GEO1003 – Shared Notes

Master Geomatics Students

January 23, 2025

Contents

6 Wi-Fi-monitoring / Fingerprinting   23

7 Location awareness and privacy   28

1 Introduction

These notes were created by students from the MSc Geomatics for the Built Environment at TU Delft.

They are based on the lectures and literature provided by the course GEO1003 (Positioning and Location Awareness) by Edward Verbree.

2 How does GNSS work?

2.1 Introduction

GPS (Global Positioning System), also known as **NAVSTAR** (NAVigation Satellite Time And Ranging) had its first satellite launched in 1978.

Below are the 4 constellations of GNSS systems:

- **Global Positioning System (GPS)** - United States

    - *Standard Positioning Service (SPS)*
    - *Precise Positioning Service (PPS)*

- **GLONASS** - Russia
- **Galileo** - Europe

    - *Open service (OS)*
    - *Public regulated service (PRS)*

- **Beidou(/Compass)** - China

Their properties are:

Table 8.14 Properties of GNSS Mid-Earth Orbits

Constellation	Number of Planes	Radius (km)	Height (km)	Period	Orbits per Sidereal Day	Ground-Track Repeat Period (Sidereal Days)	Inclination Angle
GPS	6	26,580	20,180	11 hr, 58 min	2	1	55°
GLONASS	3	25,500	19,100	11 hr, 15 min	2.125	8	64.8°
Galileo	3	29,620	23,220	14 hr, 5 min	1.7	10	56°
Beidou	3	27,840	21,440	12 hr, 52 min	1.857	7	55°

Figure 1: Properties of GNSS systems

2.2 GPS segments

The GPS system consists of *three segments*:

1. **Space segment** (satellites with atomic clocks)
2. **Control segment** (ground stations for clock offsets)
3. **User segment** (receivers)

GNSS orbital planes are **inclined** with respect to the equator (at 55° for GPS). All the satellites form a **constellation**.
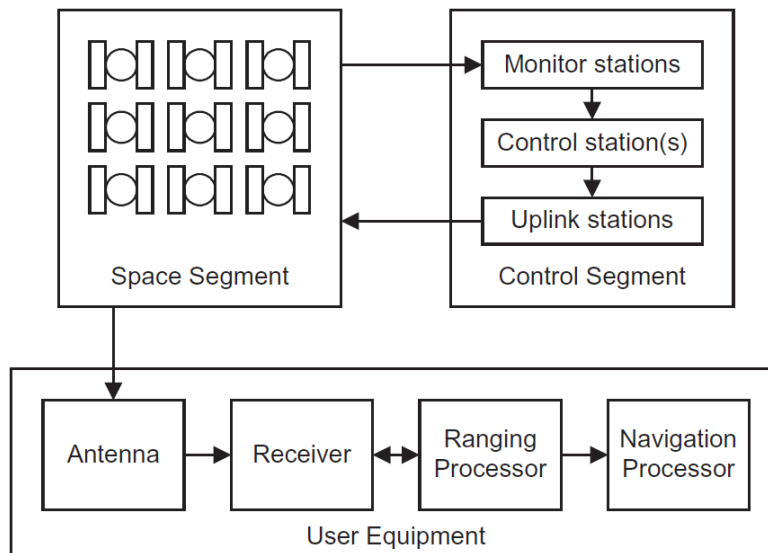
Figure 2: GPS segments

2.3 Radio Signal

2.3.1 GPS L1 CA-signal

The GPS radio signal is modulated through **Biphase shift key (BPSK) modulation**, with the amplitude of the signal given by:

$$s(t) = \sqrt{2P}C(t)D(t)\cos(2\pi f_{\text{ca}}t + \phi_0)$$

with:

- P: the signal power.
- $C(t)$: the **spreading code** (± 1). It is also called the **Pseudo Random Noise** (PRN) and is unique to each satellite, publicly available.
- $D(t)$: the **navigation data** (± 1). It contains the satellite orbit and clock information.
- f_{ca}: the **carrier frequency**. It is in the L-band between 1 and 2 GHz.
- t: time.
- ϕ_0: phase offset.

2.3.2 Message Format

There are two main formats of **navigation data message**:

- **Fixed frame**: data always transmitted in same order with same repetition intervals
- **Variable frame**: a serie of fixed-length messages may be transmitted in any order
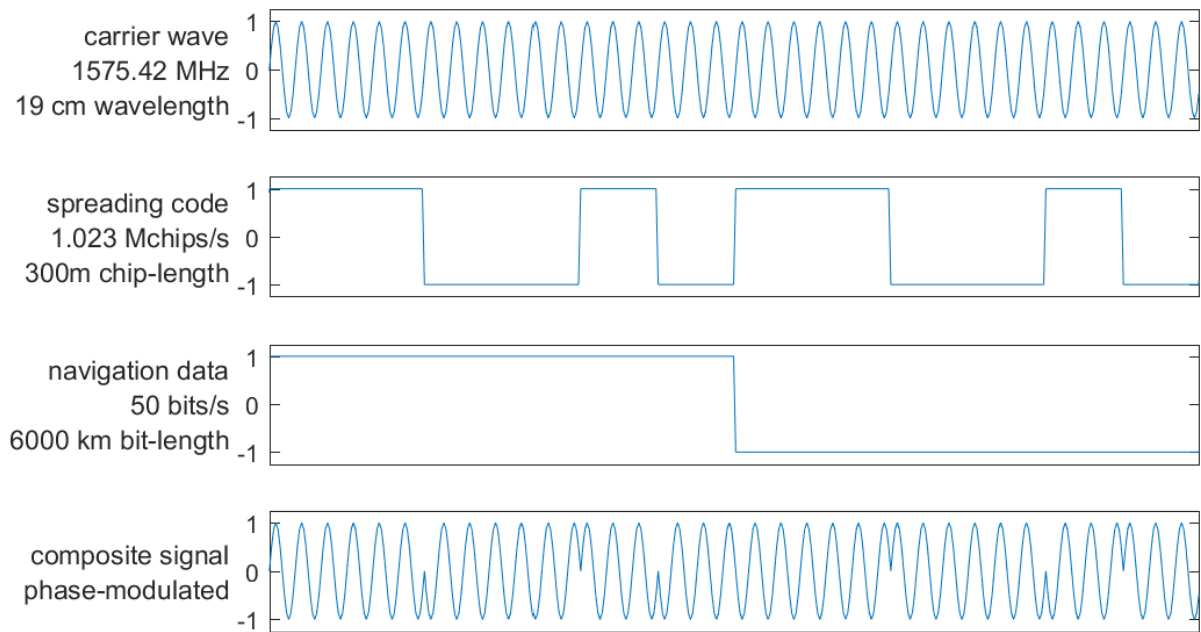
Figure 3: GPS L1 CA-signal (scale is not accurate)

2.4 Initialisation

When starting, GPS receivers try to find a particular GPS satellite on *each of their channels* (tens to hundreds). This is done by **overlaying the received signal** with a replica of the **spreading code** and then shifting it until correlation shows a maximum (best fit, or match).

