WebSocket subscription), and the alarm module (Bluetooth scanning and the state machine). The three are independent of each other: failure of map tile loading does not affect the alarm, and a push interruption does not affect browsing of the already cached map.

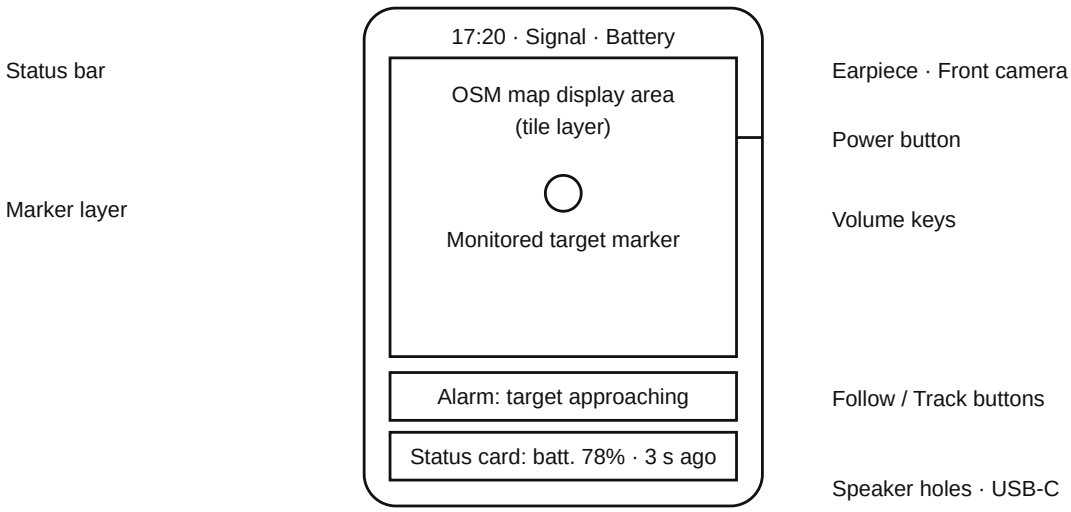


Figure 7-1 Front black-line diagram of the receiving terminal (smartphone). Inside the screen are the application interface zones (status bar, map area, marker, alarm banner, status card); on the sides and lower edge are the physical keys and interfaces. Internal modules are not visible in the diagram; see the item-by-item introduction in Section 7.1 below.

Phone Parts and Interface Zones, Item by Item

Earpiece, front camera: the earpiece is one sound channel for the alarm tone; the front camera is unrelated to this system and the application does not invoke it. **Status bar:** the top line of the screen, showing time, cellular signal and phone battery; it belongs to the phone system, not the application data - judge position freshness by "updated x seconds ago" in the status card, not by the status bar time. **Map display area:** the main body of the screen, rendering the OSM tile base map (tile layer); pre-cached tiles are shown offline. **Monitored target marker:** the only position marker on the map (marker layer), which moves smoothly to the new coordinates on each WebSocket push; after more than 15 s with no new point it is greyed out and annotated with the last position time. **Alarm banner:** a prompt bar in the lower-middle of the screen, normally hidden; when the BLE state machine enters the alarm state it pops up and simultaneously triggers a tone and vibration. It is triggered by local scanning and does not depend on whether map data has arrived. **Device status card:** the information card below the banner, showing the positioning terminal's remaining battery, positioning source (GNSS / LBS) and data update time - the basis on which the guardian judges "can this position be trusted, and how long can the terminal last". **Follow / Track buttons:** the bottom operation area. "Follow" keeps the map centre on the marker automatically, and "Track" reviews the historical route; a manual drag of the map exits Follow automatically, so view and operation do not fight each other. **Power key, volume keys:** physical keys on the side of the body. After the power key locks the screen, the application must be kept alive by a foreground service / background Bluetooth mode (see Section 7.5); the volume keys determine the alarm tone volume, and at deployment it should be confirmed that the volume is not muted. **Speaker holes, USB-C interface:** the speaker holes on the lower edge are the outlet for the alarm sound and must not be blocked by a phone case; the USB-C port is for charging and data connection and is unrelated to the positioning link. **Internal modules (not visible in the diagram):** the BLE module scans beacon broadcasts in the background and measures RSSI, and is the hardware precondition for the 10 m alarm; the cellular / Wi-Fi module maintains the WebSocket long connection to the VPS.

