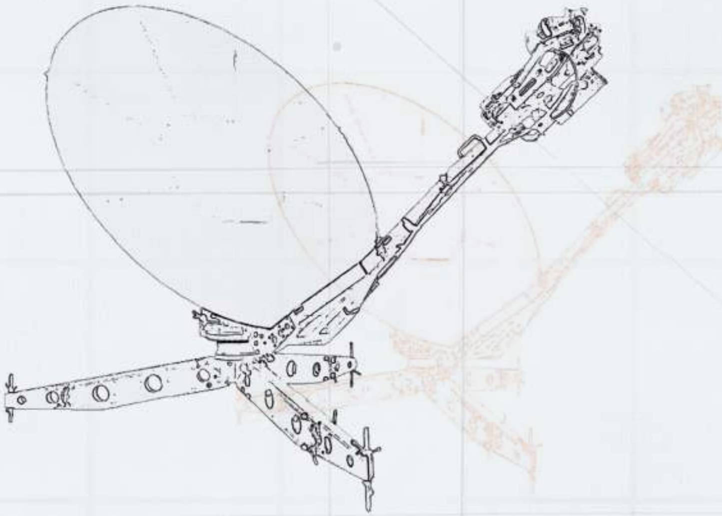
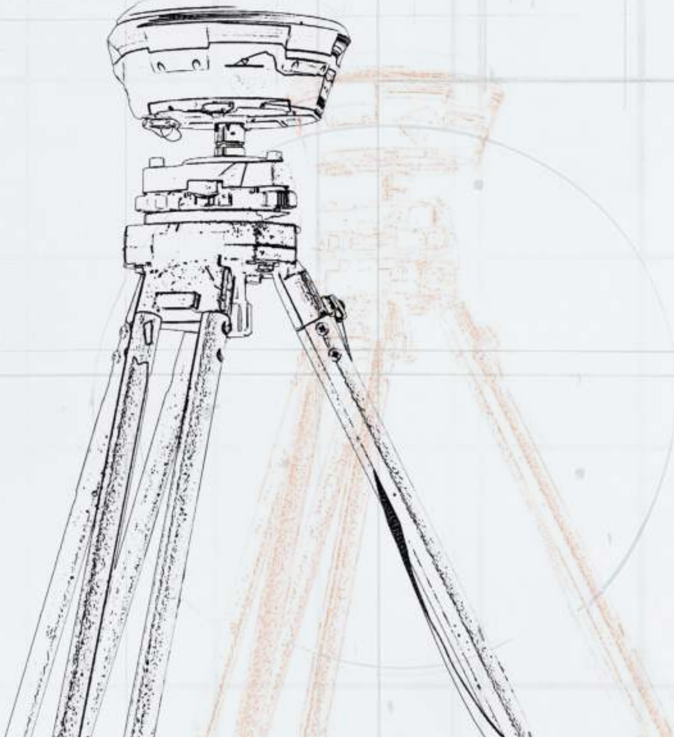
GNSS and Secure SATCOM

User Technology Report

2025 / ISSUE 1





EDITOR'S SPECIAL

Synergies from space

#EUSpace

EUSPA European Union Agency for the Space Programme

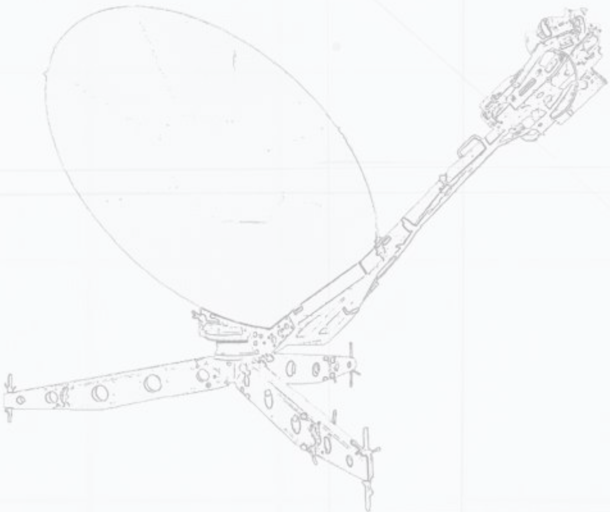
More information on the European Union is available on the Internet (http://europa.eu).
Luxembourg: Publications Office of the European Union, 2025

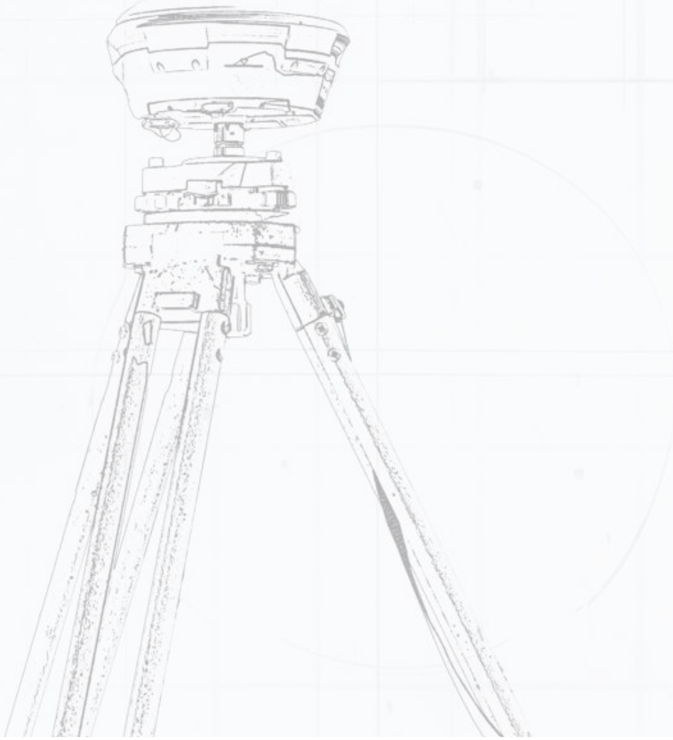
Catalogue Number: TS-01-25-000-EN-N
ISBN 978-92-9206-088-6
doi: 10.2878/9596833

GNSS and Secure SATCOM

User Technology Report

2025 / ISSUE 1





#EUSpace

EUSPA
European Union Agency for the Space Programme

FOREWORD

Dear Reader,

The space industry is rapidly evolving as we enter a new era of satellite communications and GNSS advancements. Agile New Space players are leveraging these trends to create services which benefit a wide range of users in both the public and private sectors.

Secure satellite communications (secure SATCOM) and GNSS are crucial for ensuring the resilience and strategic autonomy of the European Union and its Member States, both in space and on the ground.

The European Union is actively working on the deployment of GOVSATCOM, with EUSPA implementing the GOVSATCOM Hub. In addition, the EU is preparing the ambitious IRIS², the new Secure Connectivity Programme. These systems will complement the existing EU Space Programme's components for Navigation (Galileo and EGNOS), Earth Observation (Copernicus), and Space Situational Awareness.

In this context, EUSPA drafted the first edition of the GNSS and Secure SATCOM User Technology Report. This report is designed to offer you a comprehensive understanding of the latest developments and trends in Global Navigation Satellite Systems (GNSS) and secure Satellite Communications (SATCOM), two pivotal technologies that are increasingly intertwined and essential in our modern world.

The rapid evolution of GNSS technology is reshaping how we perceive and interact with satellite navigation. As new frequencies and signals become available for civilian use, receiver manufacturers are continuously innovating to ensure compatibility and enhanced performance, facilitating the adoption of open access signals with standardised frequency plans and modulation schemes. This global effort is steering GNSS towards a service-oriented model, promising users improved accuracy and security. The European Union Galileo system exemplifies this shift with its High Accuracy Service (HAS) and Open Service Navigation Message Authentication (OSNMA) feature, setting new benchmarks in the field.

Turning our attention to secure SATCOM, the report highlights significant technological advancements and trends redefining this domain. The push for digitalization and the integration of artificial intelligence (AI) and cloud computing are driving enhanced performance and system management. The deployment of large Non-Geostationary Orbit (NGSO) constellations is revolutionizing the field by reducing latency and improving global coverage. This comes, however, with the challenge of developing sophisticated user terminals capable of managing multiple fast-moving satellites.

Security remains a paramount concern in SATCOM facing risks from malicious actors. As a result, the development of governmental and commercial SATCOM systems is increasingly driven by the growing demand for enhanced confidentiality, integrity and availability when it comes to satellite communication links.

In the Editor's special section, we explore the potential and existing synergies between GNSS, Earth Observation (EO), and secure SATCOM at both infrastructure and user levels.

We hope this report provides valuable insights and a deeper appreciation of the dynamic GNSS and secure SATCOM user technology domains. We aim to inspire further innovation and collaboration, contributing to the future of the European Union by developing its resilience and business responsiveness.

Rodrigo da Costa
Executive Director
European Union Agency for the Space Programme (EUSPA)
January 2025

How to read this report

The first GNSS and Secure SATCOM User Technology Report builds upon the legacy of three previous issues of GNSS User Technology reports and the Secure SATCOM Market and User Technology Report. **It addresses both the GNSS and Secure SATCOM domains**, with the first two main sections providing insights into their technology and trends. The third and final section is devoted to the Editor's special focus on synergies between these domains, including Earth Observation where relevant.

GNSS user technology section

The opening section provides a summary of recent developments and future trends in GNSS technology relevant to end users. Updates on Galileo, GPS, GLONASS, BeiDou, and Regional Navigation Satellite Systems, along with the **unprecedented potential to exploit a wide range of signals and frequencies**, are described in detail. The recent **GNSS service approach** is also discussed, as well as the latest developments in the area of GNSS augmentations. **GNSS security is an increasing concern**, and vulnerabilities are analysed along with countermeasures implemented. Complementary PNT technologies are also presented as they can strengthen GNSS resilience.

Cutting-edge technologies and upcoming innovations are explored, focusing on key trends in receiver electronics design and signal processing, aimed at improving performance or reducing power consumption. Multi-frequency capabilities, PNT processing strategies, and advances in antenna design are identified as key drivers shaping the future of GNSS receiver technology. One page is dedicated to innovation activities supported by EUSPA through the **EU Fundamental Elements** R&D funding mechanism, which is instrumental in the development of EGNSS-enabled chipsets, receivers, and antennas.

In the second part of the GNSS section, **GNSS receivers are categorised into five families** based on their technological and functional commonalities: mass-market entry level and mass-market premium; professional non-regulated and professional regulated; and special applications for niche use cases.

Secure SATCOM user technology section

The secure SATCOM section of the report guides the reader through the **current status of SATCOM systems and the relevant technological evolutions** that affect the user experience, with particular emphasis on systems and technology providing a security layer. To better depict the context of 'secure' connectivity, the first section introduces the **concept of secure SATCOM and the related global players** along with a focus on the user segment and its typical architecture.

The authors have then selected major evolution trends relevant for future and forthcoming secure SATCOM systems and technology, such as: the next generation of satellite communication, which includes the **expansion from Geostationary Orbit (GEO) satellites to Non-Geostationary Orbit (NGSO) constellations**, the increase of bandwidth (**Very High Throughput Satellites – VHTS**) and the introduction of **low latency orbits**. The report elaborates on **multi-orbit terminals, digitalisation (including Cloud), AI**, and **integration of space-based satellite communication systems with 5G terrestrial networks**. Specific focus is given to **cybersecurity and quantum communication**, addressing security elements. The first part of the section ends with a brief presentation of selected **secure SATCOM EUSPA projects** funded under Horizon Europe, the EU's leading initiative for research and development.

As regards the user terminals of the secure SATCOM systems, the authors **have segmented the terminals available on the market into three main user technology types**: On-The-Move/On-The-Pause (OTM/OTP), deployable, handheld and secure IoT; and fixed and backhauling. Each of the three user technology types is specifically addressed in the second part of the secure SATCOM section providing details on their typical use cases, their main technical aspects, their related challenges, and main evolution trends.

Annexes and Editor`s special: synergies from space

The Editor's special closing the report covers the relevant **synergies among GNSS and secure SATCOM** space domains both at infrastructure and user level. Where relevant, Earth Observation (EO) contribution is described but also current or potential relevance of EU space programme components, such as Galileo or Copernicus. **Annexes** close the report with the definition of parameters and terms (Annex 1), list of acronyms (Annex 2), a general overview of GNSS constellations and frequencies (Annex 3), the methodology used for creating this user technology report (Annex 4) and information about the authors (Annex 5).

Executive summary

The first edition of the GNSS and Secure SATCOM User Technology Report provides insights into the technology features and trends of both GNSS and secure SATCOM domains and their possible synergies.

As **new GNSS frequencies** and signals become available for civilian applications, receivers' manufacturers are keeping up to speed by upgrading their receivers' baselines, thus addressing most of the 110 GNSS satellites in Medium Earth Orbit. This advancement in receivers' technology is well supported by the international coordination among GNSS, RNSS, and SBAS providers that has led to the adoption of open access signals with compatible frequency plans, common multiple access schemes, and modulation schemes. Also, a **GNSS service-oriented approach** is clearly emerging; building on top of the infrastructure development, an extended service portfolio will provide the GNSS users with increased performance and security. European GNSS is at the forefront of this process as underscored by the recently rolled-out **Galileo High Accuracy Service (HAS)** or **Open Service Navigation Message Authentication (OSNMA) feature**.

Ground and space infrastructures to augment 'native' performances of GNSS signal are also evolving to provide **better SBAS coverage and performances**, such as the SBAS Dual-Frequency Multi-Constellation (DFMC) services or the high accuracy service to enable sub-metre accuracy at global level and free of charge.

Spoofing and jamming threats are becoming a priority to be addressed both at the system and user level. Solutions like the Galileo OSNMA authentication, more resilient receivers with multiple antennas and sensors hybridisation are being explored and are starting to be implemented.

In contrast to the GNSS User Technology report published in 2020, the four receiver macrosegments have been redefined into five families of **GNSS receivers** to better reflect the current technology and capability commonalities of GNSS receivers. The largest share of current GNSS devices falls into two families, **mass-market entry-level** and **mass-market premium**, both of which are produced in very large quantities. Although the distinction can sometimes be blurred, entry-level devices prioritise low power consumption and affordability, while premium devices focus on higher performance with less emphasis on power efficiency, resulting in different technical solutions for each family.

In the **professional non-regulated family**, the diversity of applications drives a broad spectrum of device capabilities, with manufacturers often specialising in specific areas to meet the unique demands of their markets. These devices are critical in high-accuracy applications such as precision agriculture and timing solutions. Also, a specific **professional regulated family** is introduced to take into account the set of professional receivers that must fulfil regulatory standards such as the devices used for positioning in aircraft navigation, landing and take-off. Finally, a **special application family** is added to cover receivers for diverse and niche applications such as PNT in space or geodesy.

The present report also outlines **key evolutionary trends in the secure SATCOM domain** by emphasising enhanced performance and system management optimisation that can now rely on digitalisation processes, cloud environments, the advent of AI techniques and the standardisation effort for the integration of non-terrestrial networks in the 5G ecosystem. Ongoing deployment of large NGSO (Non-Geostationary Orbits) constellations is also aiming at improved performances, most notably reduced latency transmissions, relying on more advanced user terminals that need to track and switch among multiple fast-moving satellites across the sky.

This report also emphasises significant developments that directly affect users, particularly those requiring enhanced security in SATCOM transmissions. **Like terrestrial communications, satellite communications face risks from malicious actors**, including communication disruptions (availability threats), eavesdropping (compromising confidentiality), and content tampering (impacting integrity). Over the last decades, cyber-attacks targeting SATCOM systems have indeed increased sharply. "Traditional" signal jamming attacks, which began over 40 years ago, have recently been accompanied by more sophisticated threats such as Distributed Denial-of-Service (DDoS) attacks, Advanced Persistent Threats (APTs), and malware deployment. As a result, the development of governmental and commercial **SATCOM systems is increasingly driven by the growing demand of enhanced confidentiality, integrity and availability** when it comes to the satellite communication links.

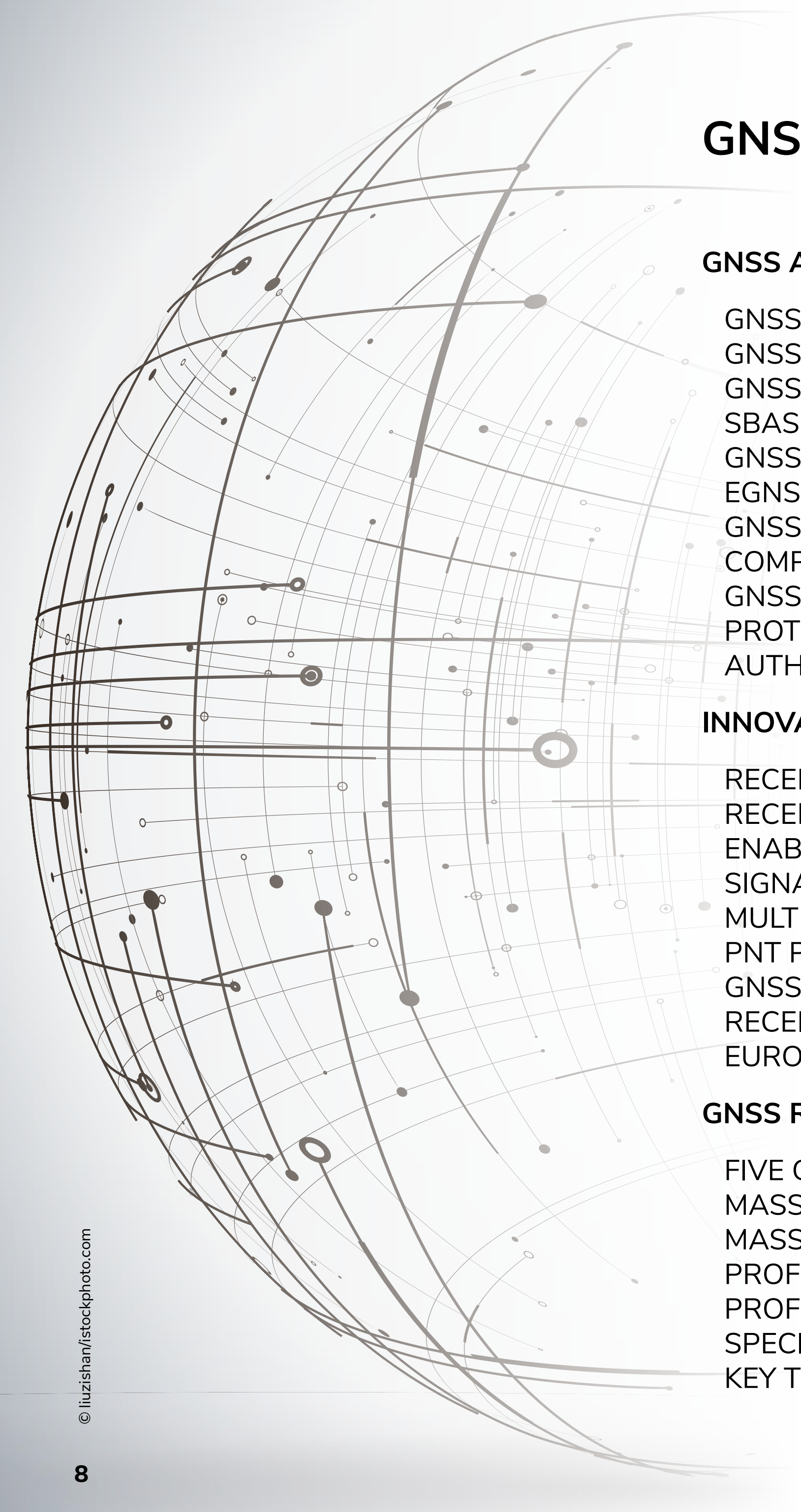
With the **digitalisation of core system components**, SATCOM systems are transitioning from legacy hardware-centric designs to modern software-oriented solutions, including those at the user terminal level. This digital shift enables user terminals to leverage multiple constellations and frequencies, significantly **improving communication link availability** thus mitigating disruptions caused by natural factors (e.g., unfavourable weather conditions or signal obstructions) or intentional interferences (e.g. jamming attacks). Additionally, advancements such as the **integration of modern 5G security features, the use of optical communications**, which are inherently more resistant to jamming and spoofing, and experimental **quantum communication links** for ultra-secure encryption key distribution are all addressing the evolving threat landscape.

To better describe the secure SATCOM user technology and address its relevant technological trends, the secure SATCOM user terminals have been categorised by the authors into **three "user technology types"** describing their main operational use, technical aspects, related technological factors, and main evolution trends.

The Editor's special closing the report covers the main synergies trends among GNSS, EO, and secure SATCOM space **domains at infrastructure level**: institutional space initiatives as well as new space endeavours are starting to break the past silos approach used in the definition of space missions. Also, the Editor's special illustrates how **synergies across different space domains already exist at user level**. Since the last decade, users enjoy the synergies among the different space systems and related applications, as in the case for EO data relayed through SATCOM systems; GNSS enabling the operations of NGSO SATCOM terminals; complementary use of GNSS and secure SATCOM in transport and emergency management; remote sensors used by Copernicus utilising both GNSS and SATCOM; or high-accuracy GNSS positioning in remote areas enabled by SATCOM.

Go to main table of contents

Table of Contents



GNSS user technology overview

GNSS AND AUGMENTATION SYSTEMS

INNOVATIONS AT THE RECEIVER LEVEL

GNSS RECEIVERS' TECHNOLOGY FAMILIES

Interoperable multi-frequency, multi-GNSS is the current reality

Multiple systems provide continuous worldwide navigation services

The four **Global Navigation Satellite Systems (GNSS)—GPS** (USA), **Galileo** (EU), **GLONASS** (Russia), and **BeiDou** (China)—will continue to provide navigation services with global coverage for the foreseeable future, with more than 110 GNSS satellites in Medium Earth Orbit.

Two **Regional Navigation Satellite Systems** (**RNSS**)—India's **NavIC**, and Japan's **QZSS**—further enhance navigation capabilities in their respective areas. A third regional system, the **Korean Positioning System** (**KPS**), is set to join them by 2035.

Satellite-Based Augmentation Systems (**SBAS**) broadcast signals similar to those of GNSS, primarily to provide integrity information and wide-area corrections. These signals may optionally be used also as additional navigation signals (e.g. the United States's Wide Area Augmentation System –**WAAS**).

Global harmonisation of open access GNSS signals: realising a seamless multi-GNSS world

International coordination among GNSS, RNSS, and SBAS providers has led to the adoption of open access signals with compatible frequency plans, common multiple access schemes, and modulation schemes. For example, GLONASS is adding CDMA to its legacy FDMA scheme, while Galileo E1 and GPS L1C signals are very similar and therefore highly interoperable. This facilitates the design of multi-constellation GNSS chipsets and receivers, benefiting end users.

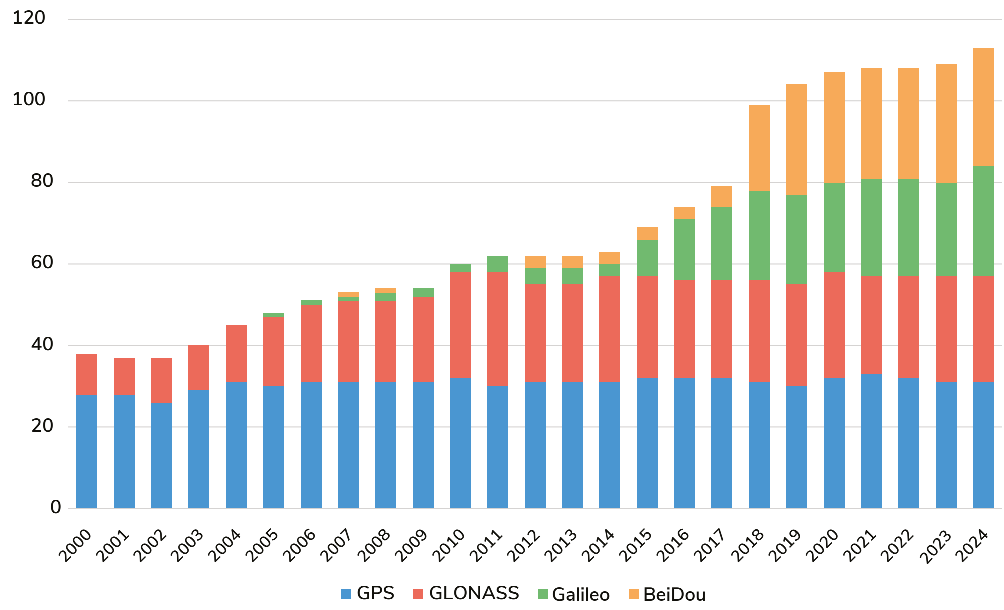
All GNSS and RNSS constellations broadcast open access signals in common multiple frequency bands. SBAS plans to upgrade services to support multiple frequencies and constellations in the coming years.

The GNSS world is now firmly established as multi-frequency and multi-constellation.

More services available to end users

In addition to their core Open PNT service supported by interoperable open access signals, each GNSS/RNSS provides specific services through dedicated signals and frequencies. This includes governmental services[1] like Galileo's Public Regulated Service (PRS) or GPS's Protected Positioning Service (PPS), and value-added services such as Galileo's High-Accuracy Service (HAS), QZSS's Centimetre Level Augmentation Service (CLAS), or BeiDou's regional short communication (RSMC) service.

OPERATIONAL[2] GNSS SATELLITES (MEO ONLY)



Frequencies: a scarce resource to be protected

These systems transmit or plan to transmit navigation signals in two common frequency ranges: L5/E5/B2/L3 signals in the lower L-band (1164-1215 megahertz) and L1/E1/B1 signals in the upper L-band (1559-1610 megahertz). These frequency bands, often referred to by their signal names (e.g., L1 or E5 band), are allocated worldwide to GNSS on a primary basis and are shared with aeronautical radio navigation service (ARNS) systems.

To ensure the harmonious development of GNSS services, the International Telecommunications Union (ITU) establishes criteria and recommendations to ensure that the different systems and signals can coexist without causing mutual harmful interference.

1: Not discussed in this report
2: Excluding test satellites. Reporting global coverage only (Medium Earth Orbit).

GNSS infrastructure evolves to provide better quality of services

GNSS

GPS www.gps.gov

The USA is currently deploying GPS III satellites. As of July 2024, the operational GPS constellation includes six such satellites. These are the first satellites to feature the new L1C signal, almost identical to its Galileo E1C counterpart. They also broadcast the legacy L1 C/A and the more recent L2C and L5 signals, resulting in the future availability of four civil GPS signals.
In mid 2024, L2C is available on 24 satellites and L5 on 18 satellites, both with a "pre-operational" status. L1C is broadcast on the six GPS III satellites.

GLONASS www.glonass-iac.ru

The first of the latest generation GLONASS-K satellites entered service in February 2016. These satellites transmit CDMA signals (currently at L3 = 1202.025 megahertz in the E5 band, and in the future at the L1 and L2 frequencies) in addition to the legacy FDMA signals and include a SAR transponder. The previous generation GLONASS-M satellites were used until 2019 for constellation maintenance but have been superseded by GLONASS K1 and K2 satellites from 2020 onwards.
In the future (post-2025), the current MEO-only constellation could be augmented by six additional satellites in Highly Elliptical Orbits (HEO), named GLONASS-V.

Galileo www.gsc-europa.eu

Operational since December 2016, Galileo is continuously evolving. Its first generation provides high-quality Open Service using innovative E1 and E5 band signals, while the Second Generation is in development. Galileo, the first GNSS constellation with a SAR capability, offers a return link for users in distress. Upcoming unique features include the Navigation Message Authentication (OSNMA) and an encrypted E6 signal, known as the Signal Authentication Service (SAS), which will offer the first anti-spoofing protection for civilian GNSS users. Since January 2023, Galileo's High Accuracy Service (HAS) has been available via an open data channel on the E6 frequency for high-accuracy augmentation messages.

BeiDou en.beidou.gov.cn

The third-generation BeiDou system (BDS-3) has been fully deployed since June 2020, with 30 satellites (24 MEO, 3 GEO, and 3 IGSO) providing global and regional services. The system transmits signals at B1 (E1/L1), B2 (E5/L5), and B3 (~E6) frequencies. Sharing frequency bands and similar signal waveforms with GPS and Galileo, BDS-3 significantly enhances the interoperable, multi-GNSS world. BeiDou operates the largest constellation of 30 satellites plus possible in-orbit spares. Regional services include a Precise Point Positioning (PPP) Service, and a Regional Short Message Communication (RSMC) Service.

RNSS

NavIC www.isro.gov.in

Navigation with Indian Constellation (NavIC), formerly known as the Indian Regional Navigation Satellite System (IRNSS), covers India and a region extending 1,500 kilometres around it. There are plans for further coverage extension by increasing the number of satellites in the constellation from 7 to 11. NavIC provides a Standard Positioning Service and a Precision Service, both carried on L5 (1176.45 megahertz) and S-band (2492.028 megahertz). A new civilian signal is being introduced in the L1 band (1575.42 MHz), which is interoperable with other GNSS signals. All forthcoming NavIC satellites will broadcast SPS signals in L1, L5, and S-bands.
The NavIC seven-satellite constellation is functional, and the first of the follow-on satellites, NVS-01, with indigenous atomic clocks and the new L1 civilian signal, was launched in May 2023.

QZSS qzss.go.jp

QZSS (Michibiki) has operated as a four-satellite constellation since November 2018, with three satellites always visible in the Asia-Oceania region. It provides a GPS Complementary Service (PNT service), GNSS Augmentation Services like SLAS (Sub-metre Level Augmentation Service) and CLAS (Centimetre Level Augmentation Service), SBAS, and a Messaging Service.
Efforts are underway to expand the system to seven satellites, with launches planned from 2024 to 2025. This will enable a QZSS-only positioning capability, as well as the QZNMA (QZSS Navigation Message Authentication) service, the MADOCA-PPP service, and the extended EWSS (Emergency Warning Satellite Service).

KPS www.kari.re.kr

Korea is planning to build the Korean Positioning System (KPS) by 2035 according to its 3rd Master Plan for Space Development and Promotion. The goal is to create a precise, reliable satellite navigation system providing centimetre-level location information to the Korean Peninsula and surrounding areas. It will be compatible with the US commercial GPS to offer higher-quality service than currently available. The KPS constellation will consist of three GEO and five IGSO satellites, carrying navigation, timing, SBAS, and SAR payloads.