2.5 Pseudorange Measurement

The **pseudorange** $p_{r,s}$ is calculated by multiplying the travel time $\tau_{r,s}$ by the speed of light c:

$$p_{r,s} = c \cdot \tau_{r,s} \text{ where } \tau_{r,s} = t_r - t_s$$

with:

- t_s: signal transmission time (from satellite s)
- t_r: time of signal arrival (determined by receiver clock)

There are then two situations:

- **Signal acquisition**: pseudo-range prediction unknown, receiver-generated spreading code searched until correlation peak is found
- **Signal tracking**: pseudo-range prediction known, only vary the receiver-generated code phase slightly

Perceived carrier frequency varies due to: **Doppler effect** and **receiver clock drift**.

A **GNSS navigation solution** is *4D* with three position dimensions and one time dimension. For any satellite, the pseudo-range measurement, corrected for satellite clock error (and other known errors):

$$\rho(t_{s,a}) = \sqrt{(r_s(t_{s,t}) - r_a(t_{s,a}))^T \cdot (r_s(t_{s,t}) - r_a(t_{s,a}))} + \delta\rho(t_{s,a})$$

with:

- $r_s(t_{s,t})$: satellite position at time of signal transmission
- $r_a(t_{s,a})$: user antenna position at time of signal arrival
- $\delta\rho(t_{s,a})$: receiver clock offset

2.6 Carrier Phase Measurement

Carrier Phase Measurement:

- Measures **fractional phase difference** between the received *carrier wave* from the satellite and a locally generated *replica*.
- Provides a **very precise distance** measure (satellite to receiver)
- Needs to be **initialized** by finding the initial number of carrier wave cycles.
- Is much more precise than pseudorange code measurement. thanks to the **carrier period** being **much smaller** than code chip duration (in L1 CA-code signal, *1540 carrier periods* fit in one PRN spreading code chip).

2.7 Jamming and Spoofing

There are multiple mays a GNSS signal may be threatened, jamming and spoofing being intentional attacks.

2.7.1 Jamming

By the time GNSS signals arrive at the antennas of a GNSS positioning system, the power level of these signals is very low. This low power level makes the signals susceptible to interference from other signals transmitted in the GNSS frequency range.

Jamming is a special case of signal interference where an attacker tries to block the incoming GNSS signal to a specific person/area.

GNSS receivers can use several methods to protect against interference and jamming:

- Signal filtering
- Multiple navigation sensors. For short-term interference, other sensors can help the receiver bridge brief periods of GNSS outage.
- Multi-frequency/multi-constellation GNSS makes it much harder to jam a signal on multiple different frequencies at once.
- Anti-jam antennas use multiple antenna elements to control the amount of signal received from a particular direction. When an anti-jam system senses interference from a direction, it turns down the antenna gain for it.

2.7.2 Spoofing

Unlike interference where GNSS is denied by overpowering the satellite signal, spoofing tricks the receiver into reporting an incorrect position. Spoofing is done by first jamming the GNSS receiver and then providing a false satellite signal that is either created by a signal generator or is a rebroadcast of a pre-recorded GNSS signal. Unlike interference, spoofing is always an intentional attack.

To protect against spoofing the same methods apply as against interference. Additionally, one of the most effective ways to protect against spoofing is to track encrypted signals that are broadcast by several of the GNSS constellations. Access to the encrypted signals is restricted and not available to all users.

2.7.3 Signal blockage

The GNSS signal can be blocked by many objects like trees or buildings, especially in urban areas. The main protection is again using multiple constellations and using additional sensors like an IMU.

2.7.4 Constellation failure

Although it is extremely unlikely that an entire constellation will fail, receivers that can track more than one constellation protect against this unlikely scenario.

3 GNSS performance

3.1 Error Sources
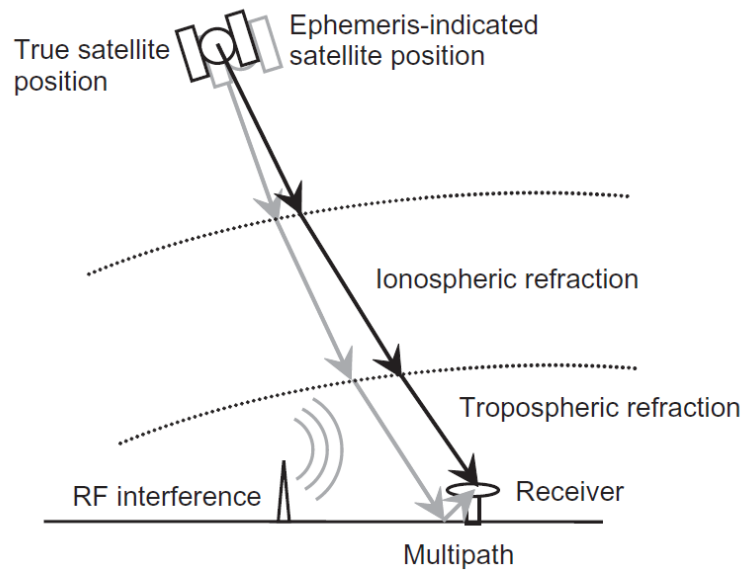
Figure 4: Principle sources of GNSS errors

3.1.1 Pseudorange Calculation

Multiple issues affect the calculation of the pseudorange:

- **satellite clock offset** (known).
- **receiver clock offset** (unknown).
- **ionosphere delay** (unknown).
- other errors, such as *multipath* (unknown).

The calculation is very sensible since $c \approx 3 \times 10^8$ m/s, and a **1 µs** error will cause a **300 m** error in the calculated distance, since we have:

$$p_{r,s} = r_{r,s} + c \cdot (\delta t_s - \delta t_r)$$

where:

- $p_{r,s}$: pseudorange
- $r_{r,s}$: actual range
- δt_s: satellite clock offset
- δt_r: receiver clock offset

3.1.2 Ionosphere Delay

Ionospheric delay:

- Is due to **free electrons** in the ionosphere.
- Is highly variable (depends on **time** and **space**).
- Ranges from *a few meters to hundreds of meters.*
- Is maximum near geomagnetic equator, around local noon and during solar maxima.
- Is proportional to $1/\text{frequency}^2$.
- Can be estimated using two frequencies. This is why satellites emit at **L1** (1575.42 MHz) and **L2** (1227.60 MHz).