7 Receiving Terminal and Electronic Map (continued)

7.2 Map Presentation Rules

- **Initial view:** on opening, the application positions to the centre of the preset area (calibrated at deployment), at zoom level 17-18, so that one screen covers the whole monitored area.
- **Follow mode:** the map centre moves with the monitored target marker; after the user drags manually it switches automatically to free viewing, avoiding a fight between view and operation.
- **Smooth movement:** between two adjacent points (5 s apart), movement is presented with about 1 s of linear interpolation. Note that interpolation only improves the appearance and does not reduce the real latency, so the interface should display the data time at the same time.
- **Failure presentation:** after more than 15 s with no new point, the marker is greyed out and annotated "last position · xx seconds ago"; LBS-sourced points are presented in a distinct style with an accuracy prompt.

7 Receiving Terminal and Electronic Map (continued)

7.3 Map Data Source Selection: A Registration-free Open Solution

STAS uses OpenStreetMap (OSM) data and the Flutter map component flutter_map as its map base. The selection rests on three grounds. First, OSM requires no developer registration, real-name authentication or key application, so the deployment threshold is zero - particularly suitable for scenarios where a guardian assisting a minor user faces obstacles in completing real-name registration. Second, OSM data natively uses the WGS-84 coordinate system, consistent with the positioning terminal's output, so the whole link avoids coordinate system conversion, a common source of error. Third, tiles can be pre-cached to the terminal locally, which suits the reality of uneven cellular signal within an area.

Comparison item	OSM + flutter_map (this system)	Commercial map SDK (alternative)
Registration and key	No registration, no key required	Key must be applied for after developer real-name authentication
Coordinate system	WGS-84, consistent with the terminal's raw coordinates	Domestic services are mostly GCJ-02, requiring conversion across the whole link
Offline use	Area tiles pre-cached, a few MB in size	Offline package capability varies by vendor
Detail and rate limits	Building and road outlines satisfy small-area use; the public tile service has call rate limits, and large-scale use requires a self-built tile service	Richer place information, stable within quota

If a commercial map is needed later, only the application-layer map component and the coordinate conversion step need replacing; the sensing, transport and platform layers are unaffected - this is the direct benefit of the layered architecture for map selection.

7.4 Receiving-end Positioning Strategy: Option 1 (No Positioning)

The receiving terminal adopts "Option 1": the application does not request its own positioning result for business logic, does not draw the guardian's position on the map, and the server has no guardian position field. Its basis is the one-way visibility principle of Section 1.2: the guardian judges the relative relationship between themselves and the monitored target by relying on the monitored target's absolute position on the map and the surrounding building and road references, with no need for the system to know the guardian's coordinates.

As an optional extension, "Option 2" allows the application to draw a guardian position marker locally for intuitive comparison, but that coordinate only participates in local rendering and is prohibited from entering any network packet. The two options share the same code path and differ only by a local switch; the default delivery configuration is Option 1.

7.5 Offline Operation and Keep-alive

Offline map: at the deployment stage, tiles for the monitored area at levels 15-18 are pre-downloaded and cached in a networked environment; at area scale the data volume is about a few MB. With no network the base map still displays normally, and position points continue to be pushed after the connection recovers.

Background keep-alive: on Android a system foreground service maintains the WebSocket and Bluetooth scanning, and on iOS the system background Bluetooth mode is used; in both cases the user must be guided to add the application to the battery optimisation whitelist, otherwise scanning and push will be reclaimed by the system after the screen locks.

8 Server Software Structure and Processing Flow

8.1 Component Division

The platform is deployed on one cloud server. The open-source positioning platform Traccar runs in a container and undertakes protocol access and device management, while self-developed services undertake filtering, distribution and business interfaces. Traccar has built-in parsing and track storage for mainstream protocols such as GT06 and JT808, and adopting it directly avoids the compatibility risk of self-developed binary parsing; the self-developed code does not touch the raw byte stream, and its starting point is the standard position object after parsing.