Back to main table of contents | Back to GNSS user technology overview page

All systems are planning to offer additional civil signals

New signal components for civilian users

GNSS and RNSS providers are continually enhancing the quality of their services by introducing new capabilities and improving performance and coverage. These efforts are leading to improved user experience and greater interoperability across systems.

As a result, new signals are being gradually introduced for civilian users, while maintaining backward compatibility with existing receivers by continuing to support legacy signals. All systems will therefore offer at least three open signals across three different frequency bands, supporting standard navigation services and often providing new, enhanced services.

Regional complements

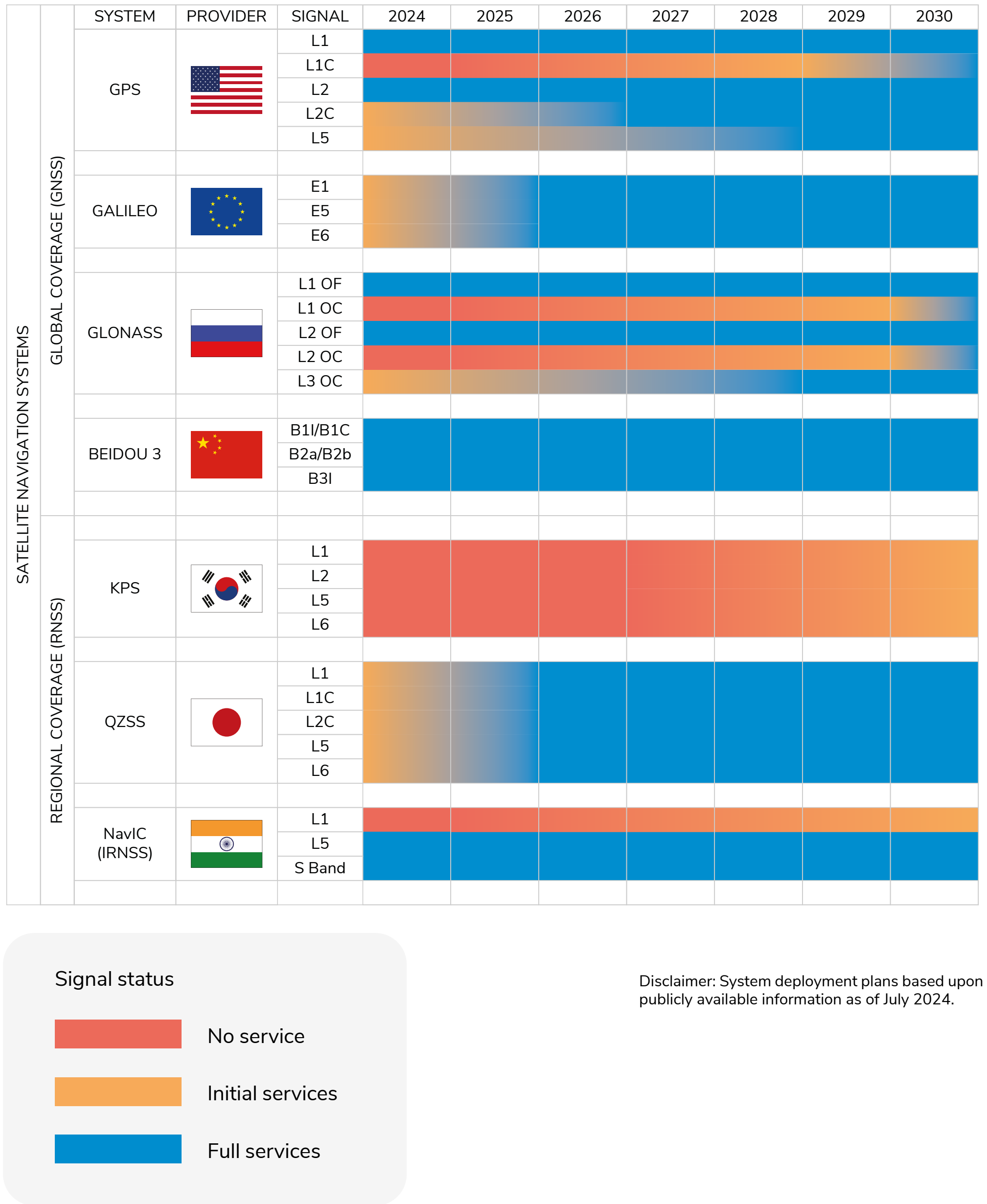
While the four major GNSS systems are designed to provide global coverage, two of them are also incorporating—or planning to incorporate—a regional complement to enhance satellite availability and services:

- **BeiDou** includes several IGSO and GEO satellites. Some of these are legacy satellites from BeiDou-2, originally a regional system, while others are newer BeiDou-3 satellites that support services like B2b PPP and RSMC.
- **GLONASS** currently consists solely of MEO satellites but plans to deploy six IGSO satellites. These additions aim to improve PDOP, enhancing navigation in challenging environments like dense urban areas in the Eastern Hemisphere, and to broadcast GLONASS High-Accuracy Service PPP corrections within the service area.

Ground segment updates

Satellite navigation systems rely not only on a space segment to broadcast signals but also on a sophisticated ground segment to control the constellation's operation and to monitor the performance of each signal and of the overall system.

Updates that are visible to end users, such as new signals or services, are only made possible by less visible enhancements to the ground segment of these systems. For instance, in March and April 2024, the ground segment of the Galileo satellite navigation system underwent a significant upgrade without any disruption to the services. This update, which enhances the Galileo Control Segment responsible for managing the orbiting satellite constellation, involved improvements to both the operational control centres and the extensive network of ground stations.



Disclaimer: System deployment plans based upon publicly available information as of July 2024.

SBAS enhance GNSS performance and enable safety critical operations

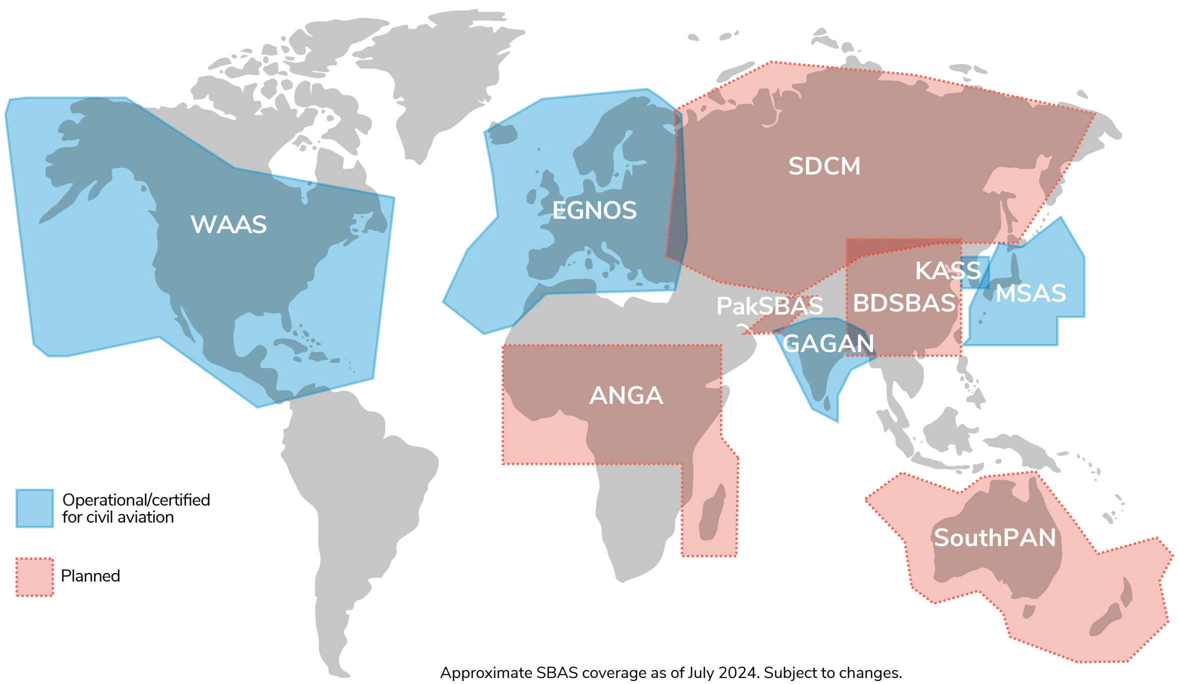
Definition, purpose and benefits of SBAS

Satellite-Based Augmentation Systems (**SBAS**) are wide area augmentation systems that enhance the Global Navigation Satellite System (GNSS), providing users with more accurate and reliable navigation services than GNSS alone.

While GNSS is sufficient for many users, it does not fully meet the stringent safety requirements of civil aviation. Safety in this context refers to the probability of GNSS failure leading to an accident. SBAS offers a comprehensive and flexible solution for integrating GNSS into civil aviation by monitoring and correcting GNSS signals and ionospheric conditions in real time.

SBAS delivers significantly enhanced navigation accuracy over basic GNSS systems, coupled with the high integrity required for aviation operations. It is a vital component of **Performance-Based Navigation** (**PBN**), enabling improved operational efficiencies, cost savings, and reduced emissions. Although primarily designed for civil aviation, SBAS can also benefit other transport modes, such as maritime and rail, as well as other high-accuracy fields, such as geomatics and precision farming.

SBAS INDICATIVE SERVICE AREAS



Approximate SBAS coverage as of July 2024. Subject to changes.

Interoperability and availability

To ensure seamless operation, each SBAS system is developed according to **International Civil Aviation Organisation** (**ICAO**) **Standards and Recommended Practices** (**SARPs**) Annex 10. Receivers designed in compliance with RTCA or EUROCAE **Minimum Operational Performance Standards** (**MOPS**) are interoperable with SBAS systems that adhere to these standards, allowing aircraft to transition smoothly between different SBAS coverage areas. Regular meetings of SBAS service providers in the **Interoperability Working Group** ensure continued coordination and interoperability.

As of July 2024, there are five certified SBAS in operation for safety-critical aviation operations, with five others in various stages of development. Current SBAS service coverage is provided by a network of interoperable systems, and global SBAS coverage continues to expand (see figure above).

SBAS first generation and evolution (DFMC)

The initial Satellite-Based Augmentation Systems (SBAS) were designed with **only the US GPS** in mind, utilising the **L1 frequency band**, which was then the sole GNSS-band reserved for civil aviation. Despite these limitations, they provide a 'Safety-of-Life' service to aviation users relying exclusively on GPS L1 C/A signals.

However, these constraints limit their achievable performance: legacy SBAS users cannot utilise other frequencies to calculate ionospheric delays or benefit from extra satellites for redundancy.

The allocation of the L5 band for civil navigation lifted this L1-only constraint and offered the opportunity to enhance the SBAS protocol.

The new **Dual-Frequency Multi-Constellation SBAS** (**DFMC SBAS**) protocol, nearing completion (SARPs have already been published, while work is still ongoing for the receivers' MOPS), will include both **dual-frequency capabilities and support for other GNSS constellations**. This will enable coverage in regions with fewer reference stations.

DFMC SBAS will significantly improve service availability and integrity, particularly in regions with high ionospheric activity. It will operate alongside the L1 SBAS service, allowing receivers to utilise both dual-frequency and legacy services.

A portfolio of satellite navigation services for diverse PNT needs

The GNSS, RNSS, and SBAS space and ground infrastructure outlined earlier in this report is designed to deliver signals and data that serve as the essential building blocks for services meeting user requirements for Positioning, Navigation, and Timing (PNT) information.
Given the wide range of user requirements, which vary by application area and evolve over time, no single service can meet all needs — one size does not fit all. As a result, GNSS and RNSS offer multiple services or service levels to better align with specific user demands.
Similarly, user equipment is designed to access one or more of these services, optimising their use according to the specific requirements of the intended application.

Categories of satellite navigation services

Satellite navigation services are usually classified as:

- **Core PNT Services**: At the heart of all GNSS systems, core PNT services offer users global, continuous timing information and 3D positioning with typical accuracies within metres. These foundational services have been integral to GNSS since their inception, offering open access and utilising generally interoperable signals. Most systems also include restricted governmental services, which are not addressed in this report.
- **First-Generation SBAS Services**: Originally developed as regional augmentations to the GPS L1 C/A signal, SBAS provide Safety of Life (SoL) services, principally for aviation. These services are available from regional systems such as WAAS, EGNOS, KASS, GAGAN, and QZSS. Whilst SBAS signals carry unique navigation messages, they share all other characteristics with GPS L1 C/A, enabling non-aviation receivers to utilise them for enhanced accuracy and integrity. However, only certified aviation terminals benefit from the full integrity **guarantee**.
- **SBAS DFMC Services**: Dual-Frequency Multi-Constellation (DFMC) services represent the next evolution of SBAS, standardised by the ICAO to enhance SoL services for aviation. DFMC services deliver improved performance and expanded operational areas through the utilisation of multiple frequencies and constellations. Furthermore, this development presents opportunities to further extend safety services to non-aviation domains and to introduce value-added services, including High Accuracy (HA) services.
- **High Accuracy (HA) Services**: High Accuracy services are a recent addition to GNSS and RNSS, offering accuracies ranging from sub-metre to centimetre levels. These services can be delivered directly by GNSS systems (e.g., Galileo HAS), through regional augmentations (such as SBAS DFMC spin-offs), RNSS (such as QZSS), or regional GNSS components (such as GLONASS or BeiDou).
- **Non-PNT Services**: Although the primary mission of GNSS and RNSS systems is the provision of PNT services, their infrastructure can also support other synergistic services. These additional services often exploit the systems' dual positioning and communication capabilities. Examples include Emergency Warning Satellite Services provided by QZSS or Galileo, the Return Link feature of Galileo's Search and Rescue (SAR) service, and short messaging services offered by other systems. Some non-PNT services may require additional payloads, such as those utilised in the COSPAS-SARSAT Medium Earth Orbit Search and Rescue (MEOSAR) distress system.

European GNSS (EGNSS) services

European Global Navigation Satellite Systems (EGNSS) make a significant contribution to the global provision of satellite navigation services through Galileo and EGNOS.

Galileo Services

Galileo is the EU's global satellite navigation system, offers precise and reliable global positioning under civilian control, interoperable with other GNSS systems like GPS, GLONASS, and BeiDou. Its services include:

- **Open Service (OS)**: Positioning and synchronisation with additional features like OSNMA for authentication.
- **High-Accuracy Service (HAS)**: High-accuracy positioning via supplementary data.
- **Signal Authentication Service (SAS)**[1]: Encrypted signal authentication.
- **Public Regulated Service (PRS)**: Restricted to government-authorised users for high-security applications.
- **Emergency Warning Satellite Service (EWS)**[1]: Warnings for natural disasters and emergencies.
- **Timing Service (TS)**[1], providing an accurate and robust reference time including the monitoring of accuracy level delivered, as well as the realisation of Coordinated Universal Time (UTC).

Galileo also **contributes** to:

- **Search And Rescue (SAR) support**: Part of the COSPAS-SARSAT system, relaying distress signals and providing a return link to users.
- **Safety of Life Services support**: Based on Galileo Open Service signals, as standardised at the European Union or international level for use by safety-of-life services in combination with EGNOS and other satellite navigation systems.
- **Space Weather Information and Early Warning Services**[1]: Information via the GNSS Service Centre to mitigate space-related risks.

EGNOS Services

EGNOS, the European Satellite-Based Augmentation Service, augments GPS and, in the future, Galileo. Its services include:

- EGNOS **Open Service (OS)**: Positioning and synchronisation.
- **EGNOS Data Access Service (EDAS)**: Internet access to specific GNSS data streams for the provision of added-value services, professional applications, commercial products, R&D, etc.
- **Safety-of-Life Service (SoL)**: High-continuity, high-accuracy positioning with integrity alerts, crucial for civil aviation, compliant with ICAO standards. Since March 2024, EGNOS SoL service also comprises the **EGNOS Safety of Life (SoL) assisted service for Maritime Users (ESMAS)**; enabling maritime navigation for SOLAS operations, in line with the requirements of IMO Resolution A.1046(27).

All EGNSS services are provided free of direct user charges. Further information on Galileo and EGNOS can be found in the EUSPA website (www.euspa.europa.eu).

1: Services under development as of the end of 2024

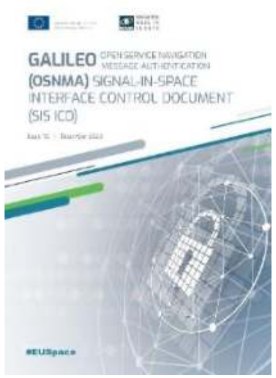
Innovative services to better serve users' needs

EGNSS: Pioneering innovative services

From its inception, Galileo revolutionised the GNSS landscape by introducing a dual-frequency Open Service (OS) in a world that had previously relied solely on single-frequency solutions. Two decades later, even entry-level receivers are adopting dual-frequency capabilities, underscoring the visionary foresight of Galileo's designers. This milestone not only challenged the status quo but set a new industry standard, highlighting the enduring impact of Galileo's innovative approach.

Galileo has consistently pushed the boundaries of GNSS technology, continuously driving progress and introducing a diverse range of services tailored to meet evolving user needs. Its ability to anticipate and adapt to future demands ensures that Galileo remains at the forefront of GNSS innovation. This forward-thinking philosophy is the cornerstone of European GNSS programmes, perfectly aligning with EUSPA's mission: "Linking Space to User Needs."

Over the years, we have witnessed the emergence of specialised services, such as the life-saving Galileo Search and Rescue Service (SAR), the Galileo High Accuracy Service (HAS), and the EGNOS EDAS service, among others. These advancements reflect the EGNSS programme's commitment to innovation and user-centric service delivery.



Key EGNSS milestones

Over the past 30 years, the European space programme has delivered the following accomplishments to the user community:

- First dual-frequency OS
- First operational MEOSAR
- First SAR return link service for distress beacons
- First terrestrial GNSS integrity data distribution service (EDAS)
- First SBAS service dedicated to maritime users (ESMAS)
- First free global High Accuracy Service (HAS)
- First GNSS data authentication capability (OSNMA)

Today, the journey of innovation continues with the evolution of EGNOS, the full deployment of Galileo's first generation (G1G), and the development of its second generation (G2G). As a result, we stand on the brink of a new era in GNSS innovation, with a wealth of new or enhanced features on the horizon.

EGNOS will naturally evolve alongside SBAS advancements, with its Safety of Life (SoL) service set to include **Dual-Frequency Multi-Constellation** (**DFMC**) capability, augmenting both **GPS and Galileo**, in addition to its current legacy implementation (GPS L1 only). Moreover, studies are underway to integrate EGNOS into the European Rail Traffic Management System (ERTMS) and to develop a tailored solution for train localisation.

Galileo services are continually being developed to enhance performance and add new capabilities. This includes full deployment of all currently defined services (see page 13) and key innovations like extending **OSNMA** to enable **GPS satellite message authentication** and expanding SAR support with **remote beacon activation** and **two-way communication**.

Galileo second generation will enable new features, including:
- Increased system robustness through generalised data authentication and ranging authentication for OS signals, enabling **PVT authentication** across the E1, E5, and E6 frequency bands;
- Support for SoL services compatible with **EGNOS DFMC** evolution and assistance for Advanced Receiver Autonomous Integrity Monitoring (**ARAIM**) via **ISM** message dissemination;
- New 'IoT-friendly' signal components allowing very fast Time to First Fix (**TTFF**) and low-energy modes.

This list is non-exhaustive, and the second generation of Galileo (**G2G**) is designed with flexibility and spare capacity for future developments.

Staying connected with end users

A key element of the EU Space Programme's user-centric approach is the commitment and ability to engage with end users, gathering their feedback and requirements. This is the mission of EUSPA, which regularly organises the **User Consultation Platform** (**UCP**). The UCP is a structured initiative that brings together stakeholders who utilise positioning, navigation, and timing as well as earth observation services and technologies. The outcomes of the UCP are also used to compile and update a series of Reports on User Needs and Requirements for each market segment. These reports are published annually, and previous editions are available at www.euspa-ucp.eu.

Besides these consultations, the EU Space Programme regularly keeps end users informed of the performance of the EGNSS services via the European GNSS Service Centre (GSC) web portal. The information provided includes performance reports both for Galileo services (OS, SAR and HAS) and for EGNOS services.

GNSS augmentations and assistance

GNSS augmentations

GNSS augmentation services enhance Global Navigation Satellite Systems (GNSS) by improving accuracy, reliability, and availability. They integrate external data to correct errors from atmospheric conditions, satellite inaccuracies, and other factors, leading to more precise positioning and navigation. Historically, systems like Satellite-Based Augmentation Systems (SBAS) and Differential GNSS (DGNSS) were developed to improve both accuracy and integrity. Assisted GNSS (A-GNSS) further enhances availability, reduces time to first fix (TTFF), and lowers power consumption.

Key methods include:

- **Differential GNSS** (**DGNSS**): Improves GNSS accuracy by using a reference receiver at a known location to calculate and broadcast corrections for satellite errors. Users apply these corrections to enhance their positioning accuracy.
- **Real-Time Kinematic** (**RTK**): An advanced DGNSS technique that provides centimetre-level accuracy by using carrier phase observables and resolving their ambiguities. It is most effective with multiple frequencies and short baselines.
- **Network DGNSS/RTK**: Extends these methods by using multiple reference sites, expanding coverage and improving redundancy.

The above methods are known as “observation space representation” (OSR) techniques because they use a lump estimation of the observation error.

In contrast, “state space representation” (SSR) techniques listed below focus on estimating the state of the specific error components like satellite clocks and atmospheric delays:

- **Satellite-Based Augmentation Systems** (**SBAS**): Employs a network of reference stations to correct satellite orbits, clocks, and ionospheric errors to provide SoL services. Several SBAS providers have announced plans to incorporate value-added services (e.g. PPP) alongside their core SoL missions discussed in page 12.
- **Precise Point Positioning** (**PPP**): Uses precise satellite orbits and clocks, often provided by services like the International GNSS Service (IGS), to model and estimate residual errors at the receiver level. This enables sub-decimetre accuracy, especially when carrier phase ambiguities are resolved, as in **PPP-AR**. Recent advancements have improved accuracy from 5-10 cm to 2-3 cm, though initial convergence still takes about 10 minutes. **PPP-RTK** integrates local atmospheric corrections alongside global PPP correction data, significantly reducing the initial convergence time. However, this additional data must be sourced from a nearby network of reference stations, which somewhat undermines the global nature of PPP. As a result, service providers must balance the performance enhancements against the additional infrastructure and communication bandwidth required.

Whatever the strategy used, it implies relying on a (network of) reference station(s) and obtaining a solution relative to it. Furthermore, a real-time communication link is required. Finally, all carrier phase-based solutions require an estimation of the ambiguities, and continuous, cycle slip free measurements (thus excluding receiver duty cycling).

A trend observed over the recent past is the provision of high accuracy augmentation services by the operators of the GNSS (Galileo HAS, BeiDou B2b) or SBAS themselves. Nevertheless, such services are still predominantly supplied on a commercial basis, as highlighted by the large number of operators that are listed on the “UseGalileo” internet site.

GNSS assistance

Unlike other augmentation methods described on the left-hand side of this page, GNSS assistance was primarily developed to enable and optimise the use of GNSS in cellular phones. This requires a very fast **Time to First Fix** (**TTFF**) and the use of short signal snapshots while maintaining sufficient sensitivity.

Assisted GNSS (**A-GNSS**) enhances GNSS performance by utilising external data from a separate communications link to support positioning. This technique is especially useful when satellite data is inaccessible or weak. A-GNSS provides information such as satellite positions, user location estimates and timing data, enabling the receiver to quickly achieve a position fix. This reduces the Time to First Fix (TTFF) and enhances performance in challenging environments like urban canyons and indoors. A-GNSS also boosts receiver efficiency and supports high-sensitivity modes for GNSS systems without pilot signals.

Specifically, A-GNSS provides:

- **Acquisition Assistance**: Coarse timing and Doppler data to speed up signal acquisition.
- **Clock and Ephemeris Assistance**: Replaces traditional broadcast navigation messages.

In summary, A-GNSS allows GNSS receivers to achieve faster position fixes with lower energy use by leveraging faster data transmission from cellular networks.

Operational benefits of A-GNSS

The main benefits of GNSS assistance are:

- **Faster Time to First Fix** (**TTFF**): A-GNSS reduces the time required for a GNSS receiver to establish its initial position, especially in challenging environments like urban canyons or indoors, by quickly narrowing down satellite searches.
- **Improved Sensitivity**: A-GNSS enhances the receiver's ability to acquire and track weak satellite signals in difficult conditions, such as inside buildings or under dense foliage.
- **Reduced Power Consumption**: A-GNSS speeds up position fixes and maintains them efficiently, which lowers power use, benefiting battery-operated devices like smartphones and wearables.
- **Enhanced Accuracy and Reliability in Urban Areas**: A-GNSS improves positioning accuracy by correcting satellite clock errors, atmospheric conditions, and signal reflections, which is particularly valuable in urban environments where buildings obstruct or reflect signals. It combines satellite data with other sensors or networks to ensure reliable positioning in conditions with weak or intermittent GNSS signals. This enhancement is crucial for applications like smartphone navigation and ride-sharing services, ensuring precise and timely location information even in challenging urban settings.

Overall, Assisted GNSS offers significant performance improvements over standalone GNSS, particularly in terms of speed, sensitivity, and reliability, making it a valuable technology for a wide range of applications.

Complementary PNT technologies are redefining navigation solutions

Complementary and alternative PNT technologies are increasingly relevant, with some providing full Positioning Navigation and Timing (PNT) and others focusing solely on Positioning and Navigation (PN) or Timing (T). As these technologies develop, it becomes clear that "one size does not fit all": the optimal choice depends on specific use cases and requirements, reflecting the diverse needs of modern applications.

Inertial Measurement Unit (IMU) dead-reckoning uses accelerometers and gyroscopes to estimate a vehicle's position by measuring its speed, direction, and rotation in real-time. When GNSS signals are weak or unavailable, as in case of spoofing and jamming attacks or satellite signal obscuration, IMU dead-reckoning can maintain **continuous navigation** by calculating the position based on previous GNSS data and sensor readings. Though less precise over time due to **drift**, it is an effective method for ensuring uninterrupted navigation in challenging environments.

Visual and Lidar-based navigation combines cameras and Lidar sensors to provide PN. Cameras capture visual data to identify and interpret landmarks and obstacles, while Lidar provides precise distance measurements and 3D mapping. Together, they enable **robust PN** by integrating detailed environmental information with visual context, making them ideal for **connected and automated vehicles** for air, sea surface, underwater, and land, **robotics**, and advanced **mapping applications**. This technology is already established and used practically in all space missions.

Quantum inertial navigation technology leverages quantum sensors to measure motion with extreme precision, providing accurate PN without relying on external GNSS signals. By detecting minute changes in acceleration and rotation, quantum sensors can track position over long periods **without drift**. This makes it highly valuable for applications in environments where conventional GNSS is **unavailable** or **unreliable**, such as submarines, spacecraft, or densely built **urban areas**. The TRL of this technology is currently low, with the expectation to improve in the following years.

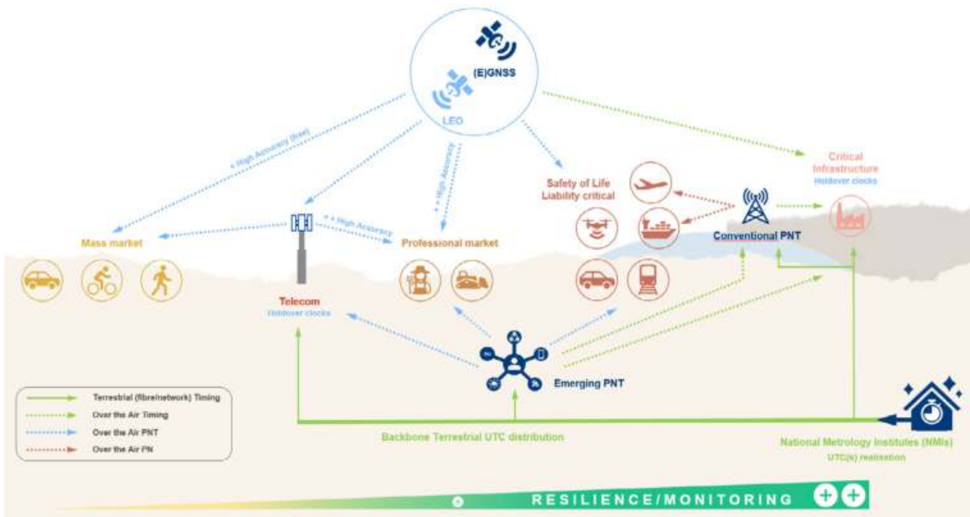
5G positioning can operate both as an alternative or complementary PNT, depending on the application and environment. While it is designed to work alongside GNSS for enhanced accuracy, especially in **urban areas**, 5G can also provide independent positioning using its **wideband signals** and infrastructure, such as base stations and mmWave signals. 5G positioning is in the early stages of widespread adoption, with ongoing advancements needed for higher accuracy and reliability.

The **White Rabbit protocol** is a mature technology which integrates Precision Time Protocol (PTP) packets with the frequency base of Synchronous Ethernet (SyncE) to achieve sub-nanosecond **time transfer**. It requires two-time sources (e.g. GNSS or atomic clocks) for redundancy, delivering 60-90 picosecond accuracy. Initially used in scientific fields like high-energy physics and astronomy, it has been adopted by industries such as telecommunications and finance.

Low Earth Orbit (LEO) PNT systems utilise satellites in low Earth orbit to provide location and timing services. They can serve as a complement or backup to traditional GNSS, potentially offering enhanced signal resilience in urban environments, **better accuracy**, and faster **signal acquisition**. LEO satellites can deliver stronger signals and thus be less vulnerable to jamming or spoofing, making them an option to consider for critical navigation and timing applications. However, LEO requires much larger constellations for full Earth coverage due to their smaller footprint and higher orbital speed compared to traditional GNSS. Another disadvantage is the complexity of the signal acquisition process, which is particularly challenging due to the rapid movement of LEO satellites. LEO for PNT is an emerging technology but is not yet operational, and current receivers are unable to process their signals, nor can they be upgraded to do so.