3.1.3 Masking Angle

GNSS receivers **ignore signals** from below a certain elevation, making them prone to errors (typically between 5° and 15°).
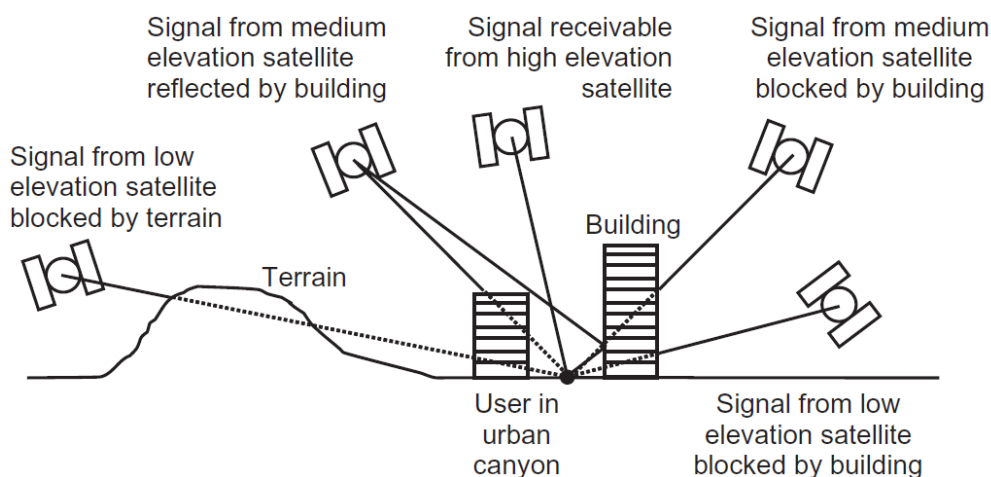
Figure 5: Errors due to terrain, buildings, and elevation angle

3.1.4 GNSS Augmentation Systems

GNSS augmentation systems supply differential corrections and integrity alerts that meet the needs of safety-critical applications. There are two types:

Criteria	Space-based augmentation systems (SBAS)	Ground-based augmentation systems (GBAS)
Coverage	Large country or small continent	Local area (e.g. an airfield)
Broadcast	Geostationary satellites	Ground-based transmitters
Precision	Lower than GBAS	Higher than SBAS

3.2 Accuracy and Precision

Accurate results may not be precise and precise results may not be accurate

- Accuracy = how close is the measurement to the actual value, can only be calculated if the ground truth is known
- Precision = how close is the measurement to other measurements, might be high even though some systematic error causes all measurements to be off

The quality of the measurement can be assessed through the carrier-to-noise-density ratio C/N_0 (signal strength).

The precision of the measurement depends on the method used:

Table 2: Precision of GNSS measurements

	Pseudorange	Carrier Phase
Precision	Few meters to few decimeters	Few centimeters to millimeter

3.3 Dilution of Precision

The geometry of the visible satellites affects accuracy. Poor satellite geometry (e.g. satellites clustered together) increases DOP, leading to less precise positioning. Good geometry (satellites spread out) reduces DOP and improves accuracy.

$$\text{Position Error} = \text{DOP} * \text{Range Error (UERE)}$$

If DOP is very high, the inaccuracy of the computed position will be much larger than the inaccuracy of the range measurement.

DOP Formula:

$$\sigma_G = \sqrt{\sigma_E^2 + \sigma_N^2 + \sigma_U^2 + \sigma_T^2}$$

Where

- σ_G is the GDOP (Geometric Dilution of Precision) value
- σ_E^2, σ_N^2, σ_U^2 are the East, North and Up variance components of receiver position estimate
- σ_T^2 is Variance of receiver clock offset estimate

If DOP is very high, the inaccuracy of the computed position will be much larger than the inaccuracy of the range measurement

Types of DOP:

- GDOP (Geometric Dilution of Precision)

  - Amplifies pseudorange error of the position determination
  - $GDOP^2 = PDOP^2 + TDOP^2$

- PDOP (Position Dilution of Precision) - 3D uncertainty representation

  - $PDOP^2 = HDOP^2 + VDOP^2$
    $\sigma_P = \sqrt{\sigma_E^2 + \sigma_N^2 + \sigma_U^2}$

- HDOP (Horizontal Dilution of Precision) - 2D uncertainty representation
$\sigma_H = \sqrt{\sigma_E^2 + \sigma_N^2}$
- VDOP (Vertical Dilution of Precision)

  - Typically, VDOP > HDOP because satellites 'below' the receiver cannot be acquired
  - This disparity increases with latitude due to less available satellites high in the sky
    * GPS constellation's orbit inclination is 55°
    * There will never be a GPS satellite directly overhead at latitudes $> 55^o$ N/S

- TDOP (Time Dilution of Precision)

Assume only 4 satellites are being observed by a receiver. Maximising the tetrahedron formed by the 4 satellite points tends to minimize GDOP.

Conversely, DOP can be infinitely large (eg: 999.0 in assignment) when receiver-satellite vectors lie in the same plane. When this happens, the solution cannot distinguish between error in receiver clock and error in receiver position.

DOP values represent accuracy, with high DOP leading to poor precision. Impact of satellite position. DOP values change with time of day and location. For example, in high-latitude areas or urban environments, poor satellite geometry can lead to high DOP and lower positioning accuracy.

3.4 Availability, Continuity and Integrity

- Availability: the percentage of time that a sufficient amount of satellites have unblocked direct lines of sight (LOSs).
- Continuity: the ability of the total navigation system to continue to perform its function during the intended operation. Continuity is critical whenever reliance on a particular system is high. For a pilot during an instrument approach procedure, continuity and integrity are vital.
- Integrity: how much the information supplied by the system can be trusted to be correct. This requires the system to provide timely warnings to the user when the equipment is unreliable for navigation purposes—due to obstructions, jamming, multipath, or any other event that degrades accuracy. Almanac: contains information about which satellite is where at which time

3.5 PPP & RTK

3.5.1 Abbreviations

- **SV**: space vehicles or orbiting space vehicles
- **RTK**: Real-Time Kinematic
- **PPP**: Precise Point Positioning
- **PPP-RTK**: Hybrid of PPP and RTK
- **CORS**: Continuously Operating Reference Station
- **NRTK**: Network RTK

- **OSR**: Observation State Representation
- **SSR**: State Space Representation

3.5.2 PPP

- **PPP** achieves decimetre-level or better accuracy by leveraging corrections transmitted via satellite or the internet.
- It utilises the **SSR** message format for efficient data transmission.
- **PPP** is suitable for global applications due to its independence from regional base stations.
- The primary limitation of **PPP** is its long convergence time, typically ranging from 5 to 30 minutes.
- **PPP** primarily corrects for orbit errors, clock errors, and biases to achieve its positioning solution.
- **PPP** offers a trade-off between accuracy and coverage, providing moderate accuracy over a wide area.
- Variations like PPP-AR and A-PPP exist, offering enhanced accuracy or specialized capabilities.

3.5.3 RTK

- **RTK** provides centimetre-level accuracy, achieving the highest precision among the discussed technologies.
- **RTK** relies on the **OSR** message format, which requires a two-way communication channel between the base station and the rover.
- The coverage area of **RTK** is limited to a short range (30-50 km) due to signal degradation with distance.
- **RTK** boasts a near-instantaneous convergence time, typically under 5 seconds.
- **RTK** corrects for various errors, including orbit errors, clock errors, bias, ionospheric delay, and tropospheric delay.
- **RTK** is widely adopted in applications demanding high accuracy within a limited area, such as surveying and agriculture.
- Developments like Network RTK (NRTK) address range limitations by incorporating networks of base stations.

3.5.4 PPP-RTK

- **PPP-RTK** combines the strengths of PPP and RTK, offering high accuracy, global coverage, and fast convergence.
- **PPP-RTK** achieves centimetre-level accuracy comparable to RTK while offering global coverage.
- **PPP-RTK** employs the efficient **SSR** message format, enabling broadcast corrections and lower bandwidth requirements.
- **PPP-RTK** utilises a network of CORS stations for precise atmospheric and clock corrections.
- **PPP-RTK** converges significantly faster than PPP, typically within 1-10 minutes, and potentially seconds under ideal conditions.