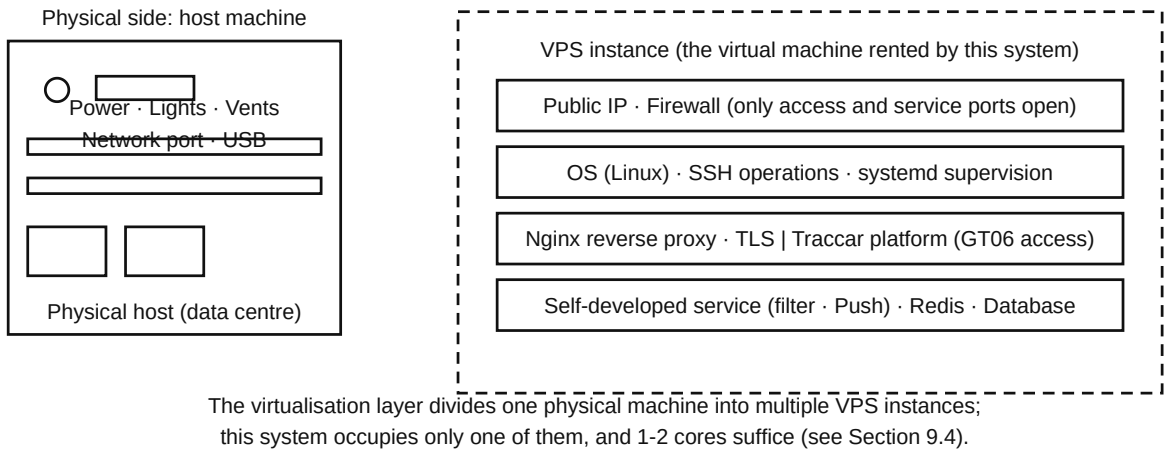


Figure 8-1 Black-line diagram of the server / VPS composition. On the left is the front of the physical host (power button, status lights, vents, network port, USB port); on the right are the software layers inside the VPS instance. What each component is and what it does is introduced item by item in Section 8.2.

8 Server Software Structure (continued)

8.2 Server Composition, Item by Item (against Figure 8-1)

Component	What it is	What it does
Physical host	A real server in the cloud provider's data centre, with power button, status lights, vents, network port and USB port on its front panel (left of Figure 8-1)	Provides the real CPU, memory and network. It is operated by the cloud provider; the user never touches the physical machine and only uses, over the network, the VPS instances divided from it.
Virtualisation layer	The software layer on the host that divides the hardware into multiple virtual machines	Divides one physical machine into several mutually non-interfering VPS instances. This system rents only one of them, invisible to other tenants on the same host.
VPS instance	The virtual server rented by this system, with its own public IP, operating system and disk (dashed box on the right of Figure 8-1)	The actual running place of the platform. In a single-target scenario 1-2 cores suffice; when the VPS is down the position link is interrupted, but the BLE local alarm is unaffected.
Public IP and firewall	The VPS's external network address and port filtering rules (top bar of Figure 8-1)	Terminals and phones find the platform through it; only the GT06 access, WebSocket and SSH ports are allowed, and all others are closed.
Operating system and operations	The Linux system inside the VPS, SSH remote login and systemd service supervision	Hosts all software processes; systemd automatically restarts a service that exits abnormally. Operations are performed only via SSH, with no graphical desktop exposed.
Nginx reverse proxy	The Web entry point and TLS termination layer at the very front of the services	Provides the encrypted WebSocket (WSS) and management pages externally, and forwards external requests to internal services, avoiding direct exposure of internal ports to the public network.
Traccar positioning platform	Open-source positioning platform software, running in a container	Undertakes GT06 access and parsing: checks the IMEI whitelist, decodes binary packets into standard position objects, and maintains device online status.
Self-developed service	The filtering and distribution program written for this system	Applies the filtering rules of Section 8.4 to position objects, and immediately pushes qualified points via WebSocket to subscribed phones. It does not touch the raw byte stream; its starting point is the object after Traccar parsing.
Redis and database	An in-memory key-value cache and a relational track database	Redis stores each device's latest position for fast reading; the database stores historical tracks by device and time for replay and acceptance. The system has no guardian position table (see Section 2.2).

8.3 Processing Pipeline

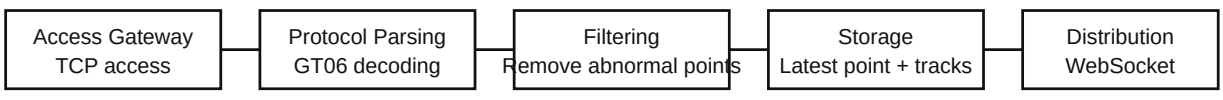


Figure 8-2 Server processing pipeline. Modules are connected by a flow of position objects and decoupled by in-memory queues / Redis, so they do not block each other. A gateway or parsing failure does not affect existing connections of the distribution module, and filtering rule updates require no restart of the access layer.