Resilient Maritime Positioning (R-Mode), which is in early-stage development, is a terrestrial-based backup navigation system designed to provide PN when GNSS signals are compromised, with limited accuracy compared to traditional GNSS. It uses existing **maritime radio** infrastructure (e.g., MF beacons and VHF signals) to calculate position through signal ranging. Primarily aimed at maritime applications, R-Mode enhances **safety** and **reliability**. It is planned to operate in GNSS-denied environments. Currently under development in Europe, it offers a cost-effective, resilient solution for coastal and nearshore navigation.

VISION FOR THE EU PNT ECOSYSTEM CONSISTING OF SPACE (GNSS, LEO) AND EMERGING PNT ASSETS (TIMING, 5G, INERTIAL)



GNSS vulnerabilities and mitigation measures

GNSS disruptions endanger safety of navigation

In recent years, the threat of cyberattacks and GNSS interference has increasingly jeopardised critical infrastructure and transportation systems, particularly in geopolitically tense regions. These incidents expose the vulnerabilities of GNSS-based systems, which are frequent targets in modern hybrid warfare. Regions such as Eastern Europe, the Eastern Mediterranean, the Baltic Sea, and the Arctic have experienced a surge in **GNSS jamming**, disrupting vital operations like aviation and scientific research and raising significant safety concerns.

In addition to jamming, **GNSS spoofing** is emerging as a serious threat across various sectors. Spoofing incidents have disrupted commercial aviation, causing unplanned landings and heightening safety risks. As these threats escalate, the need for robust defences against GNSS interference is more critical than ever.

Affected regions are implementing technological upgrades and countermeasures to safeguard their systems against persistent GNSS jamming and spoofing, which disrupt both military and civilian activities. The increasing frequency of these incidents has raised alarms within the aviation community, leading to urgent calls for international cooperation. For example, the **European Union Aviation Safety Agency** (**EASA**) released a revised Safety Information Bulletin in July 2024 addressing the growing issue of GNSS outages and disruptions, highlighting the increasing sophistication and impact of GNSS jamming and spoofing, which have become significant concerns for aviation safety.

Addressing the jamming and spoofing threats

There is no single solution to completely eliminate these threats, nor a single technology that can address them all. However, a range of mitigation measures can be recommended for competent authorities, critical service providers, equipment manufacturers, and end users:

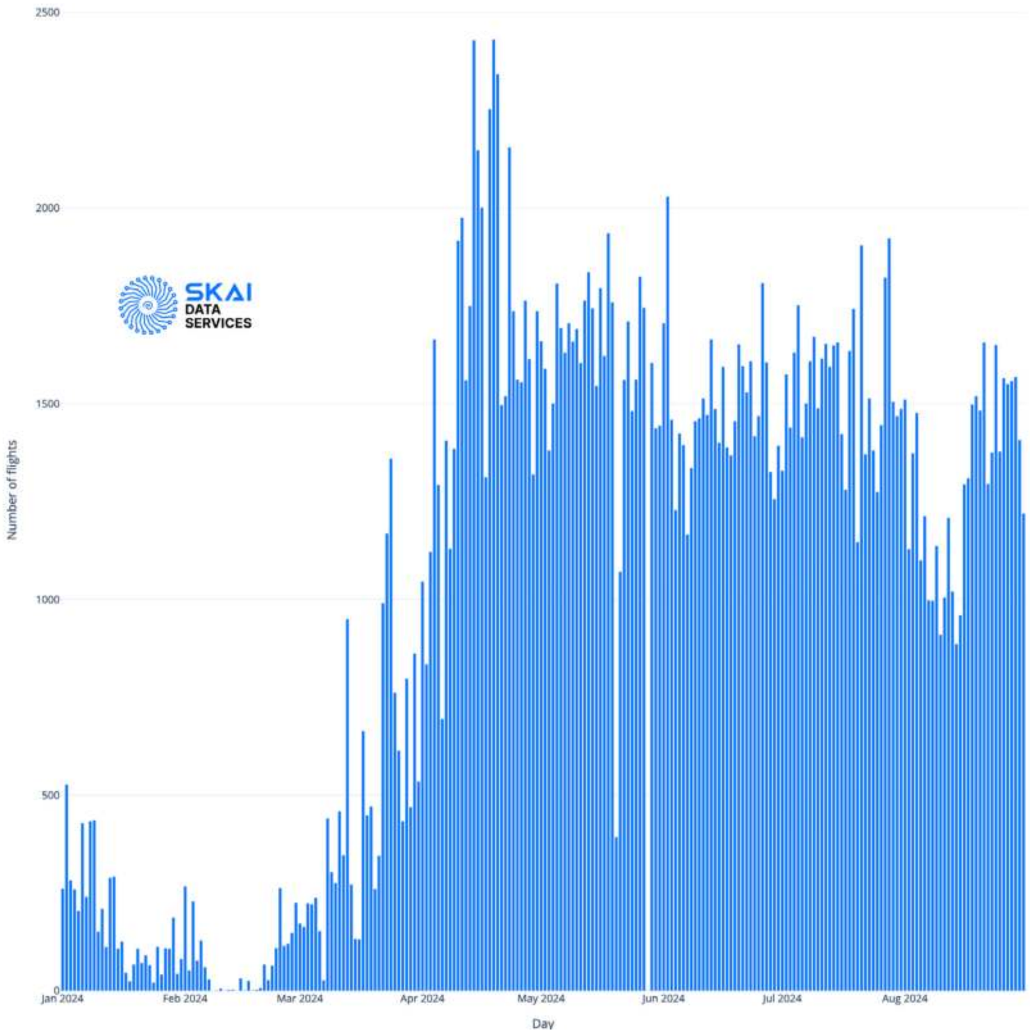
1. Ensuring a clean RF environment:
- Protect GNSS-allocated spectrum by actively monitoring for interference and jamming and prosecute illegal transmitters operating within these bands.
- Ensure that no other electronic equipment at the user or platform level produces unwanted spurious emissions that could interfere with GNSS, and design GNSS equipment to be more robust against such disruptions.

2. Enhancing antennas and setups:
- Invest in better antennas that offer a higher signal-to-noise ratio and improved rejection of unwanted signals.
- Position antennas to avoid multipath effects, ensure clear visibility to the sky, and minimise exposure to potential malevolent actors.

3. Strengthening GNSS:
- Utilise authenticated GNSS and augmentation services whenever available.
- Deploy receivers that implement anti-jamming (A/J) and anti-spoofing (A/S) techniques.

4. Diversifying sources of PNT information:
- Use multiple GNSS constellations, with multi-frequency capability recommended.
- For critical applications, implement alternative (non-GNSS) technologies as a backup to ensure continuous positioning, navigation, and timing (PNT) information.

ESTIMATED DAILY NUMBER OF FLIGHTS AFFECTED BY GNSS SPOOFING



Graph courtesy of SkAI Data Services, based upon data from the OpenSky Network.

The above plot illustrates the daily number of suspected spoofed aircraft GPS positions from January to August 2024 within the OpenSky Network coverage area. According to SkAI Data Services estimates, approximately 99% of the detected events occurred in Eastern Europe and the Middle East.
Please note that not all GPS spoofing activities may be detected, as the service capability is dependent upon ADS-B coverage and the presence of flights in the respective areas. Additionally, the OpenSky Network coverage is not global (see details at opensky-network.org), so some events may not be reported.

Civilian GNSS receivers should be better protected against RFI attacks

GNSS receivers are the frontline defence against jamming and spoofing threats, yet most civilian models are designed for benign conditions and seldom incorporate even basic anti-jamming (A/J) or anti-spoofing (A/S) measures.

Maximising the Potential of GNSS

The widely accepted recommendation to leverage diverse sources of Position, Navigation, and Timing (PNT) information should begin with fully exploiting GNSS capabilities. However, most civilian GNSS receivers fail to take full advantage of available open services, either at the single constellation level or the multi-GNSS level.

For instance, the Galileo Open Service (OS) offers frequency diversity (ranging measurements on E1 and E5) and navigation message diversity (I/NAV and F/NAV). Yet, few receivers can independently acquire these signals and messages, negating the robustness provided by such redundancy.

A similar issue arises with multi-constellation configurations: most receivers follow a sequential acquisition process, starting with GPS L1 C/A before handing over to other constellations or frequency bands. This makes the acquisition of GPS L1 C/A a single point of failure, even in systems designed for multi-GNSS and multi-frequency use.

The recently introduced E5/L5-only receivers are less vulnerable to radio frequency interference (RFI) in the upper L-band than traditional L1-dependent models. Whilst this approach offers some protection against jamming, it remains effective only until the lower L-band is likewise compromised, and merely substitutes one single point of failure for another.

An ideal receiver should support the independent and direct acquisition of any open signal from any system, enabling true redundancy and maximising the resilience of GNSS-based positioning.

Implementing GNSS receiver-based detection and awareness measures

Receiver methods for spoofing detection and signal integrity rely on monitoring signal power or carrier-to-noise density ratio (C/N0), time of arrival (TOA) discrimination, correlator output distribution checks, and consistency checks across different measurements such as ephemeris data, clock offset changes, or code and carrier Doppler.

Signal Quality Monitoring (SQM) techniques, initially developed for detecting multipath and waveform deformation, are also effective in identifying distortions in the correlation function that are typical of spoofing attacks. The main challenge in spoofing detection and rejection is discriminating between genuine signals and unwanted ones, a challenge similar to that of multipath interference, which is why similar techniques are often employed.

Novel approaches to the correlation process, such as the Supercorrelation™[1] claim the capability to separate line of sight (LOS) and non-line of sight (NLOS) signals during the correlation process. This provides multipath mitigation, anti-spoofing, and signal arrival-angle determination. Recent research suggests that Artificial Intelligence (AI) and Machine Learning (ML) can be leveraged to classify signals between LOS, NLOS, multipath, or forged, with a success rate of 75-80% in rejecting unwanted signals.

Many widely available and affordable sensors and technologies can enhance and strengthen a user terminal's PNT (Position, Navigation, and Timing) solution. While location-based services (LBS) platforms like smartphones are equipped with a variety of these sensors, they often do not fully leverage them to improve resilience.

Toughening the user terminal

While GNSS is the primary source of Positioning, Navigation, and Timing (PNT) information for most users, it is not the sole option. Many user terminals are tailored to specific use cases, integrating various GNSS implementations and complementary technologies to enhance robustness. Numerous technologies and sensors can contribute to this robustness, but there's no one-size-fits-all solution. The choice depends on the application or platform. Examples include:

- **Dual Antennas**: Estimate bearing and can detect spoofing when reporting the same position.
- **Controlled Radiation Pattern Antennas (CRPA)**: Available for civilian use albeit with a limited number of elements, provide anti-jamming capabilities.
- **Multi-GNSS and Multi-Frequency**: Adds complexity to jammers and spoofers if they need to cover all signals.
- **Jamming Analysis and Signal Classification via Machine Learning**: Enhances detection and mitigation of interference.
- **GNSS Ranging Authentication**: Should be added in the future to Navigation Message Authentication (NMA) for improved security.
- **Hybridisation with IMUs and Independent Time Sources**: Provide reliable spoofing detection and backup during GNSS signal degradation or loss.

This list, though not exhaustive, highlights key technologies that can make user terminals more resilient in contested environments.

1: Supercorrelation™ is a trademark of Focal Point Positioning Ltd.

Galileo completes its authentication portfolio, other systems to follow

SAS provides PVT authentication

The **Signal Authentication Service** (**SAS**) will provide users with an authenticated Position, Velocity, and Time (PVT) solution through secure ranging and data authentication.

Its concept relies on the Galileo Service Centre (GSC) selecting E6C **Encrypted Code Sequences** (**ECS**) to be transmitted by the Galileo E6C SiS in the future. These ECS are then re-encrypted with yet-undisclosed OSNMA keys, creating **Re-Encrypted Code Sequences** (**RECS**). The RECS are periodically uploaded to a secure public server operated by the GSC.

This additional encryption layer allows the RECS to be published in advance for a specified period (typically up to one week) and downloaded by receivers, **enabling offline operation during this time**.

Shortly after the E6 encrypted sequences (ECS) are broadcast via the Signal-in-Space (SIS), the OSNMA keys are disclosed. This allows the receiver to decrypt the stored RECS and reconstruct the original ECS. The receiver then applies a process known as "a posteriori correlation", where the ECS from the E6C SIS are matched with the decrypted ECS to generate range measurements.

This process, illustrated in the accompanying figure, produces **authenticated range measurements without requiring the receiver to decrypt signals or store secure keys**. Combined with OSNMA-authenticated clock and ephemeris data, these measurements are used to compute an **authenticated PVT solution**.

OSNMA for data authentication

The **Open Service Navigation Message Authentication** (**OSNMA**) is a data authentication function freely available to all Open Service users, allowing them to compute a PVT solution based on authenticated navigation data with minimal impact on overall performance, while OS users not exploiting it are not impacted anyhow. OSNMA enables users to verify that the navigation data received originates from Galileo and has not been altered.

This is achieved by adding authentication-specific data, including message authentication codes (MACs) and keys, to previously reserved fields within the INAV message broadcast on the E1-B signal component. By design, **OSNMA is fully backward-compatible with standard OS receivers**, though only OSNMA-ready receivers can decode these fields and authenticate the Galileo navigation data.

OSNMA test signals have been broadcast since July 2020. Following extensive testing, validation, and lasting nearly three years, OSNMA is planned to be officially launched in 2025.

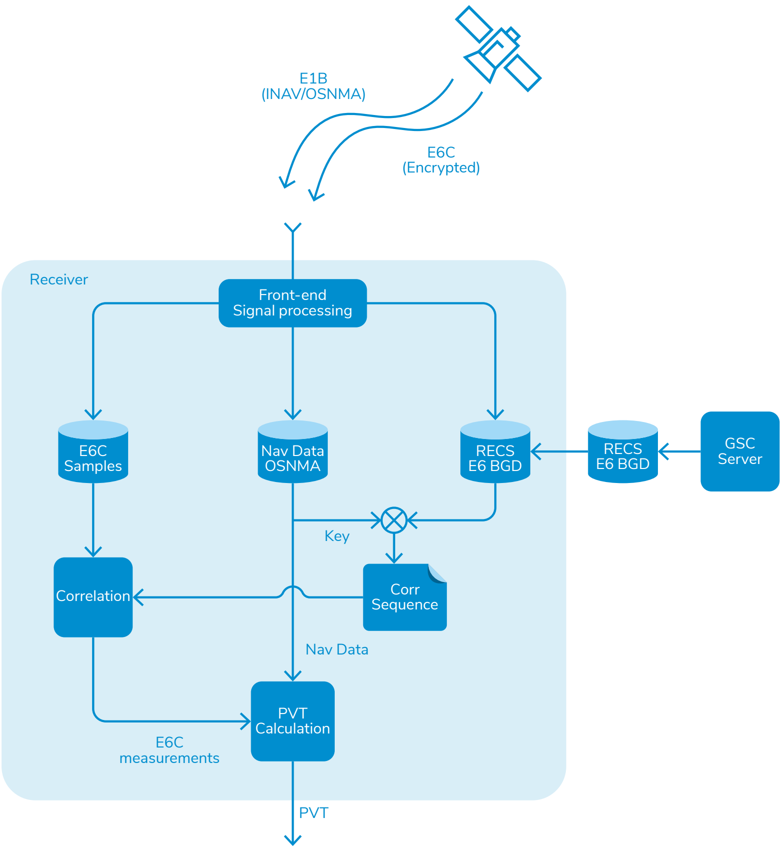
Currently focused on authenticating I/NAV clock and ephemeris data (CED), OSNMA has the capability to authenticate any type of data. This functionality will be leveraged to **support other Galileo services** and functions, such as the **Emergency Warning Satellite Service** (**EWS**) and the remote activation of SAR beacons; and to cross-authenticate **GPS** satellites navigation data.

Other GNSS authentication initiatives

Galileo is a pioneer in authentication, featuring SAS and OSNMA in its first generation, with enhanced capabilities planned for its second generation. However, other Global Navigation Satellite Systems (GNSS) and Regional Navigation Satellite Systems (RNSS) also require greater robustness. Various forms of authentication are already being planned or integrated into these systems and their augmentations, both public and private.

Examples include QZSS Navigation Message Authentication service (**QZNMA**), broadcast by QZSS since April 2024, the NavIC Standard Position Service (**SPS**) Navigation Message Authentication (**NMA**) currently undergoing testing, ongoing **SBAS authentication** studies, GPS's Chips Message Robust Authentication (**CHIMERA**) to be tested on the NTS3 satellite, and the privately operated **SatGuard®** service by Fugro.

SAS HIGH-LEVEL PRINCIPLE OF OPERATION



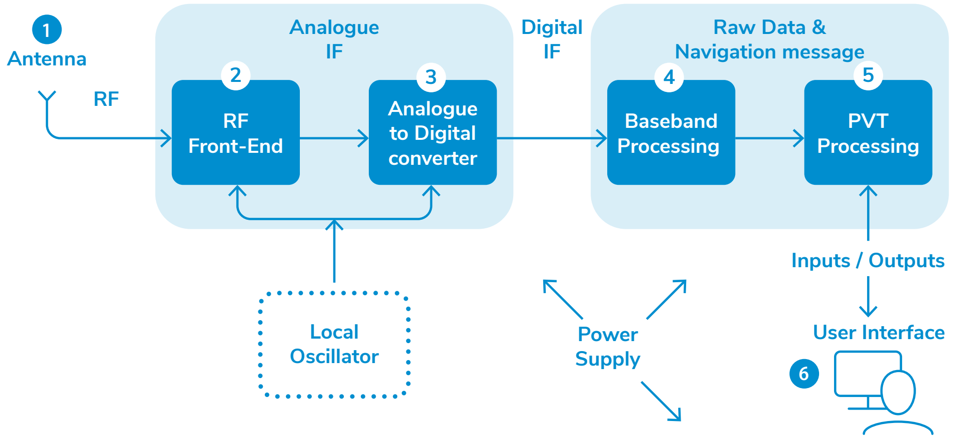
Next-Gen GNSS receivers drive innovation in PNT

Receiver designs have advanced with improved algorithms and semiconductor technology, reducing size and power consumption while enhancing sensitivity and performance. Key innovations include processing multiple channels and frequencies for greater accuracy, reduced multipath effects, and stronger defences against jamming and spoofing.

At the same time, market demands drive the push for higher accuracy, enhanced performance in all conditions, faster time to first fix (TTFF), and greater resistance to jamming or spoofing. This simplified diagram presents the building blocks of a typical GNSS receiver with its dimensions (the most important or rapidly evolving of which are highlighted in red).

This architecture is typical of a self-contained GNSS receiver. The advent of multi-frequency receivers does not significantly affect this functional diagram, but it does impact several components, notably the antenna (1), the RF front-end (2), and the Baseband processing (4) which are (in a gross approximation) replicated for each frequency.

GNSS RECEIVER FUNCTIONAL BLOCK DIAGRAM



1. Antenna (+ preamplifier)

Receives, amplifies and band-pass filters GNSS signals.

Dimensions:

- Frequency band(s)
- Active or passive
- Bandwidth
- Polarisations
- Gain
- CSWaP[1]
- Selectivity
- Noise factor
- Phase Centre
- Multi-Antenna
- (Controlled or fixed) Radiation pattern
- Multipath rejection
- Jamming and Spoofing mitigation

6. Input/ Output interfaces

Converts data produced in internal formats into such recognised formats as NMEA. After reformatting, the data is output over a suitable data interface such as RS-232, Ethernet, Bluetooth or a combination of several. The selection of the interface is often application domain specific.

2. RF down converter

Down-converts and filters RF signals to an intermediate frequency (IF) compatible with analogue-to-digital converter (ADC) acceptable input.

Dimensions:

- Input frequency/ies
- Sensitivity
- Phase noise
- Type (e.g. homodyne, superheterodyne)
- Linearity
- Automatic Gain Control (AGC)
- Isolation

3. Analogue to Digital converter

Converts the analogue IF signal into a digital representation.

Dimensions:

- Linearity
- Number of bits/Dynamic range
- Jitter
- Bandwidth
- Interface to baseband

4. Baseband processing

Acquires and tracks incoming signals, demodulates navigation data.

Dimensions:

- Number of channels
- Signal components processed
- Meta-signal processing
- Measurement rate
- Measurement noise (C/N0)
- Continuous vs. snapshot or duty cycling
- Dynamics
- Multipath mitigation
- Interference and jamming mitigation
- Spoofing mitigation

5. PVT (& Application) processing

Computes the estimated position and receiver time offset relative to the constellation's reference time.

Dimensions:

- Solution type (GNSS, DGNSS, RTK, PPP...)
- Sensor hybridisation
- Authentication
- Cloud processing
- Supported augmentation services
- Single or Multi-constellation
- Update rate
- Latency

1: Cost, Size, Weight and Power

Innovative GNSS receiver architectures are key to meet future PNT demands

The previous page presents a typical legacy architecture, while this one explores innovative architectural approaches that are becoming relevant in the GNSS user receiver market. By examining new solutions, we aim to highlight alternatives to traditional designs, which offer advancements in efficiency, capability and positioning performance.

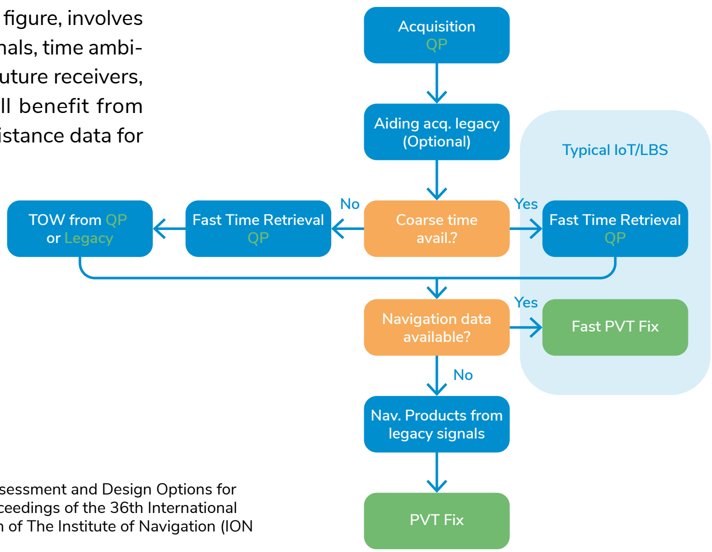
Multi-Antenna architecture

Receiver architectures using multiple antennas enhance positioning by sampling signals across **time** and **space**. Advanced algorithms improve accuracy by minimising errors in line of sight **signal estimation**. **Pre-correlation** techniques mitigate jamming and interference, while post-correlation methods tackle multipath and spoofing. Single and dual-polarisation antenna arrays, along with tensor-based signal processing, further enhance **signal separation** and reduce computational complexity.

Quasi-Pilot based architecture

The upcoming Second Generation of Galileo will introduce **low-complexity** signal components that allow faster acquisition and quicker Time-To-First-Fix (TTFF), reducing **energy consumption** in GNSS receivers. The Quasi-Pilot (QP) signal, with a short 1023-chip primary code, enables rapid Time Ambiguity Resolution (TAR) and supports long coherent integration periods, helping to accelerate TTFF and **lower power usage**. QP aids existing pilot signals and uses a Time Dissemination Scheme (TDS) for fast time ambiguity resolution. The receiver architecture for QP processing, as shown in the figure, involves acquisition, aiding of legacy signals, time ambiguity resolution, and PVT fix. Future receivers, in particular **IOT** and **LBS** will benefit from this by receiving additional assistance data for low-energy PVT solutions.

HIGH-LEVEL ARCHITECTURE FOR QP PROCESSING[1]



1: Source: Galileo Quasi-Pilot Signals: Assessment and Design Options for Acquisition and Time Dissemination, Proceedings of the 36th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2023)

Snapshot architecture

Receivers with snapshot architecture operate **on-demand**, capturing a piece of the signal when requested and estimating the necessary parameters for positioning. The snapshot architecture records a digital copy of a received GNSS signal for a **short duration** (2ms-100ms), compared to the longer recording times (1-10s) of traditional receivers. This digital copy is used to determine signal frequency and code phase, which are then used to calculate the pseudorange. This technique **reduces battery consumption** and simplifies hardware by eliminating the need for continuous GNSS signal tracking. An example of devices implementing snapshot processing are modern smartphones. The QP signals introduced by the 2nd Generation of Galileo will favour this type of architecture.

Cloud based architecture

Cloud-GNSS receivers, which offload data processing to the cloud, significantly reduce **power consumption** compared to traditional local processing. Future **IoT sensors** are expected to be smaller, more efficient, and lower in cost, making cloud-based GNSS systems increasingly attractive. By eliminating the need for local **CPUs** and **ASIC** hardware, cloud-GNSS receivers will be more cost-effective, extending the shift towards highly efficient cloud-based architectures in the coming years.

Hybridisation with 5G/6G

The hybridisation of GNSS and 5G is expected to be the **core of future location engines** for many applications. This will enhance location performance in urban areas, forming the backbone for applications for the **connected and automated vehicles and mobile robots**. 5G is widely adopted, but not yet as a location mean. The 6G technology, currently under development, aims to support advanced applications like **Virtual or Augmented Reality** and pervasive intelligence, achieving centimetre-level positioning accuracy through intelligent reflective surfaces and advanced beamforming. This precision will benefit plenty of use cases like drone delivery, asset tracking, healthcare monitoring, precision agriculture, and the connected and automated vehicles, pushing the boundaries of mobile and positioning technology.

Software defined receivers

Software-defined radio (SDR) in GNSS receivers leverages conventional antenna and frontend hardware while using a platform's **digital processing power** to handle tasks like signal and navigation solution processing, typically managed by dedicated hardware. Although SDR offers greater **flexibility** compared to traditional hardware receivers, it demands more computational resources and **higher power consumption**, limiting its efficiency. As of 2024, despite its potential as a development tool, SDR receivers have not seen widespread market adoption. It remains a niche technology rather than the approach for the majority of the GNSS market, which favours more dedicated and hardware solutions.

Powering the future of GNSS with smarter, smaller sensors and semiconductors

The evolution of GNSS receiver design is enabled by technological developments in the semiconductor industry, as a matter of fact the receiver performance is significantly influenced by the specifics of its various functional elements. Substantial advancements have been made in refining these components, with receivers becoming increasingly miniaturised due to progress in silicon structure miniaturisation down to 7nm for consumer products like smartphones.

Stand-alone sensors

Navigation techniques are divided into two main categories: position fixing and dead reckoning. Position fixing involves determining navigation states relative to known positions, such as using a GNSS system. Dead reckoning, on the other hand, measures the progression of navigation states relative to their initial values. For instance, GNSS needs a line of sight to at least four satellites, which is often impractical in urban or indoor environments. In such **GNSS-denied environments**, dead reckoning, particularly inertial navigation sensors, are used to provide navigation solutions when position fixing is not possible. Modern sensors for navigation typically include:

- **Inertial sensors**: IMUs like accelerometers and gyroscopes are improving with quantum and MEMS/MOEMS technologies, enhancing sensitivity, stability, and reducing drift. Hybrid systems combining various sensor types will further increase accuracy. Inertial sensors have reached a good level of technological maturity, offering enhanced accuracy and reliability in navigation. However, their adoption remains limited to high-end applications due to higher costs, power consumption, and the integration complexity.
- **Quantum magnetometers & gravimetry**: are showing high levels of sensitivity. Their usefulness in navigation will not only depend on cost and power efficiency but also on the complementary map-making activities. As of now, there are no commercially available GNSS receivers that fully integrate quantum magnetometers and gravimetry technology for mainstream market use. These technologies are still in the R&D phase and primarily being explored in specialised scientific fields like geophysics and space research.
- **Imaging systems**: High-resolution stereo cameras and LIDAR can aid navigation, such as interpreting star maps. Quantum techniques are also being developed for hyperspectral imaging and seeing through dispersive media, which could improve visual navigation. This technology is still not common in consumer-grade GNSS receivers but is becoming more prevalent in specialised applications like robotics, surveying, and connected and automated driving. One of the first receivers on the market featuring image aid was the Trimble **Applanix POS LV**, used for precise mapping in the connected and automated vehicles and drones.

Emerging trends in inertial sensors

The advancements described below, still at early stages of TRL, promise more efficient, precise, and adaptable navigation solutions for a variety of applications, particularly in GNSS-denied environments:

- **Nuclear magnetic resonance gyroscopes**: These gyroscopes use quantum spin for precise rotation measurements and are set to achieve high accuracy in dynamic applications within five years.
- **Cold atom sensors**: Laser-cooled atoms will allow quantum-based inertial measurements, providing high signal accuracy and low noise.
- **MOEMS sensors**: Utilising optical pick-off mechanisms, MOEMS will reduce traditional sensor errors, aiming for higher accuracy and low-cost manufacturing.

Low power techniques

Portable, handheld, and battery-powered devices are continuously pushing the boundaries with new features and functionalities to serve modern applications. Enhancing battery life by minimising power consumption is crucial for these products. Low power design encompasses techniques and methodologies aimed at reducing both dynamic and static power. **Dynamic power** includes switching and short-circuit power, while **static power** involves leakage, or current that flows through the transistor when inactive.

Techniques to reduce **power consumption** include clock gating to lower switching activity, multi-voltage partitioning to create several voltage domains, and power gating to partition chips into various power domains that can completely **shut off** certain circuit areas. GNSS receivers with tight power consumption requirements will increasingly integrate this circuit topology to manage power efficiently while maintaining excellent performance.

Future directions in semiconductor technology

The primary trend continues to be semiconductor miniaturisation, in line with Moore's law, which has transformed GNSS receivers from slow, single-correlator devices into advanced systems with massive **parallel correlations** and efficient memory use via the fast Fourier transform. Although memory remains a significant cost and size factor, new mass-market (GNSS receivers widely support dual-frequency and multi-constellation signals, with the gap between mass-market and professional applications narrowing due to innovations like **smartwatches, mHealth, and drones**. Future developments are expected to further integrate triple-frequency receivers into mass-market receivers, driven by ongoing miniaturisation and increased computational and memory needs.