- It effectively corrects for orbit errors, clock errors, bias, ionospheric delay, and tropospheric delay, allowing for integer ambiguity resolution.
- **PPP-RTK** gracefully degrades to standard PPP performance when outside the range of the CORS network.

3.5.5 Comparing RTK, PPP, and PPP-RTK

Feature	RTK	PPP	PPP-RTK
Accuracy	**cm-level** (up to 1 cm + 1 ppm)	**dm-level or better** (less than 10 cm)	**cm-level**, similar to RTK
Coverage Area	**Limited range** (typically 30-50 km from the base station)	**Global**	**Global** with graceful degradation to standard PPP outside the range of the CORS network
Message Format	**OSR** (Observation Space Representation)	**SSR** (State Space Representation)	**SSR** (State Space Representation)
Transmission Channel	**Two-way communication** between base station and rover	Corrections delivered via **satellite or the internet**	Corrections **broadcast to users**, enabling a large number of users to connect simultaneously
Convergence Time	**Near-instantaneous** (typically less than 5 seconds)	**Relatively long** (typically 5-30 minutes)	**Fast** (typically 1-10 minutes, potentially within seconds under ideal conditions)
Errors Solved	Orbit errors, clock errors, bias, **ionospheric delay, tropospheric delay**	Orbit errors, clock errors, bias	Orbit errors, clock errors, bias, **ionospheric delay, tropospheric delay**, enabling **integer ambiguity resolution**
Key Strengths	High accuracy, very fast convergence time	Global coverage, no reliance on local base stations	High accuracy, fast convergence time, global coverage, lower bandwidth requirements compared to RTK, graceful degradation outside CORS range
Key Limitations	Limited range, high bandwidth requirements, reliance on local base stations	Long convergence time, lower accuracy compared to RTK	Still requires a CORS network (though less dense than RTK) and may degrade to standard PPP with increasing distance from CORS station
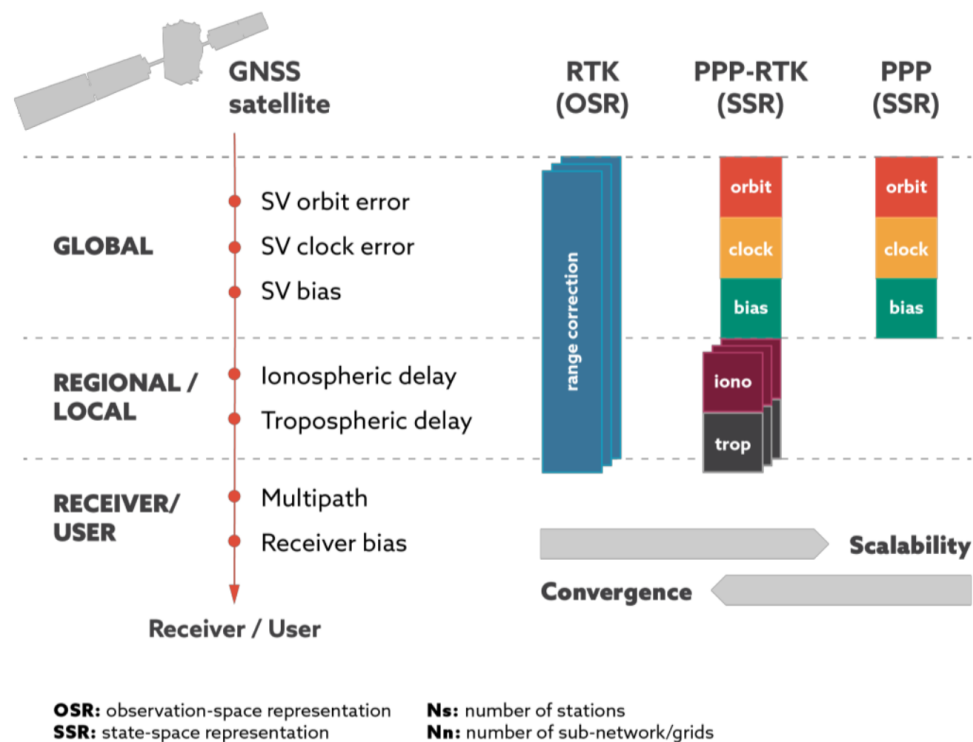
Figure 6: Difference in message format and resolved errors

3.6 Differential GNSS (DGNSS)

DGNSS improves navigation accuracy by calibrating **correlated range errors** using measurements from a **reference station** at a pre-surveyed location. However, **tracking errors, multipath effects, and NLOS reception errors** remain uncorrected since they are uncorrelated between locations.

3.6.1 How DGNSS Works

- A **reference station** transmits correction data via a data link to a **nearby rover** (within 5–10 km).
- **Key steps**:
    1. **Baseline computation**: Differences in observations between the reference and rover are used to calculate the vector between them.
    2. **Rover position**: Adding the baseline vector to the reference station's known coordinates gives the rover's position.

3.6.2 Local and Regional DGNSS

3.6.2.1 Local Area DGNSS (LADGNSS)

- Corrections from a **single reference station** are transmitted to users (rovers) within the station's range.
- User computes relative clock offsets and corrects errors for the selected satellites.

3.6.2.2 Regional Area DGNSS (RADGNSS)

- Enhances LADGNSS by using corrections from **multiple reference stations**.
- Increases accuracy for wider regional coverage.

3.6.3 Wide Area DGNSS (WADGNSS)

- Provides **meter-level accuracy** over large areas (e.g., continents or countries).
- Uses **satellite broadcasts** for corrections instead of terrestrial or network-based transmissions.
- **Corrections process**:
    - **Reference stations** send pseudo-range and ionosphere delay measurements to a Master Control Station (MCS).
    - The MCS computes corrections for satellite ephemeris, clock parameters, and ionosphere data, then broadcasts them via satellites.

3.6.4 Relative GNSS (RGNSS)

- Focuses on accurate positioning **relative to a reference station** rather than absolute accuracy relative to Earth.
- Computes the **baseline vector** by differencing pseudo-range measurements from the reference and rover.

4 GNSS in the built environment (outdoor, indoor and in between)

4.1 Multipath

4.2 Urban Canyon

4.3 Shadow Matching

5 CRS

5.1 Coordinate Systems

5.1.1 Coordinate Reference Systems

5.1.2 Geographic Coordinate Reference Systems

5.1.3 Projected Coordinate Reference Systems

5.1.4 Linear Reference Systems

5.2 Terrestrial Reference Systems and Frames

5.3 Datum and Transformations

5.3.1 Transformations and conversions

5.4 Datums

5.5 Map Projections

5.6 RDNAP

5.6.1 Coordinate Systems

Official 3D coordinate system of the Netherlands and Europe: European Terrestrial Reference System 1989 (ETRS89). ETRS89 is linked to the International Terrestrial Reference System (ITRS) by a time-dependant coordinate transformation. National coordinate systems in Europe are linked to ETRS89.