8 Server Software Structure (continued)

8.4 Filtering Rules (in Execution Order)

1. **Source filtering:** points whose source is LBS are stored only for reference; they do not enter real-time distribution or any distance-related logic.
2. **Drift filtering:** a point whose instantaneous speed, inferred from two adjacent points, exceeds a reasonable upper limit (for walking / running scenarios, 15 m/s with margin) is judged to be drift; it is discarded and does not update the latest point.
3. **Time-order arrangement:** backfilled points are sorted into the track database by packet timestamp; a packet whose timestamp is earlier than the current latest point does not trigger a real-time push, preventing the marker from jumping back.
4. **Duplicate suppression:** in a stationary state, consecutive points whose coordinate jitter is under 3 m are merged for presentation, avoiding the marker jumping in place.

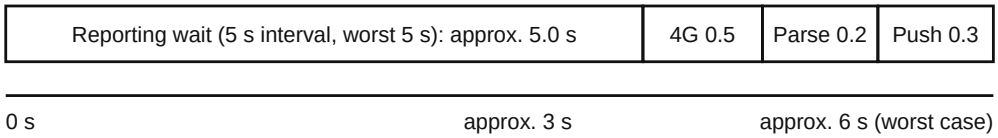
8.5 Storage Design

The latest position is stored in Redis in key-value form (one key per device) for the distribution service to read in O(1); historical tracks are written to a relational database, indexed by device and time, supporting later replay and acceptance testing. The system has no guardian position table (see Section 2.2). The position data retention period is configurable, and by default data is retained only until the end of the current monitoring task, after which the administrator performs the clearing (see Section 10.2).

9 Latency, Error and Performance Analysis

9.1 End-to-end Latency Budget

The latency of map presentation is determined mainly by the reporting interval; transport and processing stages account for a very small share. The diagram below gives the latency composition under the finalised parameters: starting from the moment the terminal completes a fix, when the guardian sees that position on the map its information age is about 5.5-6.5 s. When the monitored target moves at running speed (about 5 m/s), that latency corresponds to about 30 m of spatial lag - this is the quantitative basis for why the short-range decision cannot rely on map distance and must be completed locally by Bluetooth (Chapter 6).



The Bluetooth alarm does not pass through this chain; its local decision latency is under 1 s.

Figure 9-1 End-to-end latency budget composition. The only effective means of optimising presentation latency is to shorten the reporting interval, at the cost of increased terminal power consumption.

9.2 Reporting Interval Trade-off

Reporting interval	Worst presentation latency	Running lag distance	Reference model endurance (estimated)	Conclusion
3 s	Approx. 4 s	Approx. 20 m	Approx. 3-5 h	Good real-time performance, high endurance risk
5 s (finalised)	Approx. 6 s	Approx. 30 m	Approx. 5-8 h	The balance point; satisfies one working period
10 s	Approx. 11 s	Approx. 55 m	Over 10 h	Only suitable for low-speed, low-frequency monitoring

9.3 Error Grading

Link	Typical magnitude	Handling
GNSS positioning (open sky)	5-10 m	Used directly for map presentation
GNSS positioning (beside buildings / multipath)	10-30 m, occasional drift	Speed filtering removes abrupt points (Section 8.4)
LBS fallback	100-500 m	Source identified; does not participate in decisions
BLE near-field decision	Approx. 10 m interval decision	Threshold calibration + debounce state machine (Section 6.4)

9.4 Platform Load

In a single-target scenario the platform processes fewer than one position packet per second, so the load on a single cloud server (1-2 cores) is negligible. The horizontal scaling path is a stateless access gateway and sharding by device, with no adjustment needed within a few hundred targets. The real scaling bottleneck is rate limiting by the public map tile service, which has been avoided by the offline caching design.

10 Security, Privacy and Compliance Design

10.1 Security Mechanisms

- **Device admission:** the gateway admits devices by IMEI whitelist, and an unregistered device is not given a session; the server address can only be changed by local configuration on the terminal.
- **Channel protection:** the WebSocket between platform and receiving terminal should run over TLS and verify subscription credentials; the management back end uses strong passwords and access source restrictions.
- **Integrity:** GT06 frames carry their own checksum field, and the gateway discards a whole frame on checksum failure, preventing noise data from polluting the track.