Signal processing innovations: a glimpse into the future of GNSS

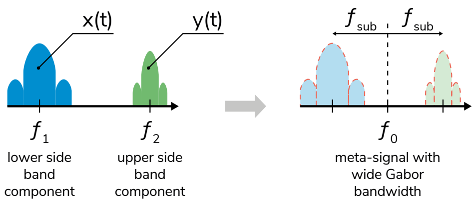
The increasing availability of future GNSS signals is leading to the use of more complex modulations and channel coding schemes. New signal modulations, such as multiplexed BOC signals, CBOC (Galileo E1-B/C), time-multiplexed BOC (GPS L1C), and AltBOC (Galileo E5, BeiDou B2), are increasing receiver complexity. As a result, innovative signal processing techniques are required to achieve exceptional performance for PNT applications, ensuring greater accuracy and reliability in demanding environments.

Meta-signal processing

Modern GNSS systems provide **synchronous signals on multiple frequencies**, which enable improved measurement and signal processing. An interesting innovation is the use of meta-signals, which consist of processing multiple narrow-band GNSS components as a **composite wide-band** signal. This approach leads to better tracking performance and more **accurate code measurements**. An example of a current meta-signal is the combination of Galileo E5a and E5b forming E5 AltBOC. However, this method has challenges: the obtained multi-peaked correlation function can cause biased measurements if the tracking loop locks onto a **secondary peak**.

This issue is exacerbated with greater **frequency separation** between components, necessitating the use of dedicated algorithms and additional correlators to avoid locking onto false peaks. Research has focused on resolving the **meta-signal ambiguity** problem, with techniques such as the Generalised Double Phase Estimator (GDPE), which effectively handles code ambiguity. Other methods like **vector signal processing**, address ambiguities across all signals simultaneously. Meta-signal processing in GNSS receivers is at an early stage, with limited adoption primarily in research applications, though it shows potential for improving signal robustness and accuracy.

TWO GNSS SIGNALS CONSIDERED JOINTLY AS A SINGLE META-SIGNAL



Machine Learning

Machine learning (ML) is transforming GNSS receivers by improving adaptability and accuracy in challenging environments like urban areas with multipath effects or signal obstructions. Unlike traditional GNSS systems, ML allows receivers to learn from signal patterns, predict changes, and adjust accordingly:

- **Dynamic signal processing:** ML algorithms optimise signal processing in real-time, enhancing tracking even in fluctuating conditions, classifying signals between LOS or NLOS and correcting for anomalies like multipath reflections.
- **Noise reduction:** ML filters out noise, improving positioning accuracy and reliability by focusing on useful signal data, especially in noisy environments.
- **Real-time accuracy:** Continuous learning helps refine positioning on the fly, crucial for high-demand applications such as connected and automated vehicles and drones.

Market adoption of Machine Learning in GNSS receivers is still in its initial phase, with increasing interest but limited implementation due to the need for further development and integration into existing systems.

Exploiting Signals of Opportunity

Signals of Opportunity (SOO) are not originally intended for positioning but can be leveraged by modern GNSS receivers to enhance signal processing. An important source of SOO is **Low Earth Orbit** (**LEO**) signals, which are primarily measured through the carrier frequency **Doppler shift**. With numerous satellites in **communication** and **IoT constellations**, LEO signals could play a significant role as complementary source of PNT information.

State-of-the-art LEO receivers measure the doppler shift and signal phase through **acquisition** and **tracking loops**, with a Kalman filter variant often used to process these parameters for adaptable navigation filtering. Despite the maturity for LEO as a SOO for PNT being still very low, the **Novatel OEM7** receiver is capable of processing LEO signals alongside GNSS ones. Over the next 5-10 years, market adoption for specific use cases could increase rapidly. However, the development of receivers exploiting SOO for PNT purposes will have to address several challenges, notably issues of compatibility and interoperability.

Mitigation algorithms

Mitigation algorithms are essential for maintaining **robust and reliable positioning** even when GNSS signals are degraded, obstructed, or partially lost. Traditional GNSS systems can struggle to provide accurate positioning when signals are weak or disrupted, such as in tunnels, mountainous terrain, or deep urban canyons. Resilient algorithms are designed to **mitigate these challenges** and ensure continuous, dependable performance:

- **Fault tolerance**: Resilient algorithms incorporate fault-tolerant techniques that allow the receiver to continue operating effectively, even when the signal quality is compromised. For example, these algorithms can use redundant signals from multiple GNSS constellations (e.g., GPS, Galileo, GLONASS) or integrate non-GNSS data sources (e.g., inertial sensors, barometers, or visual odometry) to maintain accurate positioning when GNSS signals are unreliable.
- **Sensor fusion**: By combining data from different sensors - such as accelerometers, gyroscopes, and cameras - resilient algorithms provide a more comprehensive and stable positioning solution. This sensor fusion allows the receiver to estimate its position based on the movement and orientation data when GNSS signals are obstructed or unavailable, ensuring continuous operation in environments where conventional GNSS alone might fail.
- **Predictive Modelling**: Another key aspect of resilient algorithms is the use of predictive modelling. These models anticipate the receiver's future position based on its current trajectory and movement patterns, allowing for smoother transitions between GNSS signal availability and outage periods. Predictive algorithms can even help bridge brief signal gaps by estimating position with reasonable accuracy until reliable GNSS signals are restored.

The patented **Supercorrelation™** developed by FocalPoint enhances GNSS receiver performance, particularly in environments with dense obstructions like urban canyons. This technique increases the coherent integration period beyond the typical limits of conventional systems, compensating for receiver motion and clock discrepancies to better manage signal distortion. By isolating direct satellite signals from multipath reflections, **Supercorrelation™** delivers **superior accuracy** without the need for hardware changes. Its compatibility with existing GNSS receivers means users can benefit from advanced signal discrimination, improved anti-spoofing measures, and more reliable navigation in complex environments.

Growing adoption of multi-frequency in PNT

MAJOR GNSS PNT COMPUTATION STRATEGIES

Method[1]	SPP	DGNSS	SBAS	RTK	PPP-RTK	PPP
Observable	Code	Code	Code	Carrier	Carrier	Code/Carrier
Positioning	Absolute (in the GNSS reference frame)	Relative	Relative	Relative	Absolute (in the tracking network reference frame)	Absolute (in the tracking network reference frame)
Comm Link	No	Yes	Yes (GNSS like)	Yes	Yes	Yes
Single Frequency (SF) Dual Frequency (DF) Triple Frequency (TF)	SF or DF	SF	SF current DF planned	Mostly DF	(SF) DF or TF	(SF) DF or TF
Time To First Fix (TTFF)	Rx TTFF	As SPP + time to receive corrections	As DGNSS	As DGNSS + time to resolve ambi-guities	Faster than PPP, but slower than RTK	As RTK, but time to estimate ambiguities significantly higher (more unknowns)
Accuracy Horizontal	5-10m DF 15-30m SF	< 1m to < 5m	< 1m	1 cm + 1 ppm baseline	< 10cm	< 10cm to < 1m
Coverage	Worldwide	Up to 100s Km	Up to 1000s Km	Up to 10s Km	Regional	Worldwide

1: Acronyms are defined in Annex 2

Unlocking accuracy: the power of multi-frequency in GNSS

The GNSS sector, having already adopted multi-constellation systems, is now increasingly shifting towards **multi-frequency** capabilities as a key trend. With the growing availability of signals from a larger number of satellites, GNSS receivers in various segments are incorporating multi-frequency functionality to enhance performance, especially in terms of **accuracy** and **interference robustness**. As more open signals in the E5/L5 band become accessible, E5 is progressively being used as the preferred second frequency in newer receiver models, leading to a decline in the adoption of GPS L2.

The new generation of dual-frequency GNSS receivers has seen significant growth in the last few years, particularly in the mass-market receiver families, where they have become increasingly widespread. These advanced receivers offer improved accuracy and resilience to interference by leveraging signals from multiple GNSS frequencies. In addition to consumer devices, they are now actively being developed for more **regulated** and traditionally long lifecycle **market segments** such as aviation, maritime, and rail. These segments require strict compliance with safety and performance standards, and the adoption of dual-frequency GNSS technology promises enhanced PNT accuracy and reliability.

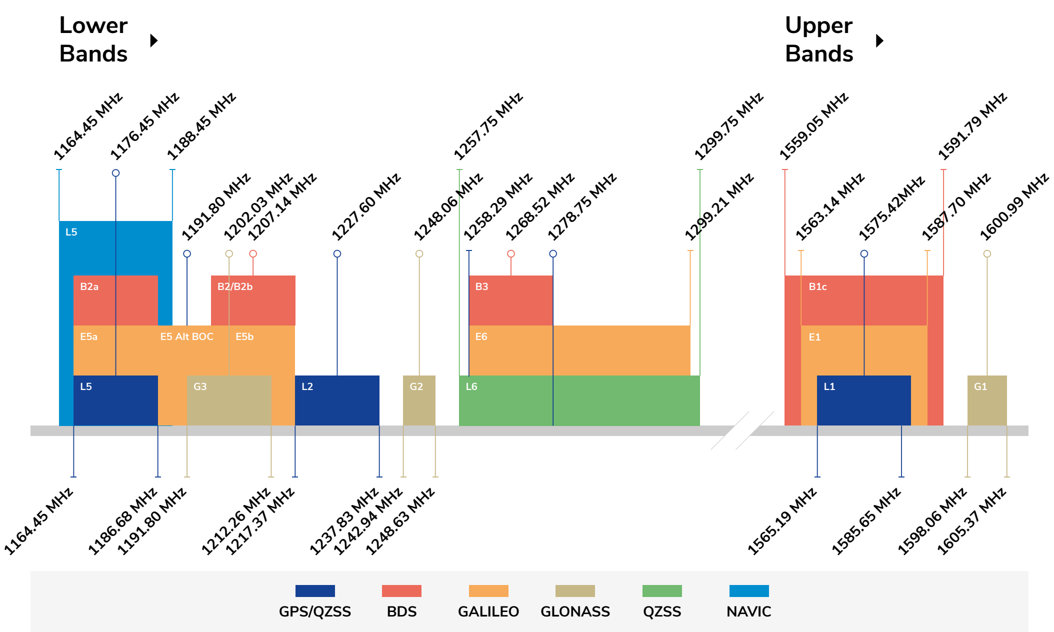
Multi-frequency: redefining receiver standards and performance

Dual-frequency GNSS receivers have become **widely adopted** in the mass-market, offering enhanced accuracy and interference resilience. Despite GPS L5 still being "pre-operational" only, the Galileo E5 frequency band is a key driver of this shift, providing stronger signals, broader satellite coverage, and regulatory protection. **Dual-frequency** processing is now the standard for advanced positioning methods like RTK and PPP, while **triple-frequency** receivers, commonly used in professional applications, further improve PVT reliability and convergence time. Although still more common in high-accuracy sectors, multi-frequency processing is gradually becoming more accessible to mass-market users as technology advances and costs decrease.

Septentrio, Unicorecomm and u-blox were the first among the few to release a triple-frequency low-cost GNSS receiver. The accuracy achieved by these receivers is at the cm to dm level in Real-Time Kinematic (RTK) processing depending on static or kinematic mode.

Most, if not all, of the mass user devices will run on batteries, which implies that they must remain small and lightweight. This will have an impact on the selection of **frequency bands** for future GNSS, as this may affect the design of components and receivers. Tracking two different frequencies will certainly result in higher accuracy and robustness, but also in higher power consumption and (marginally) in size. The implementation of multi-frequency solutions requires a careful trade-off between the two aspects.

GNSS FREQUENCIES AVAILABLE TODAY



Essential PNT processing strategies for everyday applications

GNSS signals and observables for scalable accuracy

GNSS signals consist of three key elements: the **carrier, spreading codes**, and the **data** component. The carrier, composed of sinusoidal electromagnetic waves in the 1100-1600 MHz range, is used for signal modulation and carrier phase ranging. Spreading codes, which are binary sequences generated at 1-10 MHz, help spread the signal spectrum, improving strength and interference immunity while enabling signal's use for various services. The data component, which includes low-frequency streams like satellite clock and ephemeris data, provides essential navigation information.

To compute the PVT solution, either **code** phase or **carrier** phase observables are used to determine the satellite-to-receiver range. The **carrier phase** offers significantly higher accuracy than the code phase, over hundreds of times greater, but is more fragile and involves the complex process of ambiguity resolution. In contrast, the **code phase** is more robust, offering meter-level accuracy without requiring **ambiguity resolution**. For most applications, code-based processing delivers sufficient accuracy, while carrier-based processing is employed for highly precise measurements, achieving centimetre-level accuracy in advanced systems.

ESSENTIAL PNT PROCESSING STRATEGIES OF CURRENT GNSS RECEIVERS

GNSS satellite		Code based		Carrier based		
		DGNSS (OSR)	SBAS (~SSR)	RTK (OSR)	PPP-RTK (SSR)	PPP (SSR)
GLOBAL (system)	SV orbit error	✓	✓	✓	✓	✓
	SV clock error	✓	✓	✓	✓	✓
	SV bias	✓	✓	✓	✓	✓
REGIONAL/LOCAL (propagation)	Ionosphere	✓	✓	✓	✓	✗
	Troposphere	✓	✗	✓	✓	✗
LOCAL (environment & reciever)	Multipath	Scalability		Scalability		
	Receiver errors	Accuracy		Accuracy		
Receiver / user				Convergence time		

Observation errors influenced by various physical factors

Satellite errors are mainly caused by residual errors in the Orbit Determination and Time Synchronisation process in the GNSS ground segment, which predicts the satellite clock and ephemeris data, and some imperfectly known or modelled errors in the satellite electronics and hardware.

Environmental errors are caused by the ionospheric and tropospheric layers through which the signal passes. The ionosphere modifies the electromagnetic wave's propagation speed in a frequency-dependent manner, while the troposphere generates frequency-independent delays.

Local errors are caused by sources that depend on either the measurement conditions (e.g. signal reflection/ multipath and satellite geometry), the quality of the receiver (clock stability, processing noise and hardware biases), the antenna phase centre offset, or variation.

Positioning techniques for error mitigation

GNSS errors are typically mitigated through two modelling approaches: **Observation Space Representation** (**OSR**), which delivers a single composite ranging correction from a nearby reference station, and **State Space Representation** (**SSR**), where different error sources are estimated individually by a network of Continuously Operating Reference Stations (CORS) and transmitted to the receiver. Certain parameters, such as environmental delays in **Precise Point Positioning** (**PPP**), are calculated within the receiver rather than relying on CORS networks. The **PPP-RTK** method is based on SSR and additional tropo/iono/ambiguity corrections, providing scalable accuracy across various user segments, from mass-market to high-precision applications. The growing adoption of high-accuracy mass-market applications, with the Galileo **High Accuracy Service** as a fundamental enabler, underscores the potential for widespread use of PPP-RTK.

Authentication algorithms redefine PNT reliability

GNSS systems are introducing advanced **authentication** features to enhance the security and reliability of navigation. One approach involves encrypting the **navigation message** (**NMA**) or **spreading code** (**SCA**) using public-private key algorithms to ensure signal authenticity. This requires GNSS receivers to store public keys for verification, but also demands additional **memory and processing power**. For instance, spreading code authentication for four satellites necessitates around 200 kB of **extra memory**, which presents challenges for lightweight, battery-operated devices like IoT systems. To address this, some devices may offload computations to cloud systems as previously described.

In addition to traditional methods, **RF fingerprinting** is emerging as a powerful tool in GNSS authentication. By analysing unique characteristics like clock drift and velocity, RF fingerprinting generates distinctive signatures that authenticate the receiver itself, providing a new layer of protection against threats like spoofing and jamming. These innovations in GNSS authentication ultimately offer more secure and resilient navigation solutions for a wide range of applications.

Integrity algorithms

Integrity in GNSS systems ensures the reliability and quality of navigation information, particularly in safety-critical segment like aviation or in road for automated driving. Besides SBAS and IALA DGNSS, **Receiver Autonomous Integrity Monitoring** (**RAIM**) detects satellite faults using redundant information from the GNSS constellation. **Advanced RAIM** (**ARAIM**) extends this by incorporating dual-frequency measurements and multiple GNSS systems, such as GPS and Galileo, to improve integrity and handle various failure modes. The upcoming **Galileo Second Generation** will offer robust **ARAIM capabilities** to address challenges like limited satellite visibility in more complex environments and extending high-integrity navigation to broader applications.

The future of PNT relies on antenna innovation

Antennas are increasingly recognised as crucial in GNSS receiver design across both high-accuracy and mass-market applications. With the rise of multi-frequency and multi-constellation systems, demand for advanced antenna technology is growing. Future trends include adaptive antennas, beamforming, and miniaturised designs for IoT and wearables, along with intelligent antennas that optimise performance dynamically, ensuring improved GNSS accuracy and reliability in diverse environments.

Optimising compact GNSS antennas for modern signals

Antennas are characterised by frequency range, gain, radiation pattern, noise factor, phase centre definition and stability, polarisation, and multipath and interference rejection, as well as size, shape, electromagnetic and environmental constraints.

The performance of GNSS antennas is heavily influenced by their design, with key characteristics often interdependent. For example, antenna's **efficiency** or **gain** is typically linked to the size of its radiating elements. Smaller antennas, like those used in **wearables** and **smartphones**, tend to be less efficient, which can present challenges in environments with difficult reception. To address these constraints, **miniaturisation techniques** and innovative designs, such as folding antenna wires or using high-permittivity dielectrics, help reduce size while maintaining sufficient gain.

However, these methods may reduce the antenna'S-**bandwidth**, limiting its performance in handling modern GNSS signals, which typically feature **wider bandwidth** than older legacy signals. This shift toward broader signaL-bands allows for better filtering of noise but also demands that antennas be optimised for these new requirements, something that older models may struggle to achieve, especially when they were designed with legacy signals in mind. **Next-generation** antenna designs aim to balance these factors, ensuring that compact antennas can still perform well with modern multi-band GNSS systems.

Single-frequency antennas for low-power applications

Patch antennas, which are widespread due to their characteristics, are typically used in mass-market receivers, usually supporting only the L1 band. For low-power applications the number of bands processed by a receiver becomes less important as the energy consumption is more relevant: single-frequency GNSS antennas are still expected to be employed in low-power GNSS receivers. IoT chips can still work in several frequency bands; however, in applications requiring extremely low power consumption, single-frequency signal processing is expected to be common.

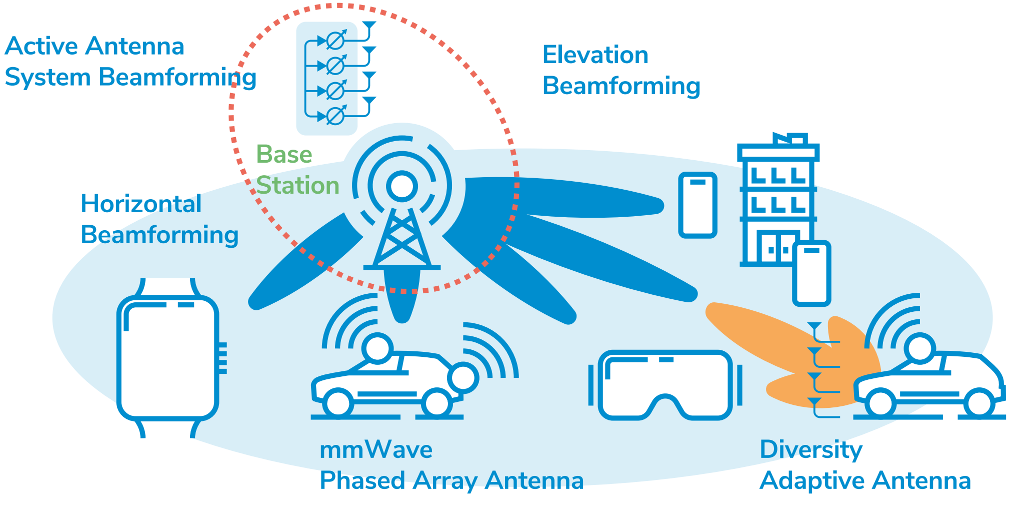
Multi-frequency antennas enabling specific use cases

A trend towards **dual-frequency** in mass-market has been observed with Broadcom launching dual-frequency chipset in 2017, Qualcomm in 2019, and Sony in 2020. In future years, **triple-frequency** antennas could be expected, not only in the professional sectors but also in mass-market receivers without strict power constraints, as the line between mass-market applications and applications requiring high accuracy is becoming blurred.

Adaptive and smart antennas for challenging environments

With the growing demand for high-performance wireless transmission, GNSS antennas are advancing rapidly to meet these needs. Future trends in GNSS antennas point toward the use of **adaptive antennas** with **intelligent learning** techniques. These systems adjust signal strength dynamically to enhance transmission efficiency. Innovations like **diversity** antennas, **phased array** antennas, and **beamforming** are leading the way, leveraging machine learning to optimise performance. For example, the **Controlled Reception Pattern Antenna (CRPA)** is a sophisticated GNSS antenna system that dynamically adjusts its reception pattern to counter interference such as jamming and spoofing, significantly improving signal reliability. While it offers superior performance in challenging environments, its complexity, higher cost, and increased power consumption make it less suitable for low-cost or power-sensitive applications. Antenna developments are expected to play a crucial role in improving the accuracy and reliability of GNSS systems in challenging environments.

THE TOPOLOGY OF THE WIRELESS INFRASTRUCTURE WITH ADAPTIVE ANTENNA AND BEAMFORMING



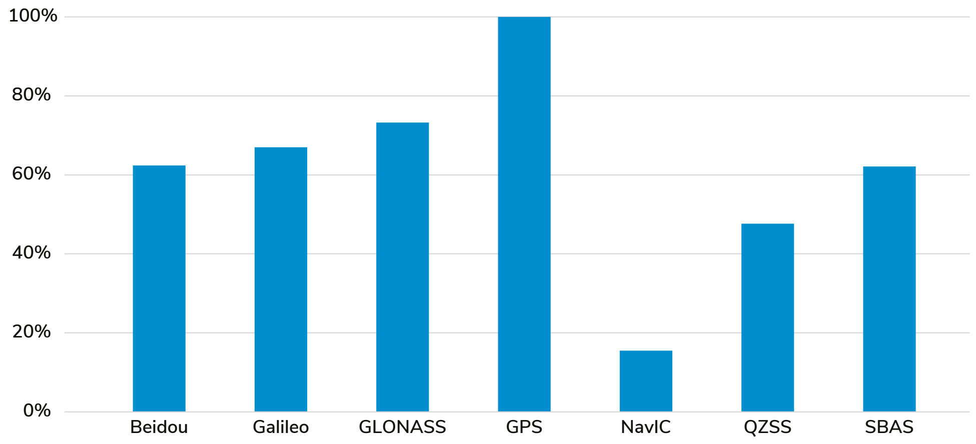
Multi-constellation is the norm in today's receivers

Multi-constellation support is increasing across all receiver families, which are described further on page 31, due to its benefits in improving signal availability, accuracy and resilience against jamming and spoofing. Single-constellation receivers are still used in three main cases because they are cheaper and simpler to design and manufacture: cost-critical, power consumption-critical, and regulated cases. The simplified hardware and reduced processing requirements mean they will remain attractive for use cases where low cost and energy consumption are the primary design considerations.

Nevertheless, more than **75% of device models support multi-constellation**, making it the preferred configuration for most use cases. Since the previous User Technology Report, the proportion of dual and triple constellation receiver models has decreased, while the proportion of receiver **models utilising all constellations has increased to almost 60%**. This trend reflects the growth to full operational capability of BeiDou and Galileo. It is likely nearing a local peak in growth until regulated markets, particularly those that depend on the use of GPS and SBAS move to multi-constellation standards.

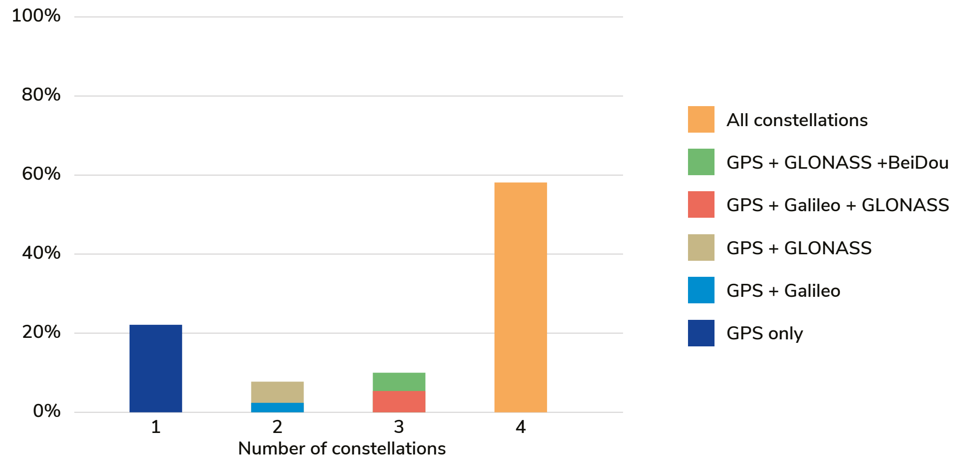
The benefits of multi-constellation support, such as increased robustness, improved availability (particularly in constrained skies, such as urban canyons), and enhanced accuracy (through better geometry offered across solutions obtained), combined with the low cost of entry, mean that **new models** in the future are overwhelmingly **likely to support all constellations**.

CONSTELLATION CAPABILITY OF GNSS RECEIVERS[1]



1: Shows the percentage of receivers capable of tracking each constellation

SUPPORTED CONSTELLATIONS BY GNSS RECEIVERS[2]



2: Shows the percentage of receivers capable of tracking 1, 2, 3 or all 4 global constellations

Analysis of GNSS receivers' capabilities

The EUSPA independent analysis assesses the capabilities of almost 650 receivers, chipsets and modules currently available on the market (end of Q2 2024). For the analysis, each device is weighted equally, regardless of whether it is a chipset or receiver and no matter what its sales volume is. The results should therefore be interpreted as the split of constellations and frequencies supported in manufacturers' offerings, rather than what is in use by end users.

Disclaimer: The above charts reflect manufacturer's publicly available claims regarding their product's capabilities and judgement on the domains to which they are applicable. Use in actual use cases may vary due to issues such as certification, implementation in the end user product, and software/firmware configuration.

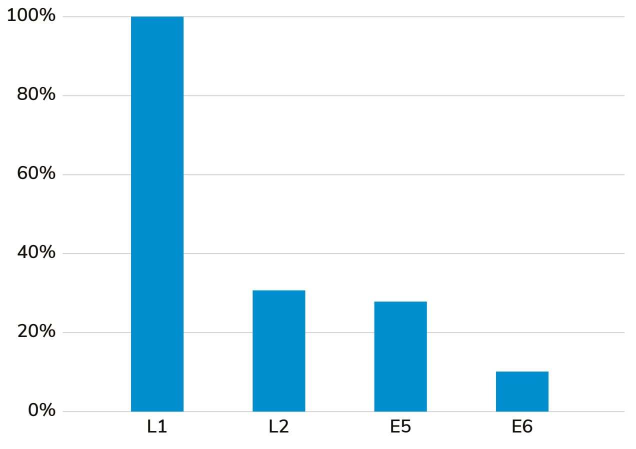
Multi-frequency adoption is being driven by performance demands

The adoption of multi-frequency GNSS receivers is increasing across all sectors, driven by the demand for higher accuracy, better signal reliability, and enhanced positioning capabilities. Consequently, manufacturers are **using additional frequencies to provide maximum availability**. Multi-frequency GNSS receivers are already prominent in the professional non-regulated receiver family, where use cases require multiple frequency bands[1] (L1, L2, E5, E6) to meet performance demands at the application level. This also provides system integrators with the flexibility to choose the best combination of constellations and frequencies for their specific environment.

A **significant portion** of mass-market entry-level devices **still operate on single-frequency (L1)**, which is sufficient for many consumer use cases where high accuracy is not required, and power efficiency is the primary consideration. Mass-market premium devices bridge this gap by progressively offering **dual-frequency support (L1 + E5) in high-end smartphones** and wearables to meet the **extra accuracy demands** and **premium consumer expectations**. This trend has led to an overall increase in dual-frequency models in recent years. However, the additional cost and complexity of triple-frequency models have resulted in stability rather than growth.

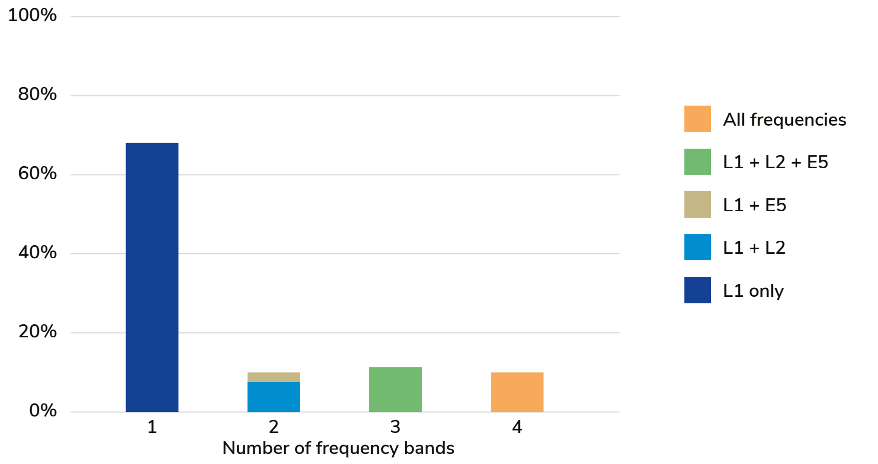
Frequency bands like **E5 and E6** are increasingly utilised to **enhance positioning accuracy** and to provide better **resistance to interference**. Support for these frequencies means that more GNSS receivers are becoming ready to benefit from the Galileo HAS service. The proportion of receiver models supporting E5, which may represent E5a (BPSK), E5b (BPSK), and E5a+b (AltBOC) signal components, or any combination of them, and E6 has grown. This growth has led to **1 in 10 receiver models now supporting all frequencies**.