5.6.1.1 Rijksdriehoeksmeting (RD) Coordinates in the Dutch Stelsel van de Rijksdriehoeksmeting (RD) are the most-frequently used 2D coordinates on land and internal waters. RD coordinates are defined by the official transformation from ETRS89 coordinates. Maintaining reference points for ETRS89 and the transformation to RD coordinates are legal responsibilities of Kadaster.

5.6.1.2 Normaal Amsterdams Peil (NAP) Heights relative to Normaal Amsterdams Peil (NAP) are the official and the most-frequently used heights on land and internal waters. The NAP is a legal responsibility of Rijkswaterstaat Ellipsoidal heights in ETRS89 can be transformed with the quasi-geoid model to NAP with a precision higher than ETRS89 coordinates obtained with most GNSS measurements.

5.6.2 Coordinate transformation RDNAPTRANS™

The official coordinate transformation between European ETRS89 coordinates and Dutch coordinates in RD and NAP is called RDNAPTRANS™

The recommended ETRS89 realisation is ETRF2000 at epoch 2010.50 (AGRS2010). When using RDNAPTRANS™2018 it is important to use this realisation and epoch, especially for the height. For applications demanding high accuracy, it is recommended to obtain the NAP height of the point of interest by levelling to nearby NAP benchmarks.
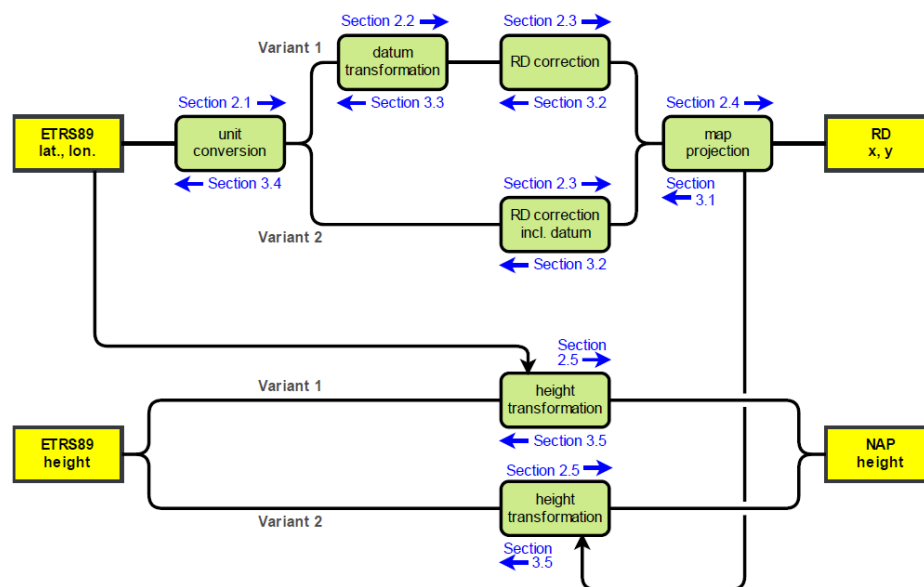
Figure 1.2.2. Guide to the sections (blue) of this document for the different steps of the transformation procedure.

Figure 7: Figure 1.2.2

There are two variants for the implementation of the horizontal component of RDNAPTRANS™2018 and two variants for the vertical component (Figure 1.2.2).

Implementation variant 1 applies the datum transformation as a separate step using a 3D similarity transformation. The advantage of implementation variant 1 is that it has no strict bounds for the area where horizontal coordinates can be transformed correctly. The disadvantage is that many software packages do not support implementation variant 1 for the horizontal component.

Implementation variant 2 includes the datum transformation in the correction grid and uses a different quasi-geoid grid for the height transformation. Implementation variant 2 for the horizontal component is supported by more software but can only be used within the bounds of the correction grid (Figure 1.1.1). The difference in the resulting coordinates between the two variants is well below 0.0010 m within the bounds of the RDNAPTRANS™2018 grids.

5.6.3 Transformation from ETRS89 to RD and NAP: Steps

1. Datum transformation

1.1 Conversion to geocentric Cartesian coordinates. Variant 1, The ellipsoidal geographic ETRS89 coordinates of a point of interest must be converted to geocentric Cartesian ETRS89 coordinates to be able to apply a 3D similarity transformation. Variant 2, the datum transformation is included in the correction grid.

1.2 3D similarity transformation

1.3 Conversion from geocentric Cartesian coordinates back to ellipsoidal geographic Bessel coordinates (Formula 2.2.3).

2. RD correction

2.1 Bilinear correction grid interpolation to obtain real Bessel coordinates.

2.2 To transform the point of interest, Determine nearest grid points

2.3 Iterative correction of the point of interest from pseudo Bessel coordinates to real Bessel coordinates,

2.4 Datum transformation in the correction grid

3. Map projection

3.1 Projection from ellipsoid to sphere (Gauss conformal projection from the ellipsoid to a sphere)

3.2 Projection from sphere to plane

4. Height transformation

4.1 Bilinear quasi-geoid grid interpolation

4.2 Transformation to NAP

5.6.4 Transformation from RD and NAP to ETRS89: Steps

1. Inverse map projection

1.1 Projection from plane to sphere

1.2 Projection from sphere to ellipsoid

2. RD correction

2.1 Direct correction

2.2 Datum transformation in the correction grid

3. Datum transformation

3.1 Variant 1, transformation from ellipsoidal geographic Bessel coordinates of a point of interest to ellipsoidal geographic ETRS89 coordinates. Variant 2 the datum transformation is included in the correction grid

3.2 the ellipsoidal geographic Bessel coordinates of a point of interest must be converted to geocentric Cartesian Bessel coordinates

3.3 The 3D similarity transformation must be applied to the geocentric Cartesian Bessel coordinates of the point of interest to obtain geocentric Cartesian ETRS89 coordinates.

3.4 The geocentric Cartesian ETRS89 coordinates of the point of interest must be converted back to ellipsoidal geographic ETRS89 coordinates. The latitude is computed iteratively.

4. Conversion of radians or decimal degrees to decimal degrees

5. Height transformation: the physical NAP height of a point of interest to the purely geometrical ellipsoidal ETRS89 height, based on the quasi-geoid model NL-GEO2018. The NAP height of the point of interest must be transformed to ellipsoidal ETRS89 height (Formula 3.5) using the interpolated quasi-geoid height of the point of interest.

6 Wi-Fi-monitoring / Fingerprinting

6.1 Wi-Fi-Based Approaches

Wi-Fi monitoring and fingerprinting are techniques used to gather information about wireless networks, but they differ in purpose, methodology, and application.

6.1.1 Wi-Fi Monitoring

- Main Idea: Wi-Fi monitoring involves passively observing and capturing Wi-Fi traffic (data packets) in the surrounding environment. This includes analyzing signals from access points (APs) and devices, such as SSIDs, signal strength, channel usage, and even packet contents (if not encrypted).
- Purpose: It's typically used for network troubleshooting, performance optimization, and security auditing.
- How It Works: A Wi-Fi adapter is set to monitor mode, allowing it to capture all wireless traffic in range, even if not destined for the monitoring device.
- Applications:

  - Analyzing traffic patterns and identifying potential interference.