10.2 Privacy Design

Privacy protection in this system is first an architecture question and only second a policy question: the one-way data flow makes the guardian's position "non-existent" rather than "protected" (Section 2.2); the collected fields are limited to the minimum set required for the function; position data is retained for a short period by default, and the track database and cache are cleared after the monitoring task ends; wearing of the positioning terminal and beacon must be with the prior explicit informed consent of the monitored target themselves (where a minor is involved, of their guardian), with the scope and purpose of collection clearly stated.

10.3 Compliance Note

Real-name requirements for map and account services, and personal information handling rules, differ by deployment-place regulations. Adopting a registration-free open map solution avoids the developer real-name step, but does not remove the data handler's notification and consent obligations; before formal deployment, the data handling process should be reviewed against the current Personal Information Protection Law and other regulations of the place of deployment. This document does not constitute legal advice.

11 Deployment, Calibration and Acceptance

11.1 Deployment Steps

1. Deploy Traccar in a container on the cloud server, open the GT06 access port and the WebSocket service port, and configure the device whitelist.
2. Insert the IoT card into the positioning terminal and, following the manufacturer's instructions, write the server address, port and reporting interval (5 s) into the terminal by SMS command.
3. Install the application on the receiving terminal, pre-cache the offline tiles for the monitored area, configure the platform address and subscription credentials, and complete the battery whitelist setting.
4. Fix the beacon and the positioning terminal at the same location on the monitored target's carried item, and record the pairing relationship between the beacon identifier and the terminal.

11.2 RSSI Threshold Field Calibration (Mandatory)

Calibrate in the typical environments of the actual monitored area (at least one place each of open ground, beside buildings, and indoors): the calibrator holds the receiving terminal while the monitored target holds the beacon, standing still for 30 s of sampling at each of 5 m, 10 m, 15 m and 20 m, recording the RSSI mean and fluctuation. Take the mean at 10 m as the alarm threshold, and check the warning band against the means at 15-20 m. Enter the results into Appendix B and write them into the application configuration. Recalibrate after a significant change in the environment (such as a new building obstruction).

11 Deployment, Calibration and Acceptance (continued)

11.3 Acceptance Indicators

Acceptance item	Pass standard
Track continuity	Continuous movement for 3 min with no abnormal jump points, and latency not exceeding 6.5 s
Short-range alarm	In the calibrated environment, on entering the 10 m interval the alarm triggers within 1 s; no false alarm beyond 15 m (continuous observation for 5 min)
Offline presentation	Within 15 s after the terminal goes offline, the last position and a time annotation are presented
One-way property check	Capture all outbound packets of the receiving end and all platform data tables, and confirm that no guardian position field exists

12 Known Limitations and Evolution Roadmap

Limitation	Impact	Evolution roadmap
No GNSS signal indoors	Indoors there is only LBS coarse position and Bluetooth sensing	Deploy BLE positioning base stations inside key buildings
Endurance bound to interval	At 5 s reporting, endurance is about one working period	Motion-adaptive reporting: reduce frequency when stationary, restore 5 s when moving
Public tile rate limiting	The base map may be limited at large scale or high refresh frequency	Self-build an area tile service or switch to a commercial map (the architecture already reserves this, see Section 7.3)
Terminal tamper resistance	Finished-product terminals have no tamper or shielding detection	Switch to a model with vibration / light sensors, or compensate with software anomaly detection
Freedom of finished-product firmware	Finished-product terminal firmware cannot be customised	In the longer term, evaluate a self-developed ESP32-S3 + 4G + GNSS module solution, with the platform unchanged

Appendix A Glossary (Excerpt)

Information age: the time difference between a presented position and the moment it was actually generated. **Hysteresis:** using different thresholds for triggering and exiting to avoid boundary jitter. **Sticky packet:** multiple frames arriving merged over TCP; parsing must split them by frame length. **Cold start:** positioning at power-on with no ephemeris available.

Appendix B Alarm Parameter Summary (Finalised Values and Calibration Blanks)

Parameter	Finalised / reference value	Field calibration result (to fill in)
Position reporting interval	5 s	-
BLE alarm threshold	Reference -65 dBm (approx. 10 m)	
BLE warning band start	Reference -75 dBm	
Alarm reset hysteresis	8 dB below threshold, sustained 5 s	

- End of Document - ShadowTrace Positioning Alarm System (STAS) Technical Document V1.0. Values marked "reference" or "estimated" are subject to physical testing and field calibration.