FREQUENCY CAPABILITY OF GNSS RECEIVERS[2]



2: Shows the percentage of receivers supporting each frequency band

SUPPORTED FREQUENCIES BY GNSS RECEIVERS[3]



3: Shows the percentage of receivers capable of tracking 1, 2, 3 or all the 4 frequencies

Analysis of GNSS receivers' capabilities

The EUSPA independent analysis assesses the capabilities of almost 650 receivers, chipsets and modules currently available on the market (end of Q2 2024). For the analysis, each device is weighted equally, regardless of whether it is a chipset or receiver and no matter what its sales volume is. The results should therefore be interpreted as the split of constellations and frequencies supported in manufacturers' offerings, rather than what is in use by end users.

Disclaimer: The above charts reflect manufacturer's publicly available claims regarding their product's capabilities and judgement on the domains to which they are applicable. Use in actual use cases may vary due to issues such as certification, implementation in the end user product, and software/firmware configuration.

1: For the sake of simplicity, this report uses the name of the first used GNSS frequency in a given band to refer to the full frequency band as described on page 24. For example, "L1" means the [1559,05 - 1605,37] MHz band, which includes GPS L1, Galileo E1, BeiDou B1c and GLONASS G1; and is called "L1" because it was first used by GPS.

EUSPA leading the charge in GNSS R&D

The Fundamental Elements of European GNSS

Fundamental Elements (FE) is an **EU R&D funding mechanism** supporting the development of EGNSS-enabled chipsets, receivers and antennas. The FE projects are part of the overall European GNSS strategy for market uptake, led by EUSPA. The main objectives of the FE are the following:

- Facilitating the **adoption** of the European GNSS Systems, building on their innovative services and differentiators;
- Improving the **competitiveness** of EU industry;
- Addressing user needs in priority market segments;
- Maximising **benefits** to European citizens.

The total budget is € 43 million for all the projects to be carried out from 2021 to 2027. It is already a second phase of the FE; the first phase ran from 2014 to 2020 with a budget of more than **€ 100 million**. The focus of the current phase is:

- User-driven development in all market segments;
- Operational implementation of current differentiators - e.g. OSNMA, HAS, triple-frequency;
- Preparing for **commercial implementation** of new EGNSS differentiators - e.g. EWS, SAS, ARAIM;
- Developing emerging, **disruptive technologies** (e.g. leveraging machine learning, artificial intelligence);
- Exploring synergies with other space systems on user technology - e.g. Copernicus, Secure Communications.

For ongoing calls for proposals within the Fundamental Elements Programme please consult the EUSPA Grants page, for seeing the full list of FE projects, go to FE portfolio page. On the right-hand side are examples of ongoing or finished FE projects.

Complementarity with H2020 and Horizon Europe

Fundamental Elements complements the EU's Horizon 2020 and its successor Horizon Europe research programmes. Horizon Europe, on the one hand, aims to foster adoption of Galileo, EGNOS and Copernicus mostly via **content and application development** and supports the integration of services provided by these programmes into devices and their **commercialisation**. Fundamental Elements, on the other hand, focuses on supporting the development of innovative chipset and receiver technologies that industry would not yet invest in on its own initiative, thus accelerating their integration of Galileo, EGNOS and Copernicus into market-ready devices.

GERMINAL: ENABLING NEXT GENERATION NAV/COM HYBRID TERMINAL

The GERMINAL project lead by GMV, aims at the development of a hybrid user terminal capable to support joint communication & PNT services, reaching TRL 7. From the communication standpoint, the Terminal will support both Terrestrial Network (TN) and Non-Terrestrial Network (NTN) communication signals. From a navigation perspective, the Terminal will be capable of processing standard GNSS signals alongside the Quasi-Pilot signals. It is natural that the LEO-based signals will be explored as well both from communication but also PNT perspective.

More information can be found on the GERMINAL page of the EUSPA website.

OSNMA+

The OSNMA+ project focused on enhancing GNSS-based PVT solutions, particularly using Galileo, to protect against increasing threats from spoofing and jamming. It was aimed at developing a receiver targeting key markets like consumer applications, critical infrastructure, road transport, and drones. The project delivered solutions that bolster security, accuracy, and connectivity for various applications, while also supporting the OSNMA service for smartphones and consumer products without requiring hardware changes.

More information can be found on the OSNMA+ page of the EUSPA website.

GALITS AND TRENI

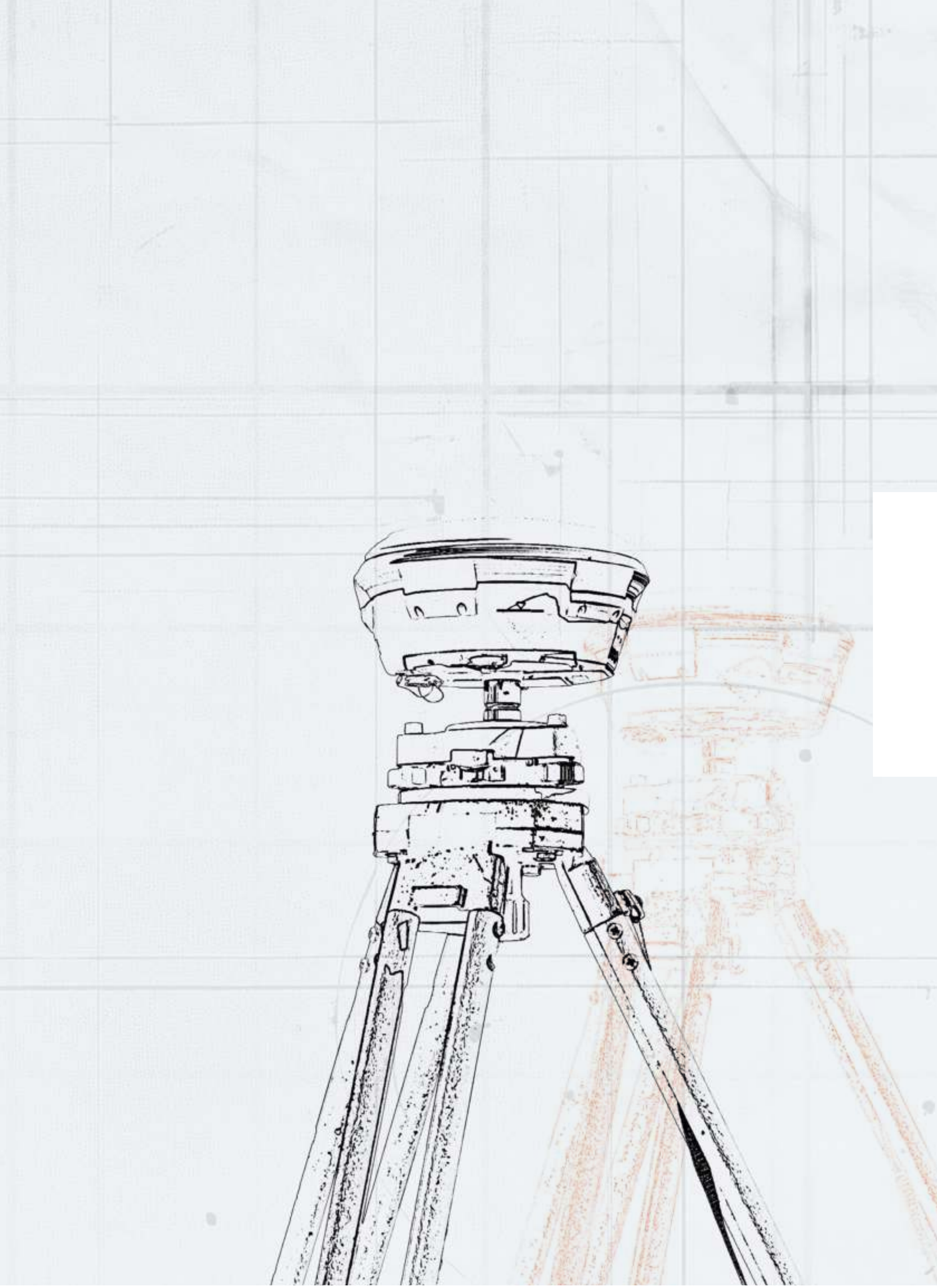
Both GALITS and TRENI projects were focusing on receivers and antennas development for Rail safety relevant applications, aiming to assist the rail stakeholders with potential future integration of GNSS within railway signalling components on board of the trains. GALITS managed by QASCOM and TRENI managed by Thales Alenia Space delivered advanced receivers addressing the PVT-hybridisation and integrity as main elements associated with the complex operational scenarios in railway domain. The antenna development addressed the necessity of compliance with the railway standards and requirements to operate under a high-voltage catenary, as well the possibility to mitigate the negative effects of the electromagnetic field generated within the interaction of the pantograph and catenary on the signal reception.

More information can be found on the GALITS and TRENI pages of the EUSPA website.

PORBEAGLE

The Blue Box Porbeagle project was focused on developing an advanced dual-frequency Vessel Management System (VMS) designed to meet regulatory standards for shipborne equipment and achieve Technology Readiness Level (TRL) 7. This system integrated anti-spoofing cybersecurity technology and improved accuracy, using the EGNSS Galileo Open Service to offer better performance compared to existing solutions. The project aimed to deliver a trusted, close-to-market, cost-effective line-replaceable unit (LRU) capable of decoding PVT information from dual-frequency E1/E5a signals. Additionally, the equipment was able to autonomously authenticate GNSS data messages through the Galileo Open Service Navigation Message Authentication (OSNMA), enhancing security and reliability for vessel monitoring.

More information can be found on the PORBEAGLE page of the EUSPA website.



GNSS RECEIVERS' TECHNOLOGY FAMILIES

Five families of receivers: an evolution and coalescence of capabilities

Issue 1 of the GNSS User Technology Report, published in 2016, grouped GNSS receivers into three macro-segments and noted that GNSS user technology was experiencing a rapid and exciting evolution. Since then, technology has indeed evolved, perhaps most strikingly within the mass-market, where the advances in transistor scaling has allowed manufacturers of high-volume chipsets to include additional GNSS capabilities in more premium devices. New use cases have arisen to take advantage of these evolving capabilities and meet new market demands. The term 'use case' is used here to refer to the way a GNSS receiver may be packaged and utilised in practice, which may come in the form of a type of application, group of applications, a service or GNSS capable device.

We therefore present an analysis and insight into the technological advancements across five families of receivers, each representing chipsets whose characteristics have converged to address groupings of similar requirements, often drawn from diverse use cases in broad markets.

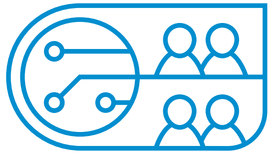
1. Mass-Market Entry-Level receivers focus on those receivers that prioritise battery life or cost over other considerations. A family of GNSS receivers is available to meet these priorities, offering low power consumption, low cost and usually minimal physical size and weight. They achieve this by providing only the **most basic GNSS capabilities**. Typical use cases include low-cost smartphones, wearables, IoT devices, PLBs, entry-level drones and basic automotive navigation devices. These receivers are overwhelmingly found **in consumer devices** and in **very high volumes**.

2. As the Galileo and BeiDou constellations reached their full operational capacity, manufacturers introduced their support, initially in more **premium devices** as a differentiator, for example, claiming **increased availability in urban environments** compared to GPS-only chipsets. Naturally, **multi-frequency capabilities** were introduced into mass-market receivers, with companies like Broadcom, Qualcomm and u-blox all introducing dual-frequency chipsets in 2017 and 2018. Over time, high-volume chipsets offering additional capabilities have emerged as a distinct family of Mass-Market Premium receivers, supporting higher performance characteristics such as accuracy, time to first fix, and robustness. Use cases include premium smartphones and wearables, basic timing solutions, prosumer drone navigation, automotive insurance, and General Aviation navigation, where cost or power consumption are typically less constraining, while **technical differentiators are demanded**.

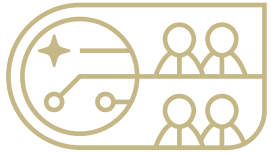
3. Manufacturers historically developed additional capabilities such as **RTK** and **PPP** to achieve the highest levels of performance in terms of accuracy. A family of Professional Non-Regulated receivers, free from power, form factor, and regulatory constraints, exists to **serve professional markets** who can achieve application-level benefits from higher performance. **Multi-constellation** and **multi-frequency** have **become the norm** for this family of receivers and are increasingly taking advantage of additional capabilities such as carrier phase observations, added value messages such as Galileo's **OSNMA** and **HAS** to maximise performance. End user devices within these use cases can often be specialised through coupling with other sensors, while the underlying GNSS capability takes advantage of all signals available. Use cases include geomatics, surveying (land, marine or drone mounted), precision agriculture and forestry, machine control and construction and high-end timing solutions.

4. Professional Regulated receivers serve **safety-critical sectors** such as aviation, maritime, and rail. Manufacturers operate under strict **internationally agreed regulatory standards**, which typically mandate exceptional reliability and integrity above other considerations. **Innovation** in such devices is **constrained** by the timescales of regulatory standards, development, and adoption, combined with rigorous testing and validation requirements. This results in a very distinct class of receivers whose design is more **market-led rather than technology-driven**, and they are thus entirely separate from other families of receivers. Use cases include aviation and maritime safety-of-life services, automotive regulatory and insurance, as well as safety-critical rail.

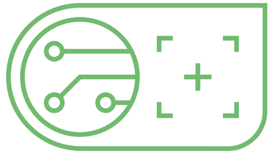
5. Due to the nature of special use cases and applications, devices in this Special Applications receiver family are designed to meet **unique operational demands at the application level**. Sometimes this can be achieved with a custom design built around an off-the-shelf GNSS receiver, but it will more likely require new algorithms and the ability to monitor the entire spectrum of constellations and frequencies. The nature of these **use cases demands specialist equipment**, of which the receiver forms only a central part. In each case, the focus is on state-of-the-art solutions capable of meeting the most demanding applications. This might mean, for example, building a high-bandwidth receiver capable of capturing the full spectrum band and utilising software-defined radios that can be configured to turn on or off capabilities as required by the special application. Use cases include, among others, spaceborne navigation and guidance, or continuously operating reference stations (CORS).



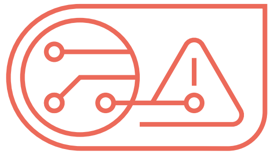
MASS-MARKET ENTRY LEVEL



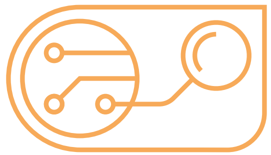
MASS-MARKET PREMIUM



PROFESSIONAL NON-REGULATED



PROFESSIONAL REGULATED



SPECIAL APPLICATIONS

Mass-market entry-level receiver family

Characterisation of receiver family

The mass-market entry-level family encompasses devices designed to provide **basic positioning** and **timing information** across a wide variety of use cases. These devices share common features and levels of performance offering essential functionality at an **affordable cost**. Since the requirements across these use cases are similar, entry-level receivers can be deployed with **minimal customisation** or variation. Typical use cases include:

- **Consumer Solutions**: low-cost smartphones, tablets, and wearables;
- **Internet of Things (IoT)**: battery operated devices requiring low power consumption with infrequent use;
- **Tracking devices**: examples include those used on wildlife, pets, containers, etc.;
- **Personal Locator Beacons (PLBs)**: devices requiring low power consumption and low accuracy;
- **Drones**: basic navigation features like return-to-home for low-cost consumer/hobby drones.

In all these cases, the emphasis is on providing a **highly available positioning solution**, designated for entry-level products. These products are often produced in large volumes, where even small cost reductions from simpler designs are prioritised over the benefits of additional GNSS capabilities.

Industrial landscape

This family is highly competitive, with multiple key players continuing to dominate the market, similar to previous years. Broadcom, MediaTek, Qualcomm and HiSilicon (Huawei) lead the consumer solutions chipset market, which includes smartphones, tablets and wearables. Manufacturers such as u-blox and STMicroelectronics specialise in GNSS solutions for wearables and tracking devices, focusing on power efficiency and compact designs.

EXAMPLES OF REPRESENTATIVE COMPONENT MANUFACTURERS[1]

ACR ELECTRONICS INC	North America	acrartex.com
BEIJING UNISTRONG	Asia-Pacific	unistrong.com
BROADCOM	North America	broadcom.com
HISILICON (HUAWEI)	Asia-Pacific	hisilicon.com
MEDIATEK	Asia-Pacific	mediatek.com
NAVICO (BRUNSWICK CORPORATION)	Europe	navico.com
QUALCOMM	North America	qualcomm.com
QUECTEL	Asia-Pacific	quectel.com
QUALINX	Europe	qualinx.io
SAFRAN	Europe	safran-navigation-timing.com
SONY	Asia-Pacific	sony-semicon.com
STMICROELECTRONICS	Europe	st.com
u-blox	Europe	u-blox.ch

1: The list is not exhaustive; its purpose is to illustrate the receiver family with typical component manufacturers. Also, the list does not include system and terminal integrators, and therefore some key industry players may not appear in the list. For more detailed list of component, receiver and system manufacturers, refer to value chain pages in EUSPA EO and GNSS Market Report, issue 2.

Key performance parameters of receiver family

This receiver family places the **highest priority on position availability**, the ability to provide a GNSS position fix at any point in time, on demand. The accuracy and integrity of this position is not as critical, which allows for decisions in the system design that ensure a position can be **provided as quickly as possible**. A coarse position of sub-10m is generally deemed sufficient and ensuring that this can be provided at any moment may lead to the GNSS receivers being integrated in parallel with other positioning solutions that are able to maintain position information indoors.

All the receivers must be able to withstand constant use in an outdoor environment with operating periods ranging from several days to multiple years. Given their portability, this means minimal power consumption is a critical factor. Often indoor positioning through complementary technologies, such as Wi-Fi positioning, are more efficient when compared to the increased cost, size, weight and power consumption that would be demanded if a higher performance GNSS antenna were used instead. In some use cases, receivers are size limited and a larger antenna would not be a solution – such as GNSS devices integrated into a System-On-Chip (SoC).

For PLBs, **low idle power consumption** and **longevity** are equally essential, as the device needs to operate for extended periods both in standby and active modes. Here, the ability to reduce energy consumption through effective power management strategies is vital.

The push for reduced power consumption permeates the GNSS component designs, specifically in relation to how the GNSS navigation messages are acquired. Use cases such as trackers will **only acquire GNSS position when needed**, sacrificing TTFF, while consumer solutions will use more energy efficient data connectivity to achieve a faster TTFF on demand.

Key Performance Parameter (KPP)[2]	Mass- Market Entry-Level Rx Family
Availability	★★★
Accuracy	★☆☆
Continuity	★★☆
Integrity	★☆☆
Robustness	★★☆
Indoor penetration	★☆☆
Time-To-First-Fix (TTFF)	★★☆
Latency	★☆☆
Power consumption	★★★

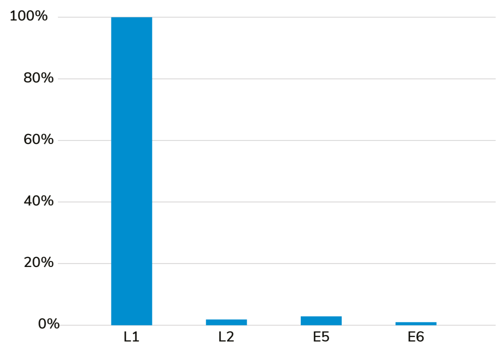
★★★ High priority ★★☆ Medium priority ★☆☆ Low priority

2: The Key Performance Parameters are defined in Annex 1

Entry-level devices remain dependent on single-frequency

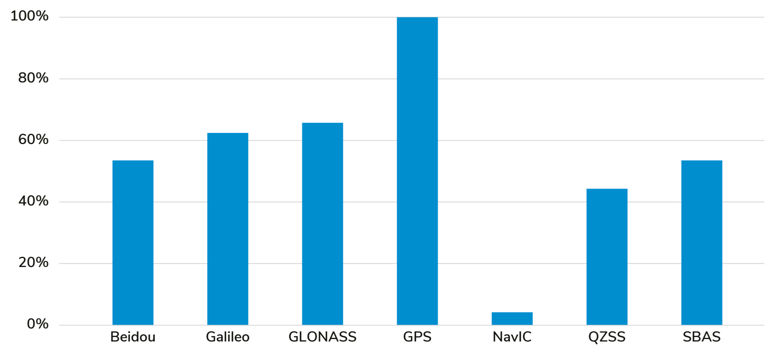
As technology improves, there is a **growing trend for multi-GNSS support**, even in affordable, entry-level devices. As use cases only require basic positioning information, manufacturers can rely on **simple GNSS chipsets**, without the need to incorporate other GNSS services, or record detailed observables for post processing. **Single-frequency** remains the norm as it **minimises cost**, reduces power consumption, whilst still meeting demanded performance.

FREQUENCY CAPABILITY OF GNSS RECEIVERS[1]



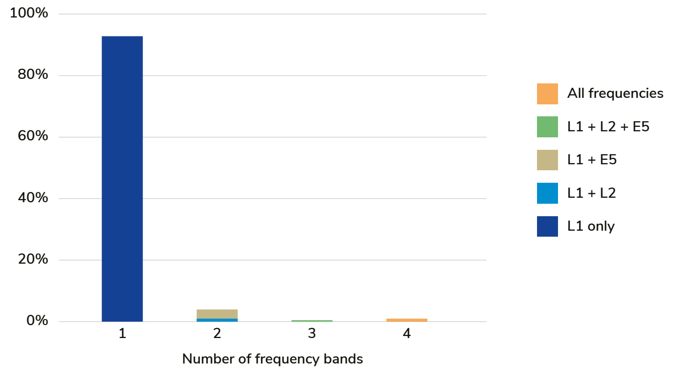
1: Shows the percentage of receivers supporting each frequency band

CONSTELLATION CAPABILITY OF GNSS RECEIVERS[2]



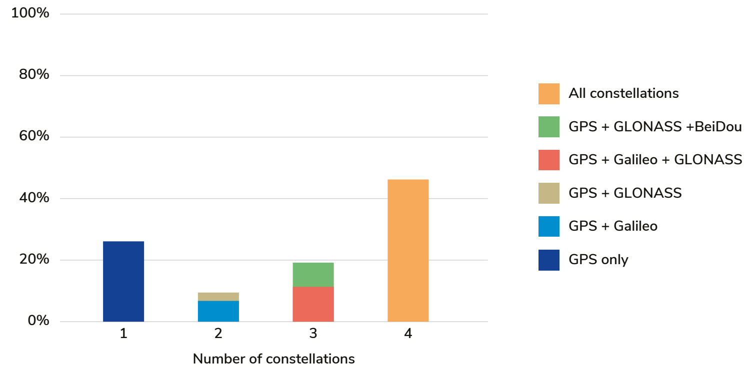
2: Shows the percentage of receivers capable of tracking each constellation

SUPPORTED FREQUENCIES BY GNSS RECEIVERS[3]



3: Shows the percentage of receivers capable of tracking 1, 2, 3 or all the 4 frequencies

SUPPORTED CONSTELLATIONS BY GNSS RECEIVERS[4]



4: Shows the percentage of receivers capable of tracking 1, 2, 3 or all 4 global constellations

Disclaimer: The above charts reflect manufacturer's publicly available claims regarding their product's capabilities and judgement on the domains to which they are applicable. Use in actual use cases may vary due to issues such as certification, implementation in the end user product, and software/firmware configuration.

More than **90% of devices support L1 frequency only**, reflecting the simple and cost driven approach typical of these receivers. This frequency has been in use since the introduction of the L1 C/A GPS legacy signal, and all subsequent constellations also operating in thiS-band. The relatively straightforward processing of the L1 signal and the reduced computational power required make them particularly advantageous for use cases that demand basic positioning. **Advanced processing techniques are unnecessary**, as code-based positioning with a single-frequency delivers sufficient performance. Consequently, carrier phase measurements are **not typically used**.

Even within L1 only, more than **45% of devices support** either all constellations or **at least one constellation and SBAS**. The more complex signals of Galileo, BeiDou and GPS III require additional front-end capabilities and processing, which deliver performance not needed in this family. Often, the capability to support the constellation at the application level is left to the system integrator, potentially utilising SoC controls to determine whether one or more constellation are decoded – and which are prioritised.

Given this complexity of integrating multi-frequency support on SoCs, there remains **limited support for the additional frequency bands** now utilised across the core constellations on which additional services are being provided.

Devices in this receiver family implement a variety of power management strategies to **maximise battery life**. At the GNSS component level, this means **avoiding continuous processing** of the navigation messages through the use of techniques such as A-GNSS or Long-Term Ephemeris depending on the design and usage of the device. Consequently, there is little compatibility with other GNSS functions or services such as OSNMA or EWS.

Minimal size and power use typify the mass-market entry-level receiver family

TYPICAL STATE-OF-THE-ART RECEIVER SPECIFICATIONS FOR THE MASS-MARKET ENTRY-LEVEL RECEIVER FAMILY

	Consumer Solutions chip	Hobby Drone chip	IoT chip
Dimensions	5 x 5 x 1mm	25 x 25 x 2mm	4 x 4 x 1mm
Weight	0.1g	8g	0.1g
Constellations	GPS, GLONASS, Galileo, BeiDou	GPS, GLONASS, Galileo, BeiDou	GPS, GLONASS, Galileo, BeiDou
Frequencies	L1	L1	L1
Power	6mW	120mW	6mW
Number of channels	48	72	66
Update rate	5 - 10Hz	10 - 25Hz	2 – 10Hz
TTFF	<30s (Cold start) <2s (Hot start)	<30s (Cold start) <2s (Hot start)	<30s (Cold start) <2s (Hot start)
Horizontal accuracy (95%)	GNSS 5 - 10m	GNSS 5m	GNSS 2m
Vertical accuracy	-	-	-
Velocity accuracy	0.05m/s	0.05m/s	0.05m/s
Timing accuracy (RMS)	30ns	30ns	30ns

Disclaimer: The above specifications represent a typical chip/SoC package or module based on manufacturer's published literature for their latest products. Consequently, discrepancies may exist between the installed receiver's characteristics and those stated above.

REMOT

The REMOT project by Stonex, funded by EUSPA, aimed to create a wearable device using a fusion between GNSS and IMU (Inertial Measurement Unit). The GNSS provides accurate real-time positioning data, while the IMU captures continuous motion parameters such as acceleration and angular velocity. Fusing these systems allowed the REMOT device to track human movement, more specifically gait, with a higher accuracy, even in environments where GNSS signals are disrupted, to enable kinematic analysis for sports and rehabilitation.

More information can be found on the REMOT page of the EUSPA website.

Typical Specifications

Technological advancements, particularly the transition to sub-10nm manufacturing nodes, have enhanced the **power** and **energy efficiency** of GNSS chipsets. The **affordability** of these advanced nodes has enabled manufacturers to integrate higher-performing GNSS receivers into entry-level products without significantly increasing expenses, while primarily **focusing on single-frequency** solutions.

Despite their core performance similarities, entry-level devices differ significantly among manufacturers and use cases, particularly regarding performance and accuracy, which depend on the power applied and the processing techniques deployed at the integration level. The example devices presented here are representative of the entry-level products, where integration with other devices may be a consideration. This is evident in the size and power requirements of the various chipsets, as some devices may be deployed to provide basic PNT being updated less frequently and remaining in a suspended state for much of their operation.

This family is driven by the widespread adoption of integrated chipsets combining GNSS receivers with various functionalities, including communication capabilities and sensor integration, all within a single package. Consumer expectations from **consumer solutions prioritise fast positioning**; therefore, high availability is crucial to providing position information as quickly as possible. The receiver may not always be powered on and might simply maintain an almanac without actively solving for position. However, it is designed to compute positions rapidly when needed.

Depending on the specific use cases, the power consumption optimisations in these devices enable them to **operate for extended periods** of time – often **exceeding ten years** when configured for specific update rates. The architecture into which these devices are integrated is becoming increasingly complex, typically involving a multi-layered system stack that combines GNSS position with other data sources in application-level algorithms. Core functionality of these devices is often enhanced by cloud-based services, which improve positioning accuracy through A-GNSS and differential correction services. This approach allows for more complex calculations without overburdening the device's local processor, thereby increasing availability and enhancing reliability.

In addition to performance variations, entry-level devices also differ in their technology usage, with some use cases beginning to **shift towards mass-market premium** receiver family. While consumer solutions typically employ single-frequency receivers to provide approximate positions, a **small minority** are starting to explore **dual-frequency** capabilities to reduce ionospheric delays and enhance accuracy.

Hobby drones demand optimised costs on all components, including the GNSS module, which is used to provide basic capabilities such as returning the drone to "home" – its approximate launch site. The moderately increased power consumption of hobby drone chips in comparison to consumer solution devices is driven by the need for reliable performance which is much more important, coupled with increased update rates.

Mass-market entry-level family sample products

Qualinx - QLX300+

The Qualinx QLX300+ chip is an ultra-low power, fully-integrated multi-GNSS single band (L1) GNSS receiver supporting GPS/QZSS/SBAS, Galileo, GLONASS, and BeiDou navigation satellite signals. Regarded as one of the world's lowest power and smallest GNSS chip, it empowers users to lengthen battery life in their products, utilising either Zinc-air or single-call batteries.

qualinx.io

Sony - CXD5642GF

The Sony CXD5642GF chip delivers one of the industry's lowest power consumption for single-band positioning, extending the operating time of IoT, mHealth and wearable products that use GNSS.

info.sony-semicon.com

Quectel - LC76G

LC76G is a multi-GNSS, single-frequency module for GPS, GLONASS, BDS, Galileo and QZSS, ensuring fast and accurate fixes in any environment. Thanks to a proprietary technology dubbed GLP (GNSS Low Power), the LC76G can adaptively adjust the on/off time based on the environmental and motion conditions to achieve a balance between the positioning accuracy and power consumption.

www.quectel.com

Hisilicon - Hi2871V100

Hi2871V100 is a Multi-GNSS (GPS, BDS, GLONASS, Galileo, and QZSS) single-frequency positioning chip designed for trackers, wearables, time serving devices, smartphones, and tablets. It provides intelligent anti-interference and it is specifically optimised to work properly even in harsh environments.

www.hisilicon.com

MediaTek - Dimensity 7200

Dimensity 7200 is a System-on-a-Chip built using a 4nm manufacturing technique. Designed to serve the mid-range market of 5G smartphones, its positioning feature allow to track multiple GNSS such as: GPS, BeiDou, GLONASS, Galileo, QZSS and NavIC signals.

i.mediatek.com

STMicroelectronics - STA8089FG

STA8089FG belongs to the Teseo III receivers' family and is an industrial grade single-frequency standalone positioning receiver IC working on multiple constellations (GPS/Galileo/GLONASS/BeiDou/QZSS).

www.st.com

The mention of specific companies or manufacturers' products on this page is for informational purposes only and does not constitute endorsement, preference or recommendation by EUSPA. These references are intended solely to illustrate the relevant receiver categories (families), highlighting those that have recently been introduced to the market.