6.1.2 Wi-Fi Fingerprinting

- Main Idea: Wi-Fi fingerprinting involves mapping and storing unique characteristics (or "fingerprints") of Wi-Fi signals at different locations to determine a device's location or context later.
- Purpose: It's primarily used for location-based services and indoor positioning systems (IPS).
- How It Works:

  - Offline phase: Wi-Fi signals (like Received Signal Strength Indicator, or RSSI) are measured and recorded at various locations to create a "radio map."
  - Online phase: The current Wi-Fi signal characteristics are compared to the radio map to estimate the device's location.

- Applications:

  - Indoor navigation and wayfinding (e.g., in malls, airports).
  - Asset tracking in warehouses.
  - Context-aware services like smart lighting or targeted advertisements.

6.1.3 Key Differences

Aspect	Wi-Fi Monitoring	Wi-Fi Fingerprinting
Objective	Traffic analysis, security, and troubleshooting	Location determination
Methodology	Passive traffic capture and analysis	Signal characteristic mapping and matching

Aspect	Wi-Fi Monitoring	Wi-Fi Fingerprinting
Scope	Focuses on network behavior and devices	Focuses on spatial signal patterns
Output	Data about devices, networks, and traffic	Estimated location or spatial context

In summary, Wi-Fi monitoring observes and analyzes Wi-Fi traffic for network insights, while Wi-Fi fingerprinting leverages signal characteristics to provide location-based information.

6.2 Radio Signal Based Techniques

6.2.1 Received Signal Strength (RSS)

RSSI values are Received Signal Strength (RSS) values averaged over a certain sampling period and are measured as a perceived power value P_r with the units of decibels. Using the physical property of **attenuation**, the gradual loss of intensity over a spatial propagation, RSS can be used to determine a distance d to an emitting source, as the output power value P_T is known.

$$P_r \propto P_T \frac{G_T G_R}{4\pi d^p}$$

Attenuation is characterised by a path loss exponent p which in free space is represented by a literature value $p = 2$, it is however heterogeneous in an indoor space. P_T is the transmitted power by the at the emitter. In theory, by calculating multiple perceived distances d from emitters to various receivers, position can be calculated via multi-lateration. This however this is subject to multi-path influences, introducing error.

6.2.2 Time of Arrival (ToA)

This principle measures the absolute travel time of a signal from transmitter to receiver. A **euclidian distance** can be derived using the wave speed.

6.2.3 Time Difference of Arrival (TDoA)

In this methodology, the differences of ToA many measurements is taken into account. For this, the possibility of a receiver's clock bias is terminated as it is subtracted in processing. By using two known emitter locations, receiver can be located as accurate as a hyperboloid (3D surface). A location of a receiver can be determined in 3D from four emitters by intersection of three hyperboloids. The precondition for this investigation is the precise synchronisation of all emitters.

6.2.4 Angle of Arrival (AOA)

This methodology aims to obtain the direction of an incident incoming wave signal. For this, directionally sensitive antennas are needed. By having sensors that are responsive to a specific direction in space, vector addition can be used to evaluate an angle of incidence (arrival).

6.2.5 Path-Loss

The ITU Model for Indoor Attenuation takes into account how radio waves propagate indoors. It models the path loss L, relative to the distance d between emitter and receiver.

$$L = 20 \log f + p \log d + c(k, f) - 28$$

Here f is the radio frequency and c is an empirical floor loss penetration factor. k is the number of floors between transmitter and receiver.

6.2.6 Fine Timing Measurement (FTM)

6.2.7 Radio Frequency Identification (RFID)

A Radio Frequency Identification system consists of an antenna which reads nearby active transceivers (transmit & receive) and passive tags on the radio wave part of the EM-spectrum. These transmit a unique tag ID. To position these tags in space the Cell of Origin (CoO) principle is used. A combination of ToA and AoA is used to pinpoint a location of an RFID tag.

Active RFID sensors are equipped with batteries which interrogate active radio transceivers. They are more costly than their passive opponent but offer long detection ranges of 30m or more. Location detection accuracies on the meter level have been proven possible.

Passive receivers rely on inductive coupling of EM waves and do not require batteries. These rely on receiving enough information by a scanner in order to transmit codes back. They are less costly, but only function in ranges smaller than 2 meters as signals need to travel two ways.

Applications of passive scanners include the identification of buried pipes as well as inventory control.

Using RFID scanners for indoor locations implies either having permanent active RFID sensors casting information or scanners suitable to detect passive ones. Both require large capital cost of installation.

6.3 Hybrid and Other Techniques

6.3.1 Meshlium

Meshlium is a device that uses WiFi and Bluetooth scanners to detect other devices, which can be used for a range of applications/research (e.g. Vehicle Traffic Detection).

WiFi and Bluetooth radios (of devices) periodically send out messages, containing:

- MAC address of wireless interface
- Strength of the signal (RSSI)
- Vendor of the smartphone
- WiFi Access Point and Bluetooth friendly name
- Class of Device (CoD) (only when Bluetooth)
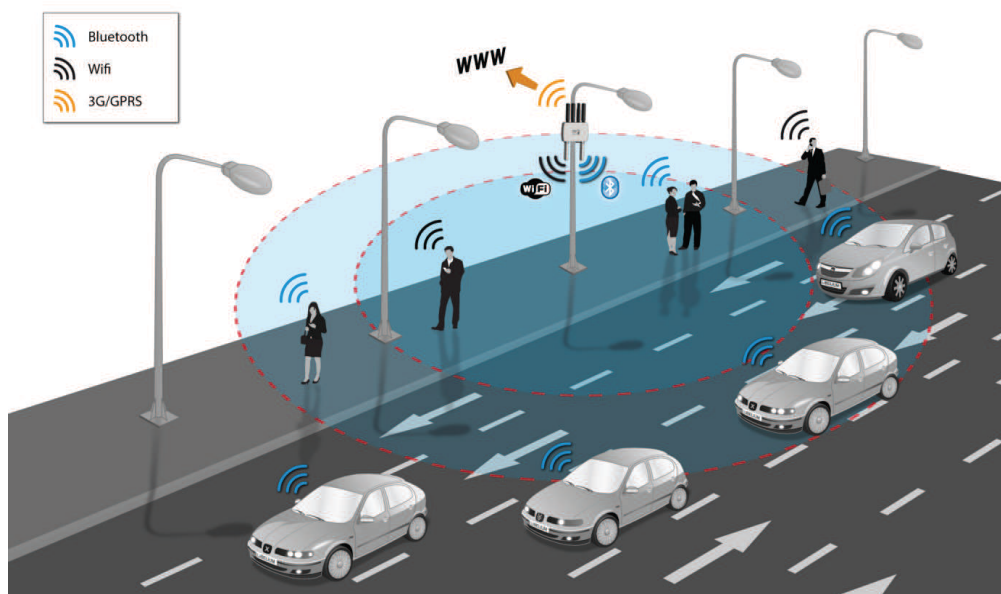
Figure 8: Meshlium Summary

MAC address randomization: for privacy randomized MAC address, reverts to **"factory" MAC address** when connected to WiFi

Adaptive Frequency Hopping (AFH): algorithm that enables Bluetooth radio to dynamically identify channels already in use and avoid them

6.3.2 Trilateration

6.3.3 Inertial Navigation Systems (INS)

6.3.4 Visual Based Indoor Localisation

6.3.5 Isovists

6.4 Performance Metrics

6.4.1 Position

6.4.2 Location

6.4.3 Yield

6.4.4 Consistency

6.4.5 Overhead

6.4.6 Latency

6.4.7 Power Consumption

6.4.8 Roll-Out and Operating Costs

7 Location awareness and privacy

7.1 Position, Location, Place and Area

Aspects of addressing space:

- **Reference**: relative (with reference to space or other objects) or absolute (agreed to by general consensus)
- **Specificity** and **Uncertainty**: the extent of the addressable space
- **Scope**: placement at different scales
- **Context**: with or without context

	Position	Location	Place	Area
Reference	Absolute (e.g. coordinate system)	Absolute (e.g. room number)	Relative, placement in a room (inside)	Relative, placement in an aggregation of rooms
Specificity/ Uncertainty	Depends on the device providing the position	Certain, defined by the physical borders (walls)	Uncertain, defined by the functional space of an object (e.g. desk)	Uncertain, defined by a more general notations (floors, parts of building)
Scope	Defined by a reference frame	Contains places	Contained in locations	Contains locations
Context	No context	Context	Context	Context
Example	"I am at 28.2314° - 33.4577°"	"I am in the living room"	"I am at the photocopier"	"I am on the second floor"

Four concepts of placement:

- **Position:** pin-point placements
- **Location:** smallest physically defined space in a building
- **Place:** placement of particular object and the uncertain (functional) space around it
- **Area:** generalised space or sub-space, containing multiple addressable locations

Framework modelling indoor space composed of:

- **Agents**: entities that navigate space, access resources and perform activities
- **Resources**
- **Space**: entirety of the enclosed environment to be navigated
- **Sub-spaces**

    - *Inert spaces*: inaccessible by agents
    - *Free spaces*:

        * Allow agents to move through them
        * Contain resources
        * Host activities

- **Modifiers**:

  - Can be applied to sub-spaces, agents and resources
  - Define the environment of a sub-space, a sub-space can be encumbered by multiple modifiers

- **Activities**

Network models: graph structure G(V, E) representing indoor space

- Nodes V: subdivisions
- Edges E: topological relationship between nodes

7.2 Personal Data Protection in the European Union

7.2.1 Data Processing Terminology

7.2.1.1 Personal Data   Under EU law, personal data is defined in the Article 4 of the General Data Protection Regulation (GDPR) as:

> [A]ny information relating to an **identified** or **identifiable natural person** ("data subject"); an identifiable natural person is one who can be identified, **directly or indirectly**, in particular by reference to an identifier such as a *name*, an *identification number*, *location* data, an *online identifier*, or to *one or more factors* specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person
>
> *GDPR, Article 4(1)*

A person who's data is being processed is a '**data subject**'.

Information that can be used to identify a person includes:

- Name
- Identification number
- Location data
- Online identifier
- Vehicle registration number
- Physical characteristics
- Genetic data
- Cultural identity

The **metadata** should also be considered, as it sometimes contains even more information. For example, the **metadata of a picture** taken with a smartphone can contain the GPS coordinates, the date and time, the author, the camera model and the settings of the camera.

The concept of identifiability is explained by the Recital 26 of the GDPR. This approach is called the **risk-based approach**:

> To determine whether a natural person is **identifiable**, account should be taken of all the means that are **reasonably likely** to be used, such as detection, by the controller or another person, to identify the natural person directly or indirectly. To determine whether the means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the **cost and time required** for identification, taking into account the **technology available at the time of processing** and **technological developments**
>
> *GDPR, Recital 26*

The form that personal data takes is not relevant to the laws that govern its usage. CCTV footage, recorded audio, pictures, DNA samples and digital communications are all examples of personal data.

All in all, this problem of distinguishing personal data from non-personal data must be handled as a **dynamic problem**. The controller must continuously **monitor the technological advancements and the capabilities of other actors** to adopt the right measures in due time.

7.2.1.2 Anonymisation Data can be kept in a form that allows for identification **no longer than is necessary for the purposes** for which the data is being processed. After personal data has served its purpose it needs to either be **erased** or **anonymised**. Data is anonymised when all identifying elements are removed.

Data that has been anonymised properly is no longer considered personal data and therefore data protection legislation no longer applies.

However, it was shown by many studies that it is possible to identify an individual through the combination of various anonymised datasets. This process is called **re-identification**.

Therefore, pretending to achieve **anonymisation that is permanent as erasure is utopic**. But it is still better than leaving the data in its initial state, reducing the risk to its lowest possible level.

7.2.1.3 Pseudonymisation In Article 4 of the GDPR, the concept of **pseudonymisation** is defined as:

> [P]rocessing of personal data in such a manner that the personal data can no longer be attributed to a **specific data subject** without the use of **additional information**, provided that such additional information is **kept separately** and is subject to **technical and organisational measures** to ensure that the personal data are not attributed to an identified or identifiable natural person
>
> *GDPR, Article 4(5)*

7.2.1.4 Data Processing **Data processing** covers a large number of possible actions. Examples include:

- collection
- organisation
- structuring
- storage
- alteration
- retrieval
- usage
- disclosure
- restriction
- erasure

Automated and non-automated processes both count as data processing.

7.2.1.5 Users of Personal Data There are two types of entities that handle personal data: **controllers** and **processors**. A controller is a natural or legal person that determines the purpose and means of processing. A processor is a natural or legal person who processes the data on behalf of the controller. A controller oversees and controls the processing, as well as being responsible and legally liable.

7.2.2 Lawfulness, Fairness and Transparency of Processing Principles

7.2.2.1 Lawfulness of Processing **Lawful processing** of personal data requires the **consent of the data subject** or **another legitimate reason**. The other five reasons are:

1. When processing personal data is necessary for performance of a **contract**.
2. For the performance of a task by a **public authority**.
3. For compliance with a **legal obligation**.
4. For the purpose of the **legitimate interests** of the controller or third parties.
5. Or if necessary to protect the **vital interests of the data subject**.

7.2.2.1.1 Consent Controllers have a duty to keep a verifiable record of any consent received. Consent can be **withdrawn at any time**. The four characteristics of consent are:

1. **Free**: Consent must be freely given.
2. **Informed**: The data subject must have sufficient information before making a decision.
3. **Specific**: For consent to be valid it must also be specific to the processing purpose.
4. **Unambiguous**: There should be no reasonable doubt that the data subject wanted to express their agreement to the processing of their data.

7.2.2.2 Fairness of Processing Data subjects should **be notified** by controllers that they are processing their data in a lawful and transparent manner, and should be able to demonstrate that they are doing so.

7.2.2.3 Transparency of Processing Controllers are obligated to take appropriate measures to ensure that data subjects remain **informed** about how their data is being used.