Mass-market premium receiver family

Characterisation of receiver family

This family's devices are distinguished by the inclusion of **additional features once reserved for professional use cases**, with a heightened **emphasis** on **multi-constellation** and **multi-frequency** support. These receivers tend to prioritise continuous operation and the ability to access raw data, enabling the potential use of **enhanced features**. Devices are typically employed in use cases that benefit from advanced capabilities, including:

- **Consumer solutions**: high-end smartphones, tablets and wearables, alongside premium PNDs used in recreational activities, where GNSS capabilities often serve as a product differentiator compared to entry-level models;
- **General Aviation (GA) non-certified**: navigation and situational awareness devices that share location with other airspace users;
- **Non-safety critical transport**: examples include rail passenger information systems;
- **Automotive**: premium navigation and smart mobility use cases that benefit from increased robustness and accuracy;
- **Infrastructure**: devices utilised in lower accuracy timing applications such as basic network operations, smart grids, telecommunications, transport infrastructure and financial record time-stamping.

These use cases demand higher levels of accuracy, availability, and robustness compared to entry-level mass-market devices. Core GNSS receiver specifications, such as supported constellations and frequencies, are now often recognised by end users and serve as key product differentiators.

EXAMPLES OF REPRESENTATIVE COMPONENT MANUFACTURERS[1]

AIROHA (MEDIATEK)	Asia-Pacific	airoha.com
ALLYSTAR (CEC)	Asia-Pacific	allystar.com
BROADCOM	North America	broadcom.com
FURUNO	Asia-Pacific	furuno.com
HISILICON (HUAWEI)	Asia-Pacific	hisilicon.com
MEDIATEK	Asia-Pacific	mediatek.com
MEINBERG	Europe	meinbergglobal.com
ONENAV	North America	onenav.ai
QUALCOMM	North America	qualcomm.com
SAMSUNG	Asia-Pacific	samsung.com
u-blox	Europe	u-blox.ch

1: The list is not exhaustive, its purpose is to illustrate the receiver family with typical component manufacturers. Also, the list does not include system and terminal integrators, and therefore some key industry may not appear in the list. For more detailed list of component, receiver and system manufacturers, refer to value chain pages in EUSPA EO and GNSS Market Report, issue 2.

Industrial landscape

This family generally comprises receivers that bring enhanced features from professional-grade devices to more widespread use cases. These devices are manufactured by companies that also target the mass-market entry-level but offer a 'premium' device that leverages additional computing power to deliver enhanced performance. This market is dominated by companies like u-blox, Mediatek, and Qualcomm.

Key performance parameters of receiver family

Availability is demanded across all use cases supported. Devices focus on **improved performance** over entry-level counterparts due to application requirements and the environments in which they are used. There is **less emphasis on cost** and more attention on overall performance, **prioritising accuracy and availability** to support their use cases.

The focus is on improving GNSS capabilities as a means to enhance service quality and user experience, prioritising accuracy, availability and robustness compared to entry-level products. Meanwhile, power requirements may be more relaxed, as devices can be components in larger products with bigger batteries or permanent power supplies, for example in automotive use cases.

In some use cases, such as general aviation, the driving KPPs are signal availability, integrity, and **robustness against external interference**, as the end user may be relying upon the device to help them navigate.

High-end consumer solutions typically come with **increased processing capabilities**. This allows the GNSS component to compute solutions from more channels (meaning both more constellations and frequencies) compared to entry-level devices, fulfilling the priority needs of accuracy, continuity and robustness. Enhanced computationaL-bandwidth and increased power budget support faster TTFF through **continuous signal processing**.

Key Performance Parameter (KPP)[2]	Mass-Market Premium Rx Family
Availability	★★★
Accuracy	★★☆
Continuity	★★☆
Integrity	★★☆
Robustness	★★☆
Indoor penetration	★★☆
Time-To-First-Fix (TTFF)	★★★
Latency	★★☆
Power consumption	★★☆

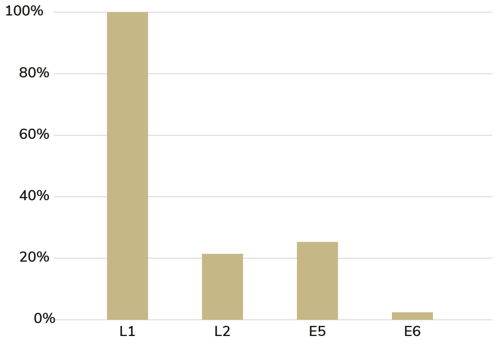
★★★ High priority ★★☆ Medium priority ★☆☆ Low priority

2: The Key Performance Parameters are defined in Annex 1

Premium devices are embracing multi-frequency support

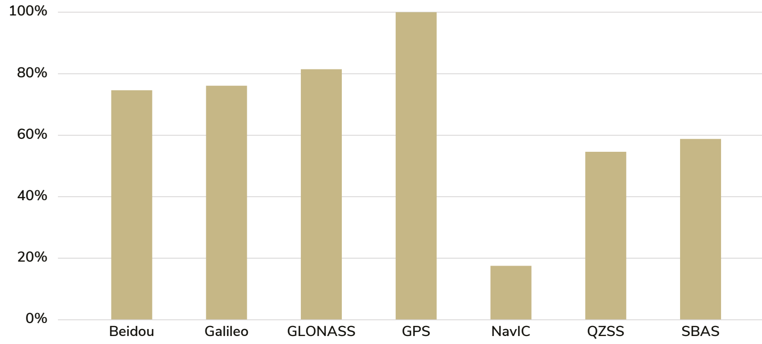
Alongside greater adoption of multi-constellation systems, mass-market premium devices are **beginning to increase their frequency capabilities**. Many premium smartphones and wearables are now moving towards **dual-frequency support**, with the second frequency shifting from the legacy L2 band to the more advanced E5 band. This transition is driven by the fact that E5 is present on **more satellites** and **offers better performance**, including higher signal levels and greater bandwidth.

FREQUENCY CAPABILITY OF GNSS RECEIVERS[1]



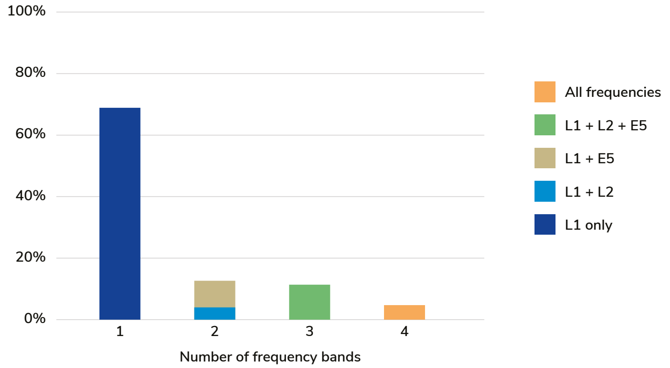
[1] Shows the percentage of receivers supporting each frequency band

CONSTELLATION CAPABILITY OF GNSS RECEIVERS[2]



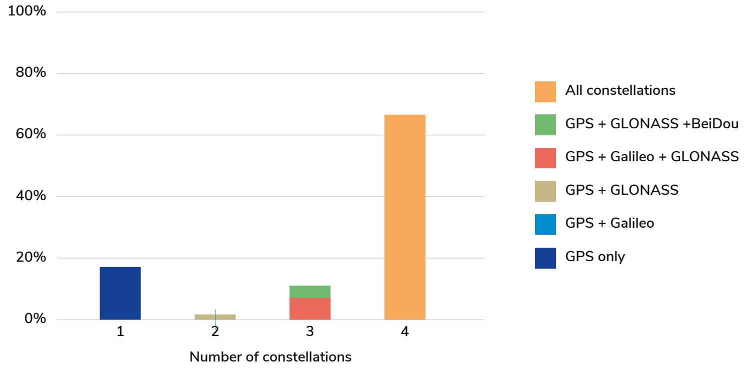
[2] Shows the percentage of receivers capable of tracking each constellation

SUPPORTED FREQUENCIES BY GNSS RECEIVERS[3]



[3] Shows the percentage of receivers capable of tracking 1, 2, 3 or all the 4 frequencies

SUPPORTED CONSTELLATIONS BY GNSS RECEIVERS[4]



[4] Shows the percentage of receivers capable of tracking 1, 2, 3 or all 4 global constellations

Disclaimer: The above charts reflect manufacturer's publicly available claims regarding their product's capabilities and judgement on the domains to which they are applicable. Use in actual use cases may vary due to issues such as certification, implementation in the end user product, and software/firmware configuration.

Over **80% of devices** in this family can support **multiple GNSS** constellations, with more than **65% supporting all constellations**. Multi-constellation support is therefore standard, and particularly in challenging environments where signals from one constellation might be obstructed. However, specific configuration is often required to enable additional constellations, allowing premium devices to optimise their use based on specific scenarios.

Almost **60% of these devices support SBAS** compatibility, which provides a relatively low-cost means of achieving improved accuracy and reliability compared to entry-level devices.

While single-frequency (L1 only) remains the most common configuration, there is a **growing trend towards dual-frequency** operation, specifically L1+E5. Although the percentage of devices supporting dual-frequency is still modest, this trend is increasing, with over **10% of devices even supporting triple-frequency** bands.

Several devices within the receiver family now also support L2, E5, or E6. Compared to previous years, this is a growing trend as priorities evolve and technology becomes easier to integrate. For the same class of devices, increased accuracy and availability are now achievable through multi-frequency support.

The readiness for **advanced GNSS features is still limited** in this receiver family, although most receivers are capable of tracking and decoding full navigation messages. This means that, of the advanced services, most are capable of tracking and decoding the full Galileo I/NAV message and are **ready for the implementation of OSNMA and EWS** when available. Depending on the use case, mass-market premium receivers can deliver **continuous carrier phase** measurements with a focus on performance over battery life. Some devices in this family also have expanded capabilities to support advanced processing modes such as **RTK** or **PPP**, provided the necessary data is supplied. In many cases, sufficient processing power is not available on the device itself without compromising battery life, but this can be addressed with internet connectivity, allowing high-accuracy solutions to be processed remotely.

Multi-frequency differentiates the mass-market premium receiver family

TYPICAL STATE-OF-THE-ART RECEIVER SPECIFICATIONS FOR THE MASS-MARKET PREMIUM RECEIVER FAMILY

	Consumer Solutions chip	Photography Drone module	Automotive[1] Tracking module
Dimensions	4 x 4 x 1mm	20 x 30 x 10mm	12 x 12 x 2mm
Weight	0.1g	50g	1g
Number of channels	72	72	184
Constellations	GPS, GLONASS, Galileo, BeiDou	GPS, GLONASS, Galileo, SBAS, BeiDou	GPS, GLONASS, Galileo, BeiDou
Frequencies[2]	L1 L2 E5	L1 L5	L1 L2 E5
Power	20mW	150mW	80mW
Update rate	5 - 10Hz	10 - 30Hz	5 - 30Hz
TTFF	<30s (Cold start) <2s (Hot start)	<30s (Cold start) <2s (Hot start)	<30s (Cold start) <2s (Hot start)
Horizontal accuracy (95%)	GNSS 2m	GNSS 2m SBAS 1.5m RTK 0.05m	GNSS 3m
Vertical accuracy	-	GNSS 4m	-
Velocity accuracy	0.05m/s	0.05m/s	0.05m/s
Timing accuracy (RMS)	30ns	30ns	30ns

Disclaimer: The above specifications represent a typical chip/SoC package or module based on manufacturer's published literature for their latest products. Consequently, discrepancies may exist between the installed receiver's characteristics and those stated above.

1: Excludes chipsets for safety-critical/autonomous use cases.

2: Users can typically specify between L1+L2 or L1+E5 model variants for their use case.

Typical specifications

The devices in the premium receiver family build on the features already present in the entry-level devices but support **additional frequencies** and access to **augmentation services** to enhance accuracy and availability. While basic **SBAS support is widespread**, the adoption of more advanced technologies, such as **RTK** and **HAS**, is emerging as a key differentiator among high-end devices where manufacturers are utilising more advanced features to distinguish their offerings.

All devices typically offer dual-frequency in a configurable design where system integrators can decide which combination of frequencies (L1 + E5 or L1 + L2) they wish to deploy depending upon use case. For consumer solution devices, this enables improved performance at a moderate increase in power consumption.

In contrast, devices targeting mobility emphasise the ability to **operate in high-speed environments**. To ensure performance in constrained environments, automotive variants process all available channels and incorporate features like MEMS accelerometers/gyros, which enhance the overall performance of the GNSS systems and maintain positioning even when satellite signals are temporarily unavailable. A drone module, adds in 3D vector determination, and optional RTK and SBAS to its capabilities. Combined with the higher update rates required to address each platform's variable speed and orientation, these characteristics **result in increased power consumption** compared to consumer solution use cases.

As premium products, they also **frequently offer upgradeable features** through firmware updates supporting configuration changes, and access to augmentation services, such as RTK support, allowing for a greater levels of performance.

The introduction of **omni-directional embedded antennas** offers comprehensive coverage, regardless of orientation or movement, and is becoming ever-present in consumer solutions.

UNION

The UNION project, funded by the EUSPA and coordinated by ROKUBUN, aimed to develop a high-precision satellite positioning solution for mass-market devices such as smartphones, vehicles, and drones. By combining RTK and PPP technologies, UNION improves navigation accuracy to meter-level for smartphones and lane-level for road use cases. The RTK mode provides fast, centimetre-level accuracy but requires a local base station, which limits the range. On the other hand, PPP works globally without the need for base stations, but typically has slower convergence and sub-meter accuracy. A hybrid system combining both modes hence improved accuracy, reliability, availability and continuity achieving precise real-time positioning with broader coverage.

More information can be found on the UNION page of the EUSPA website.

Mass-market premium family sample products

uBlox - X20

The X20 is an all-band (L1/L2/L5/L6) platform capable to receive all available GNSS satellite signals, aiming at offering the highest accuracy positioning even in difficult signal environments. The addition of the L6 band in a mass-market product represents a major market innovation, since this enables correction services, such as Galileo HAS, in a compact form factor chipset.

content.u-blox.com

Qualcomm - Snapdragon 8 Gen 3

Snapdragon™ 8 Gen 3 Mobile Platform is one of the latest SoC platform from Qualcomm® designed to best exploit 5G opportunities. It is capable to track GPS, GLONASS, BeiDou, Galileo, QZSS, NavIC, and supports triple frequency (L1/L2C/L5).
Additionally, the integration of satellite-based positioning information with other built-in sensors enables sensor-assisted Navigation.

www.qualcomm.com

Broadcom - BCM4778

BCM4778 is Broadcom's third generation dual-frequency L1-L5 GNSS receiver, featuring advanced multipath mitigation, L5 acquisition capability, in-band and out-of-band filtering, integrated PMU with direct connection to battery and jamming protection.

www.broadcom.com

Allystar - TAU1202

The Allystar TAU1202 is a high-performance dual-band multi-GNSS module supporting both the L1 and L5 bands to enhance sub-meter positioning accuracy. Multipath mitigation is ensured by leveraging the L5/B2a/E5a signal. Constellations received include GPS, Galileo, GLONASS, BeiDou, QZSS and IRNSS.

www.allystar.com

oneNav - L5-direct GNSS technology

OneNav offers “L5-direct GNSS technology”, a commercial licensable digital IP core solution that directly acquires and tracks L5 frequency only, eliminating reliance on the L1 band and claiming several benefits: simpler hardware allowing for lower battery consumption, a faster TTFF and a better accuracy in dense urban areas where L5 signals are particularly efficient in tackling multipath errors.

onenav.ai

MediaTek/Airoha - AG3335M

AG3335M is a Multi-GNSS (GPS, Galileo, BeiDou, GLONASS, QZSS) duaL-band receiver that uses advanced 12nm manufacturing technique, greatly reducing power consumption. Thanks to its low tracking sensitivity, short initial positioning time, high positioning accuracy, it claims to further improve motion and mileage accuracy, making fitness wearable data more accurate.

www.airoha.com

The mention of specific companies or manufacturers' products on this page is for informational purposes only and does not constitute endorsement, preference or recommendation by EUSPA. These references are intended solely to illustrate the relevant receiver categories (families), highlighting those that have recently been introduced to the market.

Professional non-regulated receiver family

Characterisation of receiver family

This family of devices is commonly used in use cases which require **accurate positioning, navigation, and timing (PNT) over a long term** and in which **upfront investment is accepted** as necessary to achieve higher levels of uninterrupted performance. The use cases supported by this family include:

- **Geomatics**: high-accuracy land, marine and hydrographic surveying and mapping;
- **Agriculture**: precision agriculture including tractor steering and field mapping for optimising crop yields;
- **Drones**: accurate navigation and geofencing for UAV and drones and well as georeferencing of aerial imagery;
- **Infrastructure**: Timing and synchronisation of power grids and telecommunication networks for power supply phases and data transmission. Machine guidance and robotics in construction.

These use cases have elevated requirements for accuracy, availability, and robustness compared to other sectors and **require fast adoption of new constellations and frequencies** to maintain cutting edge capabilities.

Industrial landscape

In this sector, some manufacturers **tend to specialise**. For example, Trimble leads in agriculture with the most products available within this receiver family, while Hexagon and Topcon have a significant footing in the surveying market. Others, such as Furuno in maritime and Meinberg in timing, produce devices that offer multi-constellation GNSS and SBAS support. Additionally, some manufacturers of **mass-market receivers, like u-blox, are beginning to target this family**.

EXAMPLES OF REPRESENTATIVE COMPONENT MANUFACTURERS[1]

ARBITER SYSTEMS	North America	arbiter.com
BEIJING UNISTRONG	Asia- Pacific	unistrong.com
COMNAV	Asia-Pacific	comnavtech.com
EOS POSITIONING SYSTEMS	North America	eos-gnss.com
HEXAGON AB	Europe	hexagon.com
HI-TARGET	Asia-Pacific	hi-target.com.cn
KONGSBERG	Europe	kongsberg.com
MEINBERG	Europe	meinbergglobal.com
SAFRAN	Europe	safran-navigation-timing.com
SATLAB	Europe	satlab.com.se
SEPTENTRIO	Europe	septentrio.com
TOPCON	Asia-Pacific	topconpositioning.com
TRIMBLE	North America	trimble.com

1: The list is not exhaustive; its purpose is to illustrate the receiver family with typical component manufacturers. Also, the list does not include system and terminal integrators, and therefore some key industry may not appear in the list. For more detailed list of component, receiver and system manufacturers, refer to value chain pages in EUSPA EO and GNSS Market Report, issue 2.

Key performance parameters of receiver family

This family generally comprises receivers with **enhanced features**, focusing more on multi-frequency and multi-constellation capabilities that deliver higher levels of accuracy compared to the mass-market premium families. This wide constellation and frequency support means that most manufacturers can support **advanced GNSS capabilities**, such as OSNMA. As they are not regulated, they cater to a wider set of use cases in professional areas.

Agricultural or timing applications often place these devices in very remote locations where high accuracy is challenging. In these scenarios, power consumption is of least importance, and **true dual-frequency capabilities and value-added services**, which contribute to power demand, are employed to ensure optimal positioning accuracy.

Where devices are physically handled or carried (e.g., pole-mounted RTK rovers, or other autonomous platforms), minimising the weight of the battery becomes essential to ensure the maximum utility of the device, making such use cases the exception to the rule.

Integrity of the positioning data is critical, especially in essential use cases such as timing and synchronisation within power grids. Similarly, robustness is demanded across use cases, ensuring data gathered, or navigation guidance is not compromised.

A **fast TTFF is beneficial**, particularly in situations where devices are frequently turned on and off. However, in many professional use cases, the device remains on for extended periods. Many of these use cases are outdoors, making the need for indoor positioning capabilities less of a priority.

Key Performance Parameter (KPP)[2]	Professional Non-Regulated Rx Family
Accuracy	★★★
Availability	★★★
Continuity	★★★
Integrity	★★★
Indoor penetration	★★☆
Latency	★★☆
Power consumption	★☆☆
Robustness	★★★
Time-To-First-Fix (TTFF)	★★☆

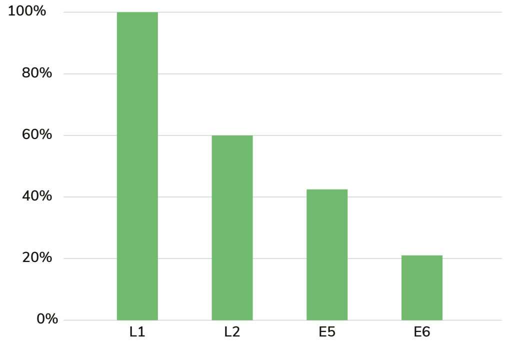
★★★ High priority ★★☆ Medium priority ★☆☆ Low priority

2: The Key Performance Parameters are defined in Annex 1

Multi-constellation capabilities supporting improved accuracy demands

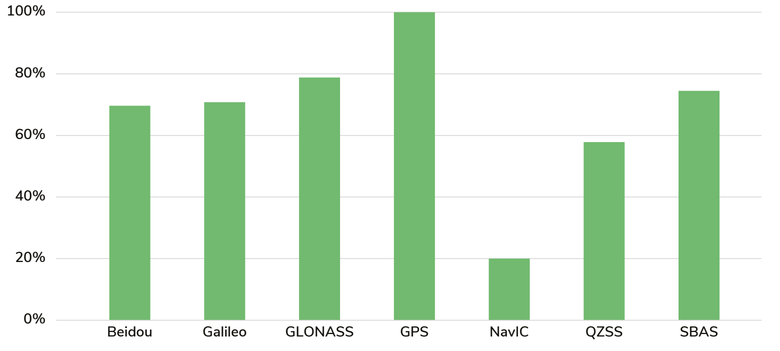
The adoption of **multiple frequency bands is ever-present** in professional non-regulated devices, where improved accuracy and the exploitation of all signals helps to **maximise value**, particularly within agriculture, timing and synchronisation, and surveying. This is driven by the nature of the market, with specialised use cases that benefit the end user through **increased productivity and reliability**.

FREQUENCY CAPABILITY OF GNSS RECEIVERS[1]



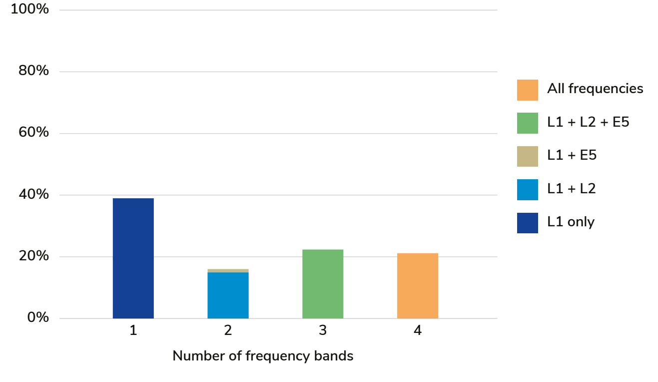
[1] Shows the percentage of receivers supporting each frequency band

CONSTELLATION CAPABILITY OF GNSS RECEIVERS[2]



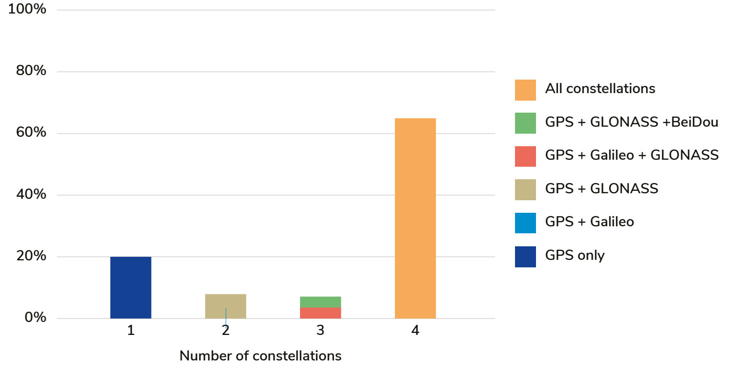
[2] Shows the percentage of receivers capable of tracking each constellation

SUPPORTED FREQUENCIES BY GNSS RECEIVERS[3]



[3] Shows the percentage of receivers capable of tracking 1, 2, 3 or all the 4 frequencies

SUPPORTED CONSTELLATIONS BY GNSS RECEIVERS[4]



[4] Shows the percentage of receivers capable of tracking 1, 2, 3 or all 4 global constellations

Disclaimer: The above charts reflect manufacturer's publicly available claims regarding their product's capabilities and judgement on the domains to which they are applicable. Use in actual use cases may vary due to issues such as certification, implementation in the end user product, and software/firmware configuration.

As with other families, multi-constellation support is on the rise, with over **65% of devices now supporting all constellations**. This uptake is happening more slowly than the mass-market due to longer product lifecycles. Conversely, the number of devices supporting **only GPS is in decline**, with less than 20% now limited to basic GPS. This trend is becoming standard in new devices as it ultimately aids operation in environments with limited visibility of satellites from a single constellation and is expected by end users who demand the best performance.

A significant proportion of devices support multiple frequencies, improving positioning accuracy and mitigating against signal interference and multipath effects which are critical for high-accuracy activities. However, approximately **40% of devices still support only L1**, often due to older devices that meet the necessary requirements for their dedicated tasks, most prominently for high-accuracy timing use cases.

The adoption of multiple frequencies continues to rise, with 60% supporting L2, over 40% supporting E5, and over 20% supporting E6. This demonstrates a trend of **gradual adoption of new signals as they become available**. These signals provide enhanced accuracy and interference resilience, solidifying their deployment in accuracy-critical use cases such as automatic steering within agriculture. As power consumption is not a priority, professional non-regulated receiver families can afford to prioritise accuracy over power efficiency, allowing devices to take advantage of the most recent signal developments over battery life.

A significant number of devices support SBAS, with more than 70% adoption. Within certain use cases, such as surveying, SBAS adoption is even higher reaching as much as 90%. While devices may **support SBAS**, its use is often superseded by application-based requirements, as is the case in agriculture where **RTK/NRTK/PPP is preferred over SBAS**.

The high proportion of E5 and E6 support in this family reflects the performance-driven approach. There is a readiness within this family for improved services such as HAS, which would deliver additional performance to decimetre accuracy.

Professional non-regulated receivers utilise advanced processing techniques

Typical specifications

Devices commonly support multiple GNSS constellations to improve accuracy, availability, and reliability compared to mass-market devices. A significant portion of these operate on multiple frequencies to **achieve sub-metre or even centimetre-level** accuracy required by applications such as surveying, agriculture or robotics. While **SBAS support is common**, many devices go further and **support RTK and PPP** services for even higher accuracy.

TYPICAL STATE-OF-THE-ART RECEIVER SPECIFICATIONS FOR THE PROFESSIONAL NON-REGULATED RECEIVER FAMILY

Features	Surveying receiver	Agriculture receiver	Infrastructure receiver
Dimensions	12 x 12cm	16 x 16 x 5cm	48 x 17 x 27cm
Weight	2kg	2kg	>5kg
Number of channels	672	544	448
Constellations	All	All	All
Frequencies	All	All	L1 E5
Power	10W	10W	50W
Update rate	10Hz	20Hz	10Hz
TTFF	<60s (Cold Start) <2s (Hot Start)	<45s (Cold start) <1.2s (Hot start)	<60s (Cold Start) <2s (Hot Start)
Horizontal accuracy (95%)	GNSS – 2m DGNSS – 0.25m RTK – 0.01m NRTK – 0.01m	GNSS – 2m DGNSS – 0.8m SBAS – 1.2m RTK – 0.03m	-
Timing accuracy (RMS)	-	-	4ns
Connectivity	NMEA 0183, GSOF, RT12 and 27, Bluetooth EDR/BR v5.1, Wi-Fi, Cellular	NMEA v2.30, 4.0 or 3.01RTCM v2.2, 2.3, 3.0 or 3.1CMR2.0 and CMR+UHF, Bluetooth 2.1, Wi-Fi, Cellular	NTPv2/3/4, SNTPv3/4, RJ45, SFP, SSH, Telnet, REST API, USB

Disclaimer: The above specifications represent a typical GNSS receiver based on manufacturers' published literature for their latest products. Consequently, discrepancies may exist between the installed receivers' characteristics and those stated above.

Depending on the use case, manufacturers prioritise different features. For land surveying, emphasis is on centimetre or sub-centimetre level accuracy, while for timing and synchronisation, it is on the timing signal, allowing for a trade-off on accuracy for faster TTFF and improved robustness. The form factor varies from compact, board-level modules designed for integration into larger systems, to standalone "box" solutions that are ready to use from the manufacturer. The choice of form factor depends largely on the specific application, with module-based solutions offering flexibility and integration options, while box solutions provide ease of deployment.

It is common for **rugged smart antennas** to be incorporated into these devices, often with high-gain and low-noise amplifiers to improve signal quality. RTK and PPP capabilities require a robust power unit to support continuous processing. These devices also feature memory for logging data as well as non-volatile memory to ensure data is not lost during power failures or unexpected shutdowns. The user interface includes hardware buttons, ports for direct connection, and wireless connectivity through Bluetooth or Wi-Fi, in addition to cellular (3-4-5G) to receive NRTK corrections. This might also be addressed through a dedicated radio modem (UHF for terrestrial or even L-band for satellite connectivity).