7.2.3 Data Processing Principles

7.2.3.1 The Principle of Purpose Limitation Data cannot be processed further in a way that is **not compatible with the original purpose**, although exceptions are possible if the new purpose is either:

- **Archiving** purposes in the public interest.
- **Scientific** or **historical** research.
- **Statistical** purposes.

7.2.3.2 The Data Minimisation Principle Processing of personal data must be **limited** to what is **necessary** to fulfil a legitimate purpose.

7.2.3.3 The Data Accuracy Principle A controller holding personal data is not allowed to process said data without ensuring with reasonable certainty that the data are **correct** and **up to date**.

7.2.3.4 The Storage Limitation Principle Data must be **deleted or anonymised** as soon as they are **no longer needed** for the purposes for which they were collected.

7.2.3.5 The Data Security Principle Controllers of personal data are required to implement appropriate **technical or organisational measures** when processing data. How appropriate a security measure is depends on the context and is determined on a **case-by-case basis** and should be regularly reviewed.

7.2.3.6 The Accountability Principle Controllers and processors are required to **actively and continuously** implement measures to promote and safeguard **data protection** in their processing activities.

7.2.4 Specific to Location Data

7.2.4.1 Sources of Location Data Location data comes from a variety of sources, including:

- **GNSS**
- **Wi-Fi**
- **Cell Phone Tracking**
- **Bluetooth Beacons transmitters**

The **diversity of sensors** inside mobile devices (microphone, camera, infrared, GPS, Bluetooth, accelerometer, Wi-Fi, fingerprint sensor, etc.) and the widespread use of various **mobile apps** make it easy to collect and combine a wide range of data. This data can then be combined with other data sources to **infer private information** about the user.

All this data is accessed by apps through APIs provided by the **operating system** (OS), which also exploits the data for its own purposes.

7.2.4.2 European Framework For location data, besides the GDPR, the European legal framework also encompasses the **e-Privacy Directive**, which establishes rules to ensure privacy and personal data protection in the electronic communications sector.

The Article 2(c) of the e-Privacy Directive defines **location data** as:

> [A]ny data processed in an electronic communications network or by an electronic communications service, indicating the **geographic position** of the terminal equipment of a user of a publicly available electronic communications service
>
> *e-Privacy Directive, Article 2(c)*

The Recital 14 the specifies that such data:

> [M]ay refer to the *latitude, longitude and altitude* to the user's terminal equipment, to the *direction of travel*, to the *level of accuracy* of the location information, to the *identification* of the network cell in which the terminal equipment is located at a certain point in time and to the *time* the location information was recorded
>
> *e-Privacy Directive, Recital 14*

The Article 9 of the GDPR also establishes **special categories of personal data** which are particularly sensitive, such as racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic biometric and health data or data concerning a natural person's sex life or sexual orientation. Location data may help infer such data, making it particularly sensitive.

7.2.4.3 Some Selected Cases

7.2.4.3.1 Location of Employees According to WP29, the use of **geolocation of employees** can find legal basis in the **legitimate interest** of the employer, who is the data controller. However, the employer must be able to demonstrate the **necessity** of the processing and the **balance of the interests** of the employer and the employees. The employer must also inform the employees about the processing of their location data. In it Opinion 8/2001, WP29 states that consent can hardly be a legal basis due to the **dependency of the employee**, making the consent **not freely given**.

In Italy, remote control of employees is limited to **specific cases** and **specific conditions** (organisational and production needs, workplace safety, protection of company assets) and must be negotiated with **union representatives** first.

In France, it is only allowed for control services related to the vehicle usage, ensuring the security of employees and goods and checking working hours. It requires a prior **Data Protection Impact Assessment** (DPIA).

7.2.4.3.2 Smart Vehicles Smart vehicles are equipped with a wide range of sensors and communication systems, which can collect a wide range of data, including location data. This location data is particularly sensitive, as it can reveal the **habits and preferences** of the driver. The **data controller** — which can be the vehicle producer, the equipment manufacturers or the service providers — shall **make the data subject aware** of how the data is processed, i.e. the frequency of collection, the possibility to shut down the tracking system and the third parties that can access the data.

The collection of location data shall be **proportionate** to the purposes by modulating the *frequency* and the *precision*. The purpose also influences the length of the data retention (data minimisation principle). For security reasons, personal data should also be **processed internally** as far as possible, and only sent to third parties when absolutely necessary.

7.2.4.3.3 Contact Tracing **Digital Contact Tracing** (DCT) apps use tracking technologies to monitor the simultaneous presence of individuals in the same place. There are two main ways to implement DCT:

- Using **proximity data**, usually with *Bluetooth Low Energy* (BLE) beacons. The absolute position is unknown and data is stored locally on the device unless a user is tested positive. This approach was used by Trace Together in Singapore.
- Using **location data**, usually with GNSS. The absolute position is known, and the data is stored on a central server. This approach was used by WeChat and Alipay in China.

In Europe, the European Commission and the European Data Protection Board (EDPB) have expressed a preference for BLE for privacy reasons. The EDPB also gave criteria for the adoption of DCT apps:

- **Voluntary** use
- **DPIA** before development
- Predilection for **proximity** data
- Disclosure of information on who the infected has been in close contact with
- Data **minimisation** and data **protection** by design
- **Encrypted identifiers** generated by BLE
- **Anonymity** of third users involved

7.3 Spaces

Perceiving and describing space:

- Empty or containing things
- Unlimited or bounded
- Physical or imaginary

Cell: is a bounded portion of space (a space unit)

Space in Positioning and Localization: partitioning space from the **sensor reception perspective**

Space classification according to reception of GPS signal:

- **Open outdoors**: outside building, open sky condition, enough satellites for positioning
- **Semi-outdoors**: outside building, slight coverage (e.g. wooded area), some satellites availability
- **Light indoors**: inside building, slight coverage (e.g. areas around windows), some satellites availability
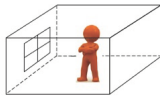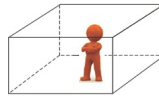- **Deep indoors**: inside building, no satellite coverage

Environment	Open Outdoors	Semi-Outdoors	Light Indoors	Deep Indoors
Definition	Outside a building	Near a building	In a room with windows	In a room without windows
Example				

Figure 9: Types of spaces for GPS

Spaces are abstracted and represented using:

- Boundary Representation (BRep)
- Constructive Solid Geometry (CSG)
- Spatial Occupancy Enumeration

Navigation network (supported by Poincaré duality theory):

- **Nodes**: associated with space units, can contain semantic information about location
- **Edges**: represent connectivity between spaces
- **Costs** (of edges): indicate distance or travel time between nodes

Space partition in 3D:

- Bottom enclosure
- Side enclosure
- Top enclosure

Field	Classification	Physical Boundary
Navigation	Functional space, Object space, Remaining space & Indoor, Semi-indoor, Semi-outdoor, Outdoor	Architectural (e.g. wall, floor, roof, fence)
Positioning and Localization	Indoor, Semi-outdoor, Outdoor	Building, waterbody, bridge, tunnel

7.4 IndoorGML