As industries like agriculture move towards automation, the need for highly accurate devices is increasing. Services like Galileo's **HAS deliver optimal accuracy** for practices such as planting seeds and applying fertilisers. Receivers in this family are already **hardware capable** and generally require just **firmware updates** to enable this capability.

VYTIS-AR

Fundamental Elements VYTIS-AR

The VYTIS-AR project, led by NTLAB, UAB, aims to develop a high-accuracy GNSS receiver for precision agriculture, leveraging Galileo's High Accuracy Service (HAS). The technical innovation integrates a universal GNSS receiver with centimetre-level accuracy via PPP (Precise Point Positioning) and RTK (Real-Time Kinematic) modes. This is supported by the NT1058.AR baseband processor which functions as the brain of the receiver by processing and decoding signals from all satellite systems and frequencies for comprehensive GNSS signal reception. The project's objectives include designing a HAS-enabled receiver, developing and testing prototypes, validating their performance in real-world agricultural scenarios, and preparing for mass production. This innovation provides cost-effective, high-accuracy navigation solutions, which will particularly benefit smaller farms.

More information can be found on the VYTIS-AR page of the EUSPA website.

Professional non-regulated family sample products

EOS - Skadi Gold™

The Skadi Gold™ receiver supports all GNSS constellations and signals and various differential corrections sources such as RTK, Atlas® or Galileo HAS. The receiver can be easily integrated with any mobile applications and upgraded with additional features to maximise field productivity, such as collecting points without "bubbling up" your survey range pole (Skadi Tilt Compensation™) or "smart handle" that combines LIDAR and MEMS technologies (Skadi Smart Handle™).

eos-gnss.com

ublox - NEO-F10T

The NEO-F10T timing module provides nanosecond-level accuracy and supports all four global satellite constellations and dual-frequency to meet the most stringent timing synchronisation requirements in 5G. The module includes built-in security features for highest robustness against malicious attacks such as advanced anti-spoofing algorithm, and T-RAIM to provide highest level timing integrity.

www.u-blox.com

Septentrio - AntaRx-Si3

The AntaRx-Si3 is a triple-band and multi-constellation smart antenna that, with RTK positioning enhanced by IMU, delivers positioning with 3D orientation down to the centimetre level. Since it is packed in a single-robust IP69k-rated housing, and is robust against shocks and vibrations, it is well suited for applications in challenging environments like construction or mining.

www.septentrio.com

NovAtel - SMART7-SI

The SMART7-SI is a ready to install positioning solution for precision agriculture systems. This multi-GNSS and multi-frequency smart antenna with IMU supports not only RTK but also L-Band signal to access world-wide corrections signals provided by Terrastar, and all modern agriculture wireless solutions for tablets and smartphones such as WI-FI, integrated NTRIP and Ethernet connectivity.

www.novatel.com

Kongsberg - Seapath 385

The Seapath 385 is a multi-constellation and multi-frequency receiver with enhanced inertial technology and processing algorithm, developed specifically for hydrographic surveying. It supports various augmentation capabilities such as SBAS, RTK, Galileo HAS or Fugro G4/G4+. The receiver is robust against GNSS dropouts, providing spoofing detection and rejection capabilities.

www.kongsberg.com

Trimble/Applanix - APX-18 UAV

The Trimble APX-18 UAV is an OEM GNSS-Inertial solution with dual GNSS antenna input and support of RTK that is well suited for a wide range of UAVs applications in geomatics or agriculture. While an extremely small package, it produces a highly accurate position and orientation solution that allows georeferencing LiDAR and other imaging data.

www.applanix.com

The mention of specific companies or manufacturers' products on this page is for informational purposes only and does not constitute endorsement, preference or recommendation by EUSPA. These references are intended solely to illustrate the relevant receiver categories (families), highlighting those that have recently been introduced to the market.

Professional regulated receiver family

Characterisation of receiver family

The professional regulated family of devices encompasses those built to **performance requirements specified** and regulated through standards at an **international or national level**. In recent years, there has been a significant **shift towards multi-constellation** and **multi-frequency** devices, which is not yet reflected in this family due to the need for changes in international standards and regulations. Typically, receivers in this family are deployed in safety-critical use cases, including:

- **Aviation and Drones**: focused on navigation and approach procedures at an aircraft level, supplementing augmentation systems (both space and ground-based), and including use cases such as ADS-B, but also includes emergency SAR beacons and support for autonomous distress tracking;
- **Maritime and Inland Waterways**: encompasses navigation use cases, SAR beacons, and support for AIS broadcast;
- **Rail**: includes automation use cases associated with train control, signalling and traffic management;
- **Insurance and Finance**: supporting payment services with accuracy time keeping within banking and insurance services;
- **Automotive**: for example, the Smart Tachograph, which is now mandatory under EU legislation and will benefit from the availability of OSNMA.

In this family, the focus is on providing devices that comply with regulatory standards with supporting evidence to achieve certification. Due to standardisation and regulatory roadmaps, as well as the **costly and time-consuming** process needed to **achieve certification**, devices in this family tend to **evolve slowly** and be supported in operation for longer periods than other families. The typical life cycle of these devices varies between **10-25 years**.

EXAMPLES OF REPRESENTATIVE COMPONENT MANUFACTURERS[1]

ACR ELECTRONICS INC	North America	acrartex.com
COBHAM	Europe	cobham.com
COLLINS AEROSPACE (RTX CORPORATION)	North America	collinsaerospace.com
VDO (CONTINENTAL)	Europe	vdo.com
ESTERLINE (TRANSDIGM)	North America	transdigm.com
FURUNO	Asia-Pacific	furuno.com
GARMIN	North America	garmin.com
HONEYWELL	North America	honeywell.com
JOTRON	Europe	jotron.com
KONGSBERG	Europe	kongsberg.com
SAAB	Europe	saab.com
SAFRAN	Europe	safran-group.com
SEPTENTRIO	Europe	septentrio.com
THALES AVIONICS	Europe	thalesgroup.com
u-blox	Europe	u-blox.com

1: The list is not exhaustive; its purpose is to illustrate the receiver family with typical component manufacturers. Also, the list does not include system and terminal integrators, and therefore some key industry may not appear in the list. For more detailed list of component, receiver and system manufacturers, refer to value chain pages in EUSPA EO and GNSS Market Report, issue 2.

Industrial landscape

This family is characterised by a diverse range of manufacturers producing devices across Europe, North America, and the Asia-Pacific region. In the aviation sector, there has been little change, with Thales, Collins Aerospace, and Garmin remaining active, and North American companies continuing to dominate. In the maritime domain, manufacturers such as Furuno, Kongsberg, and Garmin lead, particularly in the AIS market, while Jotron and Safran are prominent in the production of SAR beacons. For the rail sector, Honeywell and Septentrio are representative manufacturers, providing both rail position reference modules and receivers for integration.

Key performance parameters of receiver family

The professional regulated receiver family relies on performance to meet minimum levels determined by safety criticality or regulatory compliance, targeting specific regulations or achieving performance levels that support numerous use cases. **Overall performance is crucial** in these use cases, with equal attention given to the availability, accuracy and continuity of the GNSS position information.

Regardless of the accuracy of the GNSS position, it must be a **trusted position**, based on compliance with regulations. Therefore, the integrity and robustness of the position are paramount and are considered within these use cases. For example, the Smart Tachograph, must provide a trusted report. The receivers need to **ensure uninterrupted service**, which may involve integration with other sensors and the adoption of specific algorithms to improve the resilience of the receiver. A system view is often taken into consideration, where the performance of the **receiver and antenna designs are optimised** to deliver the most robust service possible.

This **integration with other sensors** is prevalent across the aviation, maritime, and rail industries, where overall system resilience to external interference or operation in obstructed environments, such as valleys or fjords (aviation and maritime) or cuttings and urban areas (rail), might result in GNSS signal unavailability. When this occurs, the receiver needs to regain position information as quickly as possible.

Key Performance Parameter (KPP)[2]	Professional Regulated Rx Family
Accuracy	★★★
Availability	★★★
Continuity	★★★
Integrity	★★★
Indoor penetration	★★☆
Latency	★★★
Power consumption	★☆☆
Robustness	★★★
Time-To-First-Fix (TTFF)	★★★

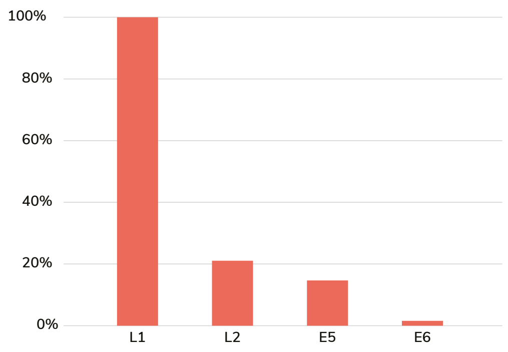
★★★ High priority ★★☆ Medium priority ★☆☆ Low priority

2: The Key Performance Parameters are defined in Annex 1

Single-frequency L1 continues to dominate

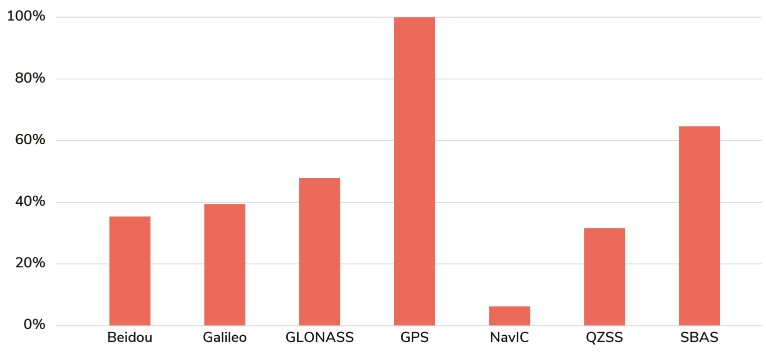
With stringent regulatory requirements put on professional regulated devices, support is generally placed on the legacy L1 frequency band, with E5 capabilities entering the picture after further testing and integrity validation.

FREQUENCY CAPABILITY OF GNSS RECEIVERS[1]



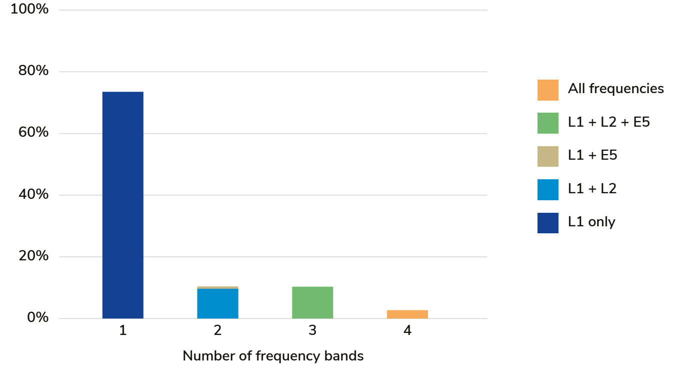
[1] Shows the percentage of receivers supporting each frequency band

CONSTELLATION CAPABILITY OF GNSS RECEIVERS[2]



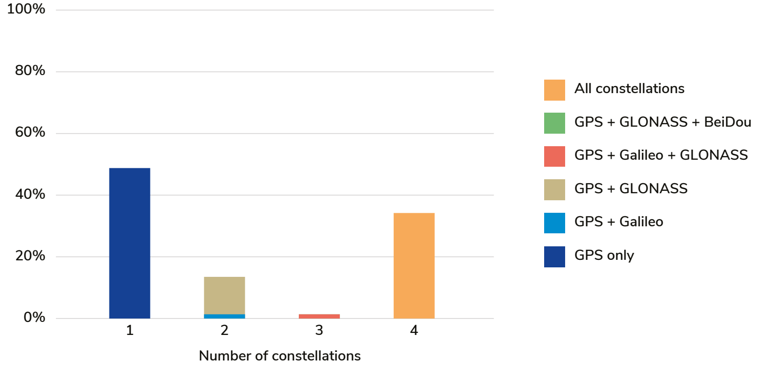
[2] Shows the percentage of receivers capable of tracking each constellation

SUPPORTED FREQUENCIES BY GNSS RECEIVERS[3]



[3] Shows the percentage of receivers capable of tracking 1, 2, 3 or all the 4 frequencies

SUPPORTED CONSTELLATIONS BY GNSS RECEIVERS[4]



[4] Shows the percentage of receivers capable of tracking 1, 2, 3 or all 4 global constellations

Disclaimer: The above charts reflect manufacturer's publicly available claims regarding their product's capabilities and judgement on the domains to which they are applicable. Use in actual use cases may vary due to issues such as certification, implementation in the end user product, and software/firmware configuration.

The majority of devices rely **primarily on GPS and SBAS** due to current regulations, and the need for trust in position information required by these use cases. However, there is a rising trend of more devices incorporating additional constellations, particularly GLONASS and Galileo. Traditionally, aviation and maritime requirements have led the way for updated device capabilities, but other use cases in insurance and finance are becoming more open to adopting systems beyond GPS. This reflects the growing **emphasis on resilience** in this family, which has also been the driver historically for **safety-of-life use cases** where trust in position information is critical.

Due to the slow pace of change, the adoption of multi-frequency devices is still relatively limited, with over **70% of devices supporting L1 only**. Ongoing efforts at international level aim to establish a dual-frequency, multi-constellation standard targeting aviation and maritime. In the meantime, there is a **growing** percentage of devices that support **dual** and even **triple** frequencies, targeting use cases beyond aviation and maritime. This is crucial for improving positioning accuracy and mitigating errors.

Overall, this family's devices rely on approved frequency bands to ensure **compliance and avoid interference** issues. 100% of devices endorse the GPS L1 frequency while alternative frequencies are far less common, with L2 capable devices at 20% and E5 at just over 10%.

The adoption of E5 within this family lags due to regulatory dependency. Whilst the signal in space has an internationally agreed format, E5 is not yet fully available for use until declared so by their respective providers. Development of minimum performance standards and initial receiver designs can continue, but manufacturers will not be able to obtain certification until they can **validate production receivers in real world conditions**. The standards, and therefore the receivers under development, will also include support for Galileo. Use cases that are not dependent on such certification are **already adopting Galileo and E5** as is the case for automotive.

Standards and regulations still dictate single-frequency

Typical specifications

Professional regulated devices provide the **backbone of critical industries** where accuracy, reliability, and regulatory compliance are paramount. These devices share several commonalities across regulated aviation, maritime, and automotive sectors. While devices generally have similar capabilities, some may only support single-frequency GPS, while others incorporate DFMC capabilities, depending on the requirements and environmental conditions they are designed for.

TYPICAL STATE-OF-THE-ART RECEIVER SPECIFICATIONS FOR THE PROFESSIONAL REGULATED RECEIVER FAMILY

Features	Aviation receiver	Maritime receiver	Automotive chip
Dimensions	16 x 12 x 27cm	26 x 17 x 7cm	16 x 12 x 3mm
Weight	4kg	2.2kg	0.5g
Number of channels	12	28	184
Constellations	GPS SBAS	GPS, SBAS, QZSS, GLONASS	All
Frequencies	L1	L1	L1 L2 E5
Power	60W	10W	400mW
Update rate	<10Hz	10Hz	50Hz
TTFF	<60s (Cold start) <5s (Hot start)	<90s (Cold start) <1s (Hot start)	<32s (Cold start) <1s (Hot start)
Horizontal accuracy	GNSS 5-15m SBAS 3m	GNSS 2.5 - 10m DGNSS 0.3 - 5m SBAS 2 - 7m	GNSS 2.5 -13m DGNSS 0.3 - 5m SBAS 2 - 8m RTK – 0.2m
Vertical accuracy	SBAS 8m	N/A	N/A
Connectivity	ARINC 429, 743	RS422 NMEA 0183 / 2000	UART, USB, SPI, I2C
Standards and certification	DO-229E, DO-245, DO-246, DO-208, DO-178/ED-12, DO-254/ED-80, DO-160/ED-14, DO-253/ED-88, ED-114, ETSO-C144/C145/C146	IEC60945, 61108-1/2/3/4, 61162-1/3, 62288, RTCM SC104 USCG or Wheelmark (EC MED)	AEC-Q100 ISO16750 ISO26262 ASIL
Other	Complete unit conforming to standard (e.g. 2 MCU). External antenna	Complete unit with built-in or remote CDU. External antenna	Receiver Chip

Disclaimer: The above specifications represent a typical GNSS receiver based on manufacturers' published literature for their latest products. Consequently, discrepancies may exist between the installed receivers' characteristics and those stated above.

Adherence to international standards and regulations (e.g., ICAO for aviation, IMO for maritime) is a fundamental aspect that heavily dictates the current technology and capabilities of the devices in this family. This can **limit innovation and development**, as these devices must conform to strict requirements that have been established for many years. For example, aviation receivers are typically limited to receiving on a single-frequency and constellation due to regulatory requirements. However, the frequencies available to other devices might be more open, allowing for improved accuracy in urban environments by prioritising robustness and availability. For example, in automotive to support **ADAS performance requirements** some receivers utilise **RTK and triple frequencies**.

These devices include an embedded processing unit to handle data processing, filtering, and augmentation. Processed data can be outputted through USB, Ethernet, or wireless connections. Some devices integrate IMUs, providing orientation and acceleration data to ensure continuous positioning is available when GNSS signals are temporarily unavailable. Antennas are commonly external to ensure a clear line of sight and avoid obstructions that could block or reflect signals.

Given the critical nature of their use cases, the receivers are increasingly equipped with **anti-jamming and anti-spoofing** technology to protect against intentional interference. The rise of autonomous platforms is creating new demand for GNSS technology. When developed alongside stringent regulations, this is expected to lead to **changes in industry standards**, allowing the adoption of multi-constellation and multi-frequency solutions in these markets.

SEGRA

Fundamental Elements

The SEGRA (Shipborne Receiver EGNOS Related Activities) project was led by the EUSPA and aimed to improve maritime navigation technology by creating new guidelines for implementing SBAS Dual-Frequency Multi-Constellation (DFMC) receivers. These guidelines aid manufacturers with the implementation of the EGNOS V3 satellite system - a maritime solution which addressed the limitations of current ground-based differential GNSS systems by offering a more cost-effective and accurate navigation signals. SEGRA's aim was to ensure that shipborne receivers could effectively use this new technology whilst adhering to international safety standards. The project also included simulations to evaluate the functionality of EGNOS DFMC to remove the need for live services.

More information can be found on the SEGRA page of the EUSPA website.

Professional regulated family sample products

Jotron - Tron 40AIS

This buoyant EPIRB is compliant with IMO and Safety of Life at Sea (SOLAS) regulations and embeds both a multi-constellation GNSS receiver and an AIS transmitter.
The beacon has the capability to use the Galileo's Return Link Service (RLS) to confirm the user that the distress signal has been received. This confirmation is implemented by means of a blue LED indicator.

jotron.com

Collins Aerospace - CGLU-2100

The GLU-2100 multi-mode receiver includes a dual-frequency GBAS, SBAS, GPS and Galileo receiver that meets the most stringent aviation standards from ICAO RTCA. The device makes use of Software Defined Radios for flexibility and has been developed to validate the latest EUROCAE ED-259 MOPS. The addition of dual-frequency SBAS will increase the availability of LPV approaches as well as well as satisfy ADS-B "Out" mandate requirements when flying in USA airspace.

www.collinsaerospace.com

Seas of Solutions - FastFind Return Link

The FastFind Return Link was the world's first PLB using the Galileo's Return Link Service (RLS).
This lightweight device can transmit the user coordinates obtained from its internal single-frequency GPS + Galileo receiver and confirm that the signal has been received by SAR authorities, for which the user is informed with a blue flashing light.

www.seasofsolutions.com

Garmin - GNX™ 375

The GNX™ 375 is an aviation GPS/SBAS navigator tailored to General Aviation users. It provides LPV approach capability and incorporates a built-in 1090 MHz ES transponder meeting ADS-B "Out" requirements, thus facilitating the compliance with the USA mandate.

www.garmin.com

VDO/Continental - DTCO®4.1

The DTCO®4.1 is Continental's 2nd version of the smart tachograph, compliant with the EU Mobility Package I regulations. It includes an enhanced GNSS receiver with Galileo OSNMA for authentication of the vehicle position. In addition, it incorporates automatic detection and registering of border crosses, thus eliminating the previous need to stop when crossing borders; and interfaces with intelligent transport systems via Bluetooth communication.

www.fleet.vdo.com

SAAB - R6 NAV PRO

The R6 NAV PRO is the high-accuracy version of Saab's multi-frequency R6 NAV, a navigation system compliant with IMO requirements for SOLAS navigation.
While other versions of the R6 NAV include DGNSS and SBAS, the PRO version adds for example compatibility with RTK and Galileo HAS, allowing accuracies below decimeter level to support hydrographic surveying and dredging operations.

www.saab.com

The mention of specific companies or manufacturers' products on this page is for informational purposes only and does not constitute endorsement, preference or recommendation by EUSPA. These references are intended solely to illustrate the relevant receiver categories (families), highlighting those that have recently been introduced to the market.

Special applications receiver family

Characterisation of receiver family

The special applications receiver family applies to those devices which **cannot be grouped into one of the four previously defined families** and tend to be more **tailored** to an individual application, such that there is **not a single characteristic** that can be used to define the receiver family.

There are multiple examples where a specific receiver design and architecture may be needed – especially in academic research or testing new algorithms as part of development activity. Within this section we examine the case of two niche examples (the use cases for **space**, and those that operate as **Continuously Operating Reference Station (CORS)**) to highlight the different demands that can result in a bespoke receiver being developed. Each has distinct requirements necessitating a specific design, and that the device might need integration with additional sensors with custom interfaces or additional computation added to address the unique characteristics demanded by the application. For example, receivers deployed in space need to be able to cope with the Doppler artefacts of high velocities relative to other satellites, while the CORS receivers are focused on stability and capturing the full range of signals to track with a high update frequency.

Industrial landscape

Due to the nature of the use cases within this receiver family, the industrial landscape tends to be **more specialised** and restricted to providers of **bespoke receivers** that are either configurable or targeted at specific use cases. This market is dominated by a few specialists with established credentials. These specialists often have a track record in the professional non-regulated receiver family, where similarly demanding requirements have led to the development of specialist receivers.

EXAMPLES OF REPRESENTATIVE COMPONENT MANUFACTURERS[1]

AIRBUS GROUP SE	Europe	airbus.com
BEIJING UNISTRONG	Asia-Pacific	unistrong.com
BEYOND GRAVITY (RUAG)	Europe	beyondgravity.com
LEICA (HEXAGON AB)	Europe	hexagon.com
JAVAD	North America	javad.com
QASCOM	Europe	qascom.com
RAKON	Asia-Pacific	rakon.com
SEPTENTRIO	Europe	septentrio.com
SPACEPNT	Europe	spacepnt.com
SSTL (AIRBUS)	Europe	sstl.co.uk
THALES ALENIA SPACE	Europe	thalesaleniaspace.com
TRIMBLE	North America	trimble.com

1: The list is not exhaustive, its purpose is to illustrate the receiver family with typical component manufacturers. Also, the list does not include system and terminal integrators, and therefore some key industry may not appear in the list. For more detailed list of component, receiver and system manufacturers, refer to value chain pages in EUSPA EO and GNSS Market Report, issue 2.

Key performance parameters of receiver family

The **overriding performance** metric in this family is **accuracy**. The speed at which this is achieved, and the power requirements are of secondary importance, considering these receivers support specialised applications—such as space receivers focusing on precise orbital determination—which will also vary depending on the satellite's mission. In the case of reference stations, it is more important to handle all the data. The use of wideband receivers able to **capture the full spectrum** of the constellations being monitored might also be coupled with multiple antennas placed within a grid. Processing this data may be done in the receiver, but support for storage of all signals and transfer for post-data analysis are also requirements, demanding integration into larger devices with **additional connectivity**.

In this receiver family, each parameter is tuned to the use case's needs and environment, potentially leading to **novel architectures**, including the use of **diversity antennas and software-defined radios**. This is the case in some satellite receivers, where the antennas provide additional visibility of GNSS satellites, for instance, where the satellite attitude may vary during orbit or for processing sidelobes which may be needed due to orbital altitudes or attitudes.

Key Performance Parameter (KPP)[2]	Special Applications Rx Family
Accuracy	★★★
Availability	★★★
Continuity	★★★
Integrity	★★★
Indoor penetration	★☆☆
Latency	★★☆
Power consumption	★★☆
Robustness	★★★
Time-To-First-Fix (TTFF)	★☆☆

★★★ High priority ★★☆ Medium priority ★☆☆ Low priority

2: The Key Performance Parameters are defined in Annex 1

Multi-constellation capability reflective of diverse mission demands

Statistics on the use of constellations or frequency bands, as well as general conclusions on receiver characteristics cannot be made for the special applications receiver family, because of both the specialist nature of the products on offer and the small sample size of receiver models considered.

Space receivers adopt multi-constellation and increasingly support multi-frequency

The vast majority of space receivers are multi-constellation receivers. This capability enables modern receivers to be more readily deployed for mission requirements since they already cater to existing technologies that might be needed by the system integrator. Historically, space receivers have been **dominated by single-frequency L1**, but **newer receivers** are now supporting more frequencies and signals allowing for the use of advanced capabilities and services, **including OSNMA and HAS**. This is not always implemented by default and is subject to software implementation in addition to the receiver.

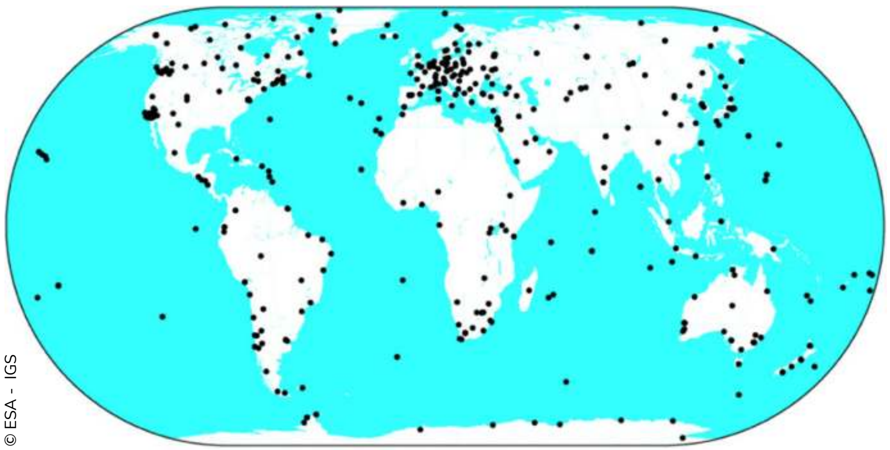
Being multi-constellation means that when the receivers are deployed in support of their mission, engineers can select the best signals available. This can include the use of PPP and other auxiliary services. Where the accuracy demands at the receiver level are even higher, some receivers also support the **use of multiple PPP signals**, taking advantage of services from multiple constellations to deliver **decimetre accuracies** in real time and subsequently, with the support of additional post-processing on the ground, reduce these to **accuracies of around 1cm**.

In some rare cases, there remain receivers on the market that maintain single-frequency, but these tend to be legacy developments still used in some specialist cases. For instance, space-based receivers tracking up to 24 satellites on a single-frequency where there is an emphasis on the ability to do doppler processing due to the high velocity of satellites, combined with processing and power limitations that reduce the number of channels that can be tracked.

Integration of the receivers onto a satellite places additional challenges. This can lead to compromises that need to be made at the antenna level to **reduce back radiation** onto the satellites and maximise the amount of signal captured. Added to the desire to employ proven technology, even with a track record of space operation, the justification for legacy technology is clear.

SPACE GNSS RECEIVER DEVELOPED IN THE FE PROJECT GEYSER

IGS GLOBAL NETWORK



© ESA - IGS

The worldwide International GNSS Station (IGS) network of CORS stations is used as a standard geographical reference and to measure shifts in the solid Earth, oceans and ice.

CORS receivers focus on capturing all available signals

CORS reference stations require the ability to **track all signals** with **utmost accuracy**, to support all current or yet unknown **scientific use cases**. In some cases, receivers for geodetic monitoring and reference stations may employ more than 500 channels, tracking all available signals — meaning all constellations and frequencies. Reference stations **operate continuously**, delivering both very high accuracy and precision, with accuracy in the order of millimetres is required. By comparing the known fixed location of a CORS station with satellite signals, the system can identify, and correct errors caused by atmospheric conditions, satellite clock drift, and other factors. This makes them **critical for demanding use cases**, such as land surveying, geodesy, and monitoring tectonic movement.

CORS receivers are **typically coupled with high-quality calibrated GNSS antennas** with low phase centre variation and often employ designs that reduce multipath errors, such as choke rings. These receivers may even include integrated spectrum analysers and radio frequency filters to **minimise pollution of incoming signals** for processing.

Special applications receiver family designed for specific use cases

TYPICAL STATE-OF-THE-ART RECEIVER SPECIFICATIONS FOR SPECIAL USE CASES

Features	Space receiver	CORS receiver
Number of channels	24	555
Code / Phase processing	Code and carrier phase Doppler	Code and carrier phase
Constellations	GPS, Galileo	All
Frequencies	L1, L2 E5a, E6	All
Power	100mW - 15W	3W
Connectivity	CAN, I2C, UART, RS422, RS485, MIL-STD-1553B	CMR, CMR+, RTCM v2.1/2.2/2.3/3, BINEX, NMEA 0183 v and via TCP/IP, Ntrip, serial, USB and Bluetooth
Data Logging	-	20 parallel data streams at 50Hz
TTFF	30s - 30min (LEO / GEO)	30s
Horizontal accuracy	<1.0 m	-
Vertical accuracy	<1.0 m	-
Standards	-	-
Form Factor	Complete unit	Complete unit with inbuilt management and secure access using HTTPS, SSL/TLS certificates, access management and port blocking, SFTP/ FTP server and client (push), Email notification, SNMP support

GEYSER

Fundamental Elements

The GEYSER (GalilEo cYber SpacE Receiver) project, led by GEA, was focused on developing advanced GNSS technology for space applications. The project has two main innovations: the GEYSER Hardware Solution and the GEYSER Software Solution. The hardware solution is a medium-grade space receiver designed for precise positioning and navigation in new satellite markets, including mega constellations and LEO systems. The software solution, compatible with Software Defined Radio boards, is made for experimental missions and in-orbit demonstrations. The objectives behind these innovations include improving satellite navigation performance, ensuring cybersecurity and authentication, and supporting precise orbit determination for space debris collision avoidance.

More information can be found on the GEYSER page of the EUSPA website.

Typical specifications

In this receiver family, the key **trend is to reflect state-of-the-art technology**, with receivers designed using the best components available. However, as with any specialist receiver, there are **design trade-offs** that can limit the benefit of processing all available constellations and frequencies. The table opposite provides two examples for space and CORS receivers, demonstrating that the number of constellations supported varies considerably, as does the ability to support multiple frequencies. This is often limited by the processing power needed and the purpose of the receiver.

Space receivers can vary in their use of constellations and frequencies; while the receiver may be capable of supporting multiple constellations, it is an integrator's decision as to which are enabled. In the majority of cases, the receiver is a standalone bolt-on box with data output over an RS422 connection. However, for small LEO CubeSats, this might be a single module integrated and connected via numerous other connections such as I2C and UART.

Indeed, in the majority of space receivers today, **single-frequency on L1 is utilised in form factors that must be hardened against space radiation**. However, the trend is expanding, with more support for additional frequencies. The support for additional frequencies opens the possibility for monitoring of terrestrial and atmospheric conditions employing diverse antennas and receivers. Examples include the use of space receivers for GNSS reflectometry, which utilises reflected GNSS signals to support measurements from the Earth's surface, similar to bistatic radar techniques.

It is interesting to note the **wide range of TTFF**, reflective of the GNSS signal environment the receiver is exposed to. Where the signals may be weaker, and the receiver has to process more Doppler signals and side lobes, the TTFF can be as high as 40 minutes, while in a good geometry, 30 seconds is typical. This is also a factor of the velocities at which the satellites are moving, with typical receivers needing to contend with orbital velocities of up to 16 km/s, and the variety of orbital altitudes from LEO to GEO.

Within **CORS reference station receivers**, the goal is to capture as much high-quality data as possible to enable **onward transmission for post-processing** and offsite monitoring of a station's displacement. To achieve this, typical receivers are designed to store substantial volumes of raw data internally and output it via multiple data streams, as required by the data centre. To ensure the quality of the captured data, these receivers are equipped with filtering and anti-jamming capabilities and are paired with calibrated antennas, thereby minimising the risk of interference or data disruption. Additionally, the receivers support software updates, offering maximum flexibility and ensuring they remain compatible with future signals and evolving message formats.

Disclaimer: The above specifications represent a typical GNSS receiver based on manufacturers' published literature for their latest products. Consequently, discrepancies may exist between the installed receivers' characteristics and those stated above.

Special applications family sample products

Beyond Gravity - PODRIX

PODRIX is spaceborne multi-constellation (GPS, Galileo) multi-frequency receiver specifically tailored to LEO applications, providing real-time navigation with an accuracy below 20cm and real time Precise Orbit Determination (POD) based on Galileo's HAS on E6 signal. To achieve that, specific features in its Kalman filtering have been added.

www.beyondgravity.com

Beyond Gravity - GRAS-2

The GRAS-2 is not only a spaceborne multi-constellation (GPS, Galileo, BeiDou) multi-frequency receiver but also a Radio Occultation (RO) instrument flying on-board various LEO satellites that allows measuring atmospheric profiles (pressure, temperature, humidity) for posterior injection in numerical weather models.
This instrument features two GNSS antennas for rising and setting occultations and an additional one for navigation.

www.beyondgravity.com

Qascom - QN500

Qascom's QN500 is a spaceborne dual-constellation (GPS, Galileo) dual-frequency (L1/L5) receiver based on COTS EEE hardware. It has been developed for new space applications that require robust PNT and cybersecurity. For this reason, it support Galileo OSNMA.
To increase its flexibility, it adopts software-defined radio solution.

www.qascom.it

Rakon - DUAL

This DUAL spaceborne multi-constellation multi-frequency COTS solution has been specifically designed for small to nano satellites. It incorporates two GNSS receivers to guarantee high availability and cold/hot redundancy. In addition, when working with 3 antennas, the system also provides full attitude determination of the spacecraft.

www.rakon.com

Septentrio - PolaRx5

PolaRx5 is multi-constellation multi-frequency receiver with advanced anti-jamming and anti-spoofing technologies. Developed specifically to support the most demanding applications for the earth science community as well as to densify GNSS reference stations, it features 544 channels for simultaneous tracking of as many signals as possible.

www.septentrio.com

Leica - GR50

The GR50 is Leica's top product for GNSS reference networks. It is a multi-frequency receiver featuring a GNSS engine with 555 channels that support all global GNSS constellations and augmentation systems. It also includes interference detection mechanisms and different layers of security to prevent unauthorised access to the receiver.

leica-geosystems.com

The mention of specific companies or manufacturers' products on this page is for informational purposes only and does not constitute endorsement, preference or recommendation by EUSPA. These references are intended solely to illustrate the relevant receiver categories (families), highlighting those that have recently been introduced to the market.

GNSS user receivers evolve hand in hand with general ICT developments

In the opening sections of the GNSS overview it is apparent how GNSS receivers' technology is evolving to meet growing demands for accuracy, resilience, and security. Coherently each of the five GNSS receivers' families presented in the previous sections benefits from these advancements, including the recent paradigm shift of GNSS systems providing services on top of pure signals in space.

Increased computing power enables increased MCMF and sensor fusion

As silicon miniaturisation allows greater compute power with lower energy consumption within a smaller physical footprint, GNSS user receivers have, and will continue to employ the technological gains in all receiver families to achieve the requirements for each new use case and optimise performance for existing use cases.

GNSS user equipment is rapidly evolving, driven by technological advancements that meet the growing demand for higher accuracy, better reliability, and availability. At the same time, the computing power available to even the most miniaturised GNSS chipsets is sufficient to process multiple constellations. Some use cases remain, and will continue to, where lower power consumption trumps all other design considerations. Across the different families, devices are becoming smaller and more integrated, especially in mass-market use cases like smartphones and wearables. This trend is enabled by **advances in semiconductor technology**, including sub-10nm chip manufacturing, which allows for **high performance in a compact form factor**.

The adoption of multi-frequency (e.g., L1, L2, E5) and multi-constellation (GPS, GLONASS, Galileo, BeiDou) capabilities is enhancing positioning data accuracy, availability, and robustness against interference and jamming. This is particularly crucial for professional non-regulated devices used in high-accuracy use cases, like agriculture, timing, and surveying. Integrating all these capabilities in the mass-market receiver families remains a challenge as **lower power consumption remains a top priority**. This is critical for devices embedded in wearables, IoT use cases, and other battery-powered devices. Special Applications and those in the professional receiver families are less impacted by this as the GNSS receivers are generally deployed attached to larger power supplies able to provide continuous operation. Geodetic monitoring devices are an example where long observation times are necessary to achieve higher accuracy levels and support long-term corrections.

The **jump from dual-frequency to triple**, or all frequencies (including E6 and the additional services it carries), substantially **increases system complexity and power consumption**, especially at the front-end. Simultaneously, the performance improvements from unlocked techniques such as Three-Carrier Ambiguity Resolution (TCAR) offer diminishing returns. As a result, triple or more frequency devices **remain the purview** of the **Professional Non-Regulated** family of receivers, and **Professional Regulated** receivers will remain mostly single-frequency until dual-frequency SBAS is realised. Sensor fusion continues to be an important feature, combining GNSS data with inputs from other sensors, such as **Inertial Measurement Units (IMUs) and accelerometers**, to enhance positioning availability. This approach is especially beneficial in environments with poor satellite visibility and is already used in navigation use cases within the aviation, road, rail, and maritime sectors. The integration of non-GNSS signals, like Wi-Fi, and mobile signals such as 4G/5G, continues to play a part in complementing GNSS positioning, especially in mass-market receiver families. These additional signals provide resilience and reliability in challenging environments where GNSS alone may be insufficient and allow fast fixing of position.

The hybrid **integration of GNSS with 5G networks**, while still in its early stages, represents a promising frontier. This integration aims to combine the high accuracy of GNSS with the low latency and high data throughput of 5G. Presently this is in the form of 5G providing a data channel, but indoor positioning through 5G may provide a strong complement to GNSS positioning in future.

Augmentation services such as **SBAS** and **RTK** networks continue to support the highest accuracy demands, and their **integration is widespread**. While single point positioning is still prevalent in many mass-market devices, there is a shift towards more sophisticated positioning techniques such as Real-Time Kinematics (RTK) and Precise Point Positioning (PPP), and moreover PPP-RTK, which combines the benefits of both approaches. Ultimately, this technique means **higher accuracy is becoming more accessible even for non-professional users**.

Processing techniques enhance performance and address vulnerabilities

Technological advancements are shaping the GNSS landscape by enhancing performance and capabilities across various use cases. Snapshot positioning is becoming increasingly common in mass-market devices, as it enables quick position fixes with minimal power consumption. Similarly, these devices are taking advantage of cloud-based solutions to offload computational tasks, reducing the burden on device processors. By **outsourcing complex calculations to the cloud**, devices with limited computational resources, such as IoT and wearables, can achieve accurate positioning **without compromising performance**.

This capability is **not limited to the mass-market**. Similar behaviours are observed in specialist use cases, such as those supported by receivers within the **special applications** family, where offloading receiver data for post-processing is standard practice. This approach has been employed in surveying applications for many years to improve the accuracy of results.

Multi-antenna processing is gaining momentum in both professional non-regulated and regulated receiver families due to its **accuracy improvements** and **mitigation against interference**. This technology is particularly valuable for manufacturers aiming to provide safe, secure, and reliable Position, Velocity, and Time (PVT) solutions in use cases where GNSS vulnerabilities are a major concern. Use cases such as power grid monitoring, connected and automated mobility, and communication network synchronisation are increasingly adopting these systems to ensure robust performance in critical environments.

Ongoing **R&D efforts to enhance the resilience** of GNSS are focused on improving the **reliability** of GNSS signals. In mass-market applications, this has been achieved by integrating multiple positioning sources with GNSS receivers. Advances in addressing natural threats, such as space weather, are now incorporated into many receivers. These include improved forecasting and monitoring capabilities, multi-frequency receivers equipped with advanced processing techniques such as carrier phase tracking, interference detection, and sophisticated error correction algorithms.

The professional regulated receiver family retains a high dependency on L1 single constellation. Future advancements aim to expand the benefits of new ionospheric modelling with multi-frequency and multi-constellation, particularly with the evolution of SBAS.

Secure SATCOM user technology overview

SECURE SATCOM OVERVIEW

INNOVATIONS ACROSS SECURE SATCOM SYSTEM SEGMENTS

SECURE SATCOM USER TECHNOLOGY TYPES

What is Secure SATCOM ?

Satellite communications (SATCOM) ensure end-to-end communications. Secure SATCOM ensures that end-to-end satcom communications are protected and monitored to achieve a certain level of confidentiality, integrity and availability standards (also known as the "CIA triad"). Secure SATCOM offers a layer of resilience and robust security features for guaranteed access to authorised users[1] only, no matter where the service or mission happens, and whether mobile or fixed. Three essential components are necessary to establish a SATCOM link between two or multiple users and/or user networks: the space segment, the ground segment, and the user segment. All these segments, in conjunction with the interfaces between them, allow for the transmission and relay of information from one user to another or from a user to a terrestrial network. Secure SATCOM enhances protection of each segment and their interfaces against interference, interception, and intrusion thus assuring availability, integrity and availability of the link and associated data transmitted through the overall system.

Secure SATCOM can be provided by any type of frequency band used by commercial satellite communications (COMSATCOM), government satellite communications (GOVSATCOM) or military satellite communications (MILSATCOM). Moving from COMSATCOM to MILSATCOM means an increase of security threshold for the provided SATCOM services. Usually, COMSATCOM services have the lower level of confidentiality and integrity, focusing on the availability of the service. GOVSATCOM services have a higher degree of confidentiality and integrity than COMSATCOM services. Moreover, MILISATCOM services are not only covering the three pillars of secure SATCOM principles, but they are enhancing the resilience and the reliability of the service to cope with the dynamicity of different types of attacks.

It is also worth mentioning **dual-use SATCOM systems**. These systems follow the general dynamic of making space SATCOM systems more flexible (software-defined satellites, or multi-orbit and interoperability features for ground segments/user terminals), offering one system capabilities for both types of users: civil and military. This dual use can come from a dual use of equipment inside the system, or the dual use at the system and network level. At the equipment level, it can be RF equipment with the ability to use civil and military frequencies, flexible modems that allow connecting to military and civil satellites, or the introduction of resilient features such as anti-jamming geolocators compatible with civilian and military frequency interferers, etc. The dual use at system and network levels also refers to the request to use civilian resources for military users, the incorporation of a dedicated core network for military purposes, or the development of separated payloads (civil and military) embarked in the same satellite that provides dual functions to military and civil users. The dual use is mainly between MILSATCOM and GOVSATCOM, and sometimes COMSATCOM and GOVSATCOM.

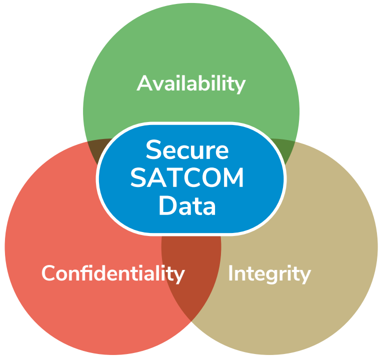
Secure SATCOM systems apply the three pillars of availability, confidentiality and integrity to address a wide area of missions and operational needs. The incursion of new technologies and the digitalisation of SATCOM systems open the door for new opportunities and challenges for secure SATCOM systems. These new opportunities also enlarge and allow for the emergence of new synergies with other space applications and systems (e.g. with GNSS or Earth Observation, seen in this report). Secure SATCOM services and technologies are also critical for the daily services of the EU economy in many vertical markets, for example in the domains of defence, security, humanitarian and emergency response, and diplomatic-related communications. They can be used as well in crisis management and coordination at the European and Member States levels.

SECURE SATCOM (Secure Satellite Communications)

Secure SATCOM is defined as satellite-based, one or two-way telecommunication service offering improved availability, confidentiality and integrity. It can be provided with any type of frequency band, by GOVSATCOM, COMSATCOM, MILSATCOM.

GOVSATCOM (Government Satellite Communications)	MILSATCOM (Military Satellite Communications)	COMSATCOM (Commercial Satellite Communications)
GOVSATCOM encompasses the communication services specifically tailored to meet the needs of governmental entities. This involves the deployment of satellite communication systems to ensure reliable, secure, and resilient communication for government operations, including defence, emergency response, public safety, and diplomatic communication.	**MILSATCOM** is a highly protected and guaranteed SATCOM, generally provided by military systems, offering highly assured and protected satellite communication capacity both in terms of nuclear hardening, anti-jamming/dazzle capacity and highly secure Telemetry, Tracking, and Command (TT&C), supplemented by an equally robust and resilient ground segment. The security and technology are highly specific and largely sovereign in nature.	**COMSATCOM** refers to SATCOM capacity and service provided on the global open market, for commercial purposes, generally with a degree of 'on-demand' access. These services usually have less stringent security requirements than GOVSATCOM and MILSATCOM and encompass a wide range of sectors, including telecommunications, broadcasting, internet access, maritime communication, aviation, and more.

SECURE SATCOM PILLARS[2]



Availability: The secure SATCOM system ensures timely and reliable access to and use of information.

Confidentiality: The secure SATCOM system preserves authorised restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

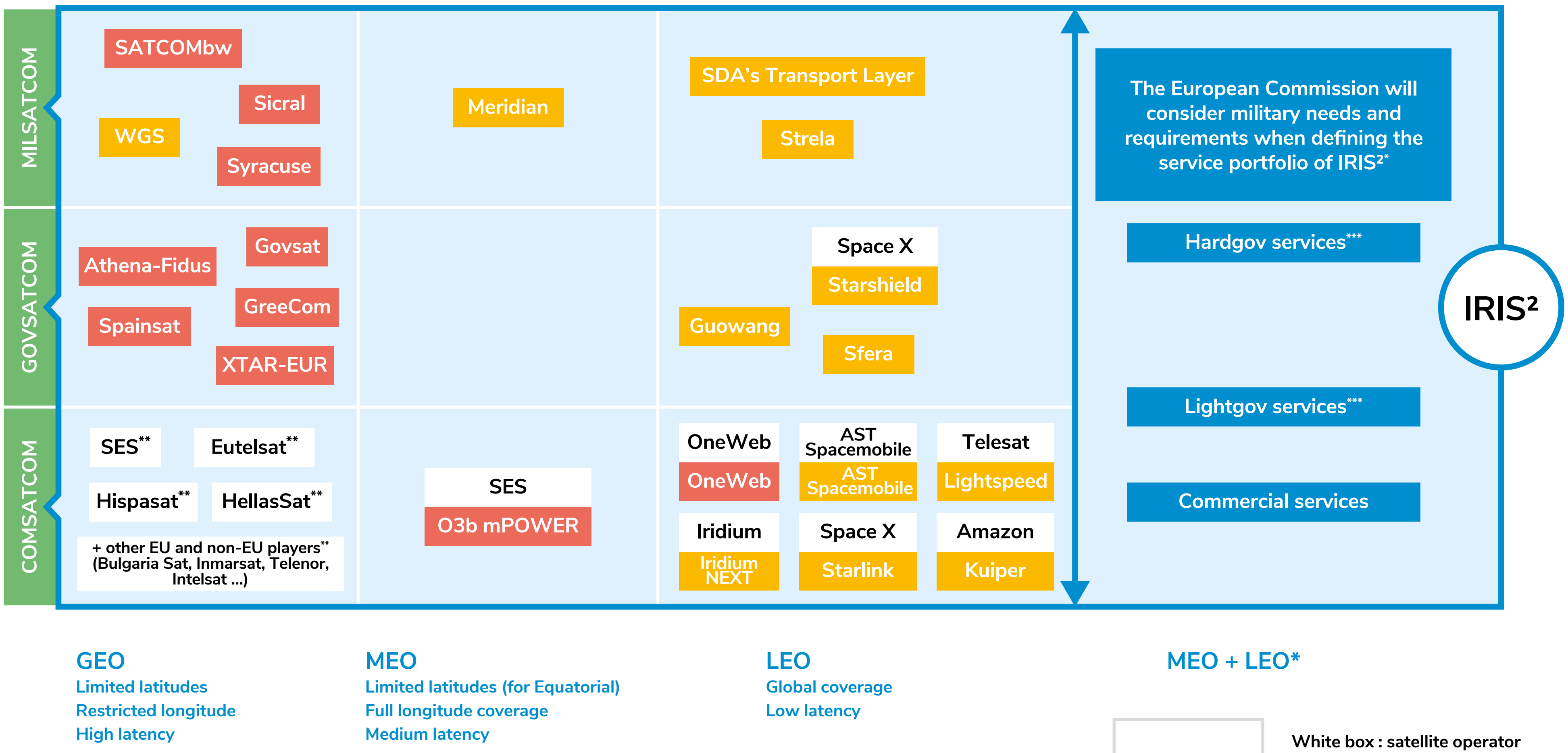
Integrity: The secure SATCOM system is protected against improper information modification or destruction and ensuring information non-repudiation and authenticity.

1: An authorised user is any appropriately provisioned individual who is permitted to access an information system.
2: Similar terms are used are used in the GNSS domain, but they are defined differently from the GNSS Key Performance Parameters which are defined in Annex 1A.

Back to main table of contents | Back to secure SATCOM user technology overview page

Secure SATCOM market analysis

The table below presents the positioning between IRIS² with respect to a selection of existing/future GEO/NGSO constellation systems. The list of GEO/NGSO constellation systems is not exhaustive and mainly focuses on NGSO high-throughput for FSS (Fixed Satellite Services) systems. It is also worth mentioning that the position of the GEO/NGSO systems in each box does not illustrate a potential ranking. IRIS² will be a multi-orbit constellation (LEO and MEO)* able to serve COMSATCOM, GOVSATCOM and MILSATCOM market segments. IRIS² will be able to fill the gap that space powers are pursuing.



White box : satellite operator

Red box : European GEO/NGSO system

Orange box : Non-European GEO/NGSO system

* European Commission, 10 March 2023, European Union Space Strategy for Security and Defence, and European Commission, 16 December 2024, Commission takes next step to deploy the IRIS² secure satellite system.

** For those satellite operators, we mean their satellite fleet can be used to provide satellite communications services.

*** The IRIS² infrastructure shall comprise a multi-orbit constellation system. The IRIS² infrastructure will be composed of two components to serve both governmental and commercial services: a) **Governmental infrastructure** called "Hardgov", (whose assets would be owned by European Union) dedicated to deliver strengthened governmental services and b) **Commercial infrastructure**, called "Lightgov", (not owned by the European Union) able to provide services to governmental users and commercial services.

Overview of the secure SATCOM user segment

The user segment and its importance for secure SATCOM

Before examining the technological trends and user types stated, a general overview of the segment and its architecture is provided on the following page. As an introduction, it is necessary to highlight the **importance of the user segment** in shaping the secure SATCOM requirements and functions.

The user segment of a SATCOM system connects the users, through ground-to-space links, to the space segment of a SATCOM system. In the case of a secure SATCOM system, this connection should **ensure the fulfilment of the secure SATCOM system requirements**. These requirements must consider the ground segment, as recognised in Regulation (EU) 2021/696 of the European Parliament and of the Council, dated 28 April 2021, establishing the Union Space Programme and the European Union Agency for the Space Programme (EUSPA).

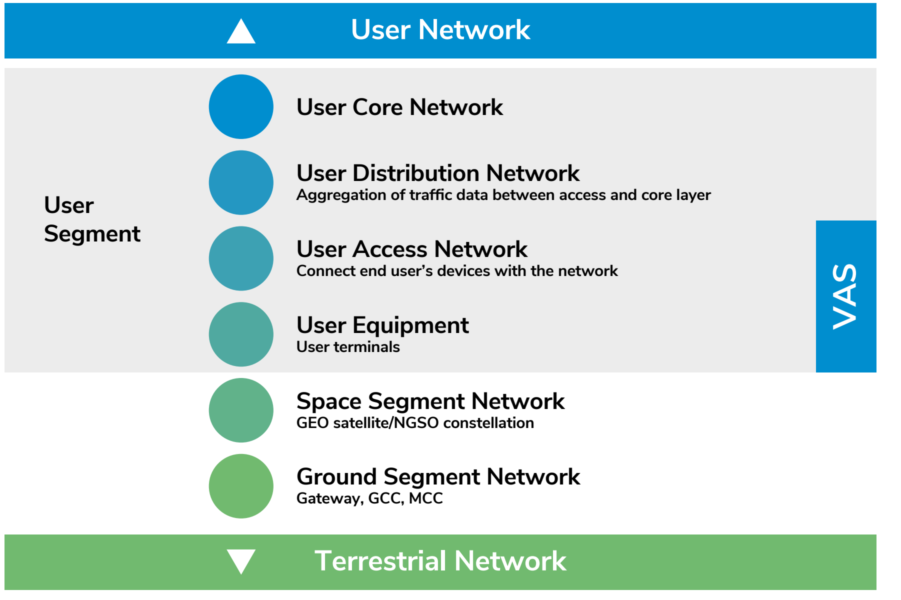
In SATCOM systems, including secure ones, the **user segment, like ground and space segments, represents a possible gateway for attackers** aiming to compromise SATCOM networks. Intrusions into the user segment allow attackers to move horizontally and vertically in the SATCOM network. Thus, they enable the attacker to affect other portions of the user segment SATCOM network or even gain access to the space segment of the SATCOM network. An example of one of these types of attacks is the February 2022 Viasat KA-SAT network cyber-attack[1], which started through a ground-based network intrusion that managed to obtain remote access to the trusted management segment of the KA-SAT network, using it to access and execute legitimate management command on a large number of residential modems in Ukraine and the rest of Europe. These management commands consisted of destructive commands that overwrote key data on the modems, rendering modems unable to access the network, and thus disconnecting them from Viasat's KA-SAT network. For these reasons, it is crucial that **secure SATCOM systems carefully address the vulnerabilities and challenges introduced by the user segment to protect the overall system**.

The user segment connects user networks with the secure SATCOM network via secure SATCOM user terminals. However, this network linkage introduces potential vulnerabilities that must be mitigated to maintain a secure SATCOM environment. While ensuring that different users in various scenarios can reliably connect to the network, the system must also guarantee the availability of secure SATCOM services.

The Secure SATCOM user segment encompass the user terminal component. Very different SATCOM user terminals can support secure satellite communications providing enhanced confidentiality, integrity and availability. In the frame of this report, **three user technology types** have been define covering the vast majority of the available secure SATCOM terminals: a) On-The-Move/On-The-Pause (OTM/OTP); deployable, handheld and secure IoT; and fixed and backhauling. See the dedicated section starting on page 71 for the characterisation of these categories, their main features related to the user operations, and their evolution trends.

1: Source: https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview

USER SEGMENT AT THE HEART OF THE END-TO-END NETWORK



User segment hierarchical network layers

The user segment consists of the user equipment (i.e. user terminals) plus the following three user segment network layers:

- **Access network** connects end-user devices with the network, providing the physical and logical interface between the user equipment and the distribution layer. The access network contains the secure SATCOM user terminals and their interfaces to the distribution network.
- **Distribution network** is responsible for aggregating traffic data between the access layer and the core layer. It provides connectivity, manages network traffic, and ensures security and quality of service features. The distribution network contains components such as routers and switches.
- **Core network** transports traffic between sites and networks. It also manages network systems, and monitors, and controls network performance. Examples of technologies in the core layer include Multiprotocol Label Switching (MPLS) and Virtual Private Networks (VPNs).

In addition to these network layers, a value-added service (VAS) layer is often provided by secure SATCOM providers to offer comprehensive support. This layer typically includes integration, installation, and maintenance of the user segment, along with support for user hardware and software components, such as user terminals or Application Programming Interfaces (APIs). Space and Ground Segment Networks are not addressed in this report.

Building blocks of secure SATCOM user terminals

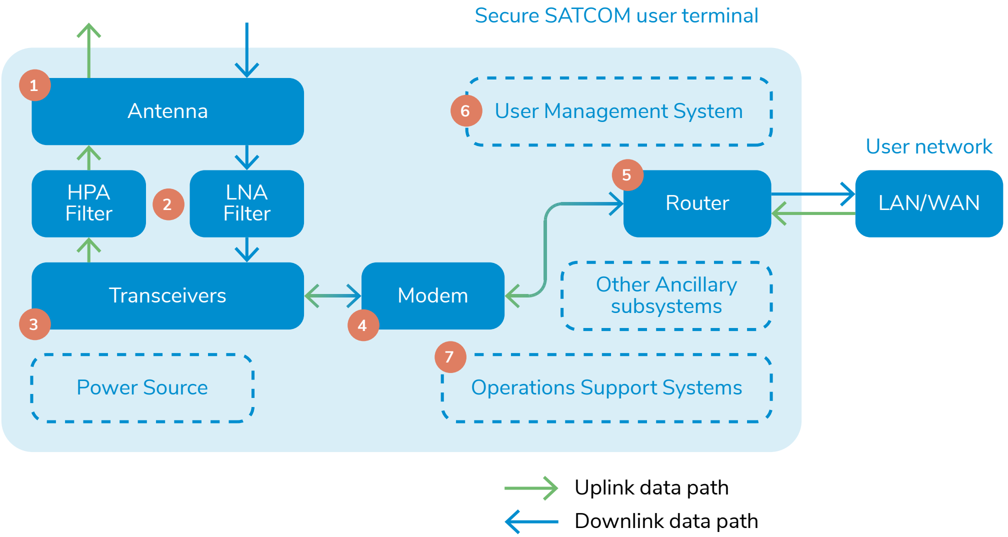
In the user segment of a secure SATCOM architecture, the main component remains the user terminal (otherwise referred to throughout the report as terminal) since it is ensuring the transition between RF and the network. Secure SATCOM user terminals are devices that enable communication services through the SATCOM system, typically enabling one or two-way communications by establishing and managing ground-to-space links (uplink & downlink) between the user and the SATCOM network.

User terminal functional requirements

The design and functionality of terminals vary based on the user's operational needs, associated services, installation, and technical features. The categorisation of SATCOM terminals is explored in greater detail in the user technology types section (pages 70 to 96) of this report. This section, however, focuses on the **basic components and building blocks of a SATCOM terminal**, building on the concepts introduced in the EUSPA Secure SATCOM Market and User Technology Report 2023.

In the context of secure SATCOM, terminals play a critical role in ensuring the **confidentiality, integrity, and availability of the system** from the user's perspective. This is achieved by ensuring that the user segment comply with the overall secure SATCOM system requirements. To this direction, the user terminal must align with secure SATCOM network standards to create a fully secure connection environment both for the user uplink & user downlink which are key entry points for attacks targeting both the user and space segments.

GENERAL ELEMENTS IN A SATCOM USER TERMINAL



SECURE SATCOM USER TERMINAL

It is the user's device that allows connection to the SATCOM systems. It is the main component of the access layer. User terminals vary in function of the user needs and SATCOM systems. It typically consists of several pieces of RF equipment, network and signal processing, and ancillary systems. In addition, it includes a power source and user interfaces. The basic components of a user terminal are:

RADIO FREQUENCY EQUIPMENT	1	Antenna	For the transmission and reception of signals between the terminal and satellites (through ground-to-space links). The antenna must operate at the satellite signal frequency and have the ability to point accurately toward the satellite.
	2	RF Front End	The RF Front End is composed of amplification and filtering functions. An amplifier boosts the strength of the RF signal and is used both on transmission path (HPA) and reception path (LNA). The filtering function is to pass or reject specific frequencies and attenuate unwanted signals to clean transmission and reception.
	3	Transceivers	The transceiver adjusts the signal levels of radio frequency (RF) and performs frequency conversion between the RF band and a lower frequency band. It combines a transmitter and a receiver into a single unit. It also includes necessary filter functions.
NETWORK AND SIGNAL PROCESSIONG	4	Modem	The modem performs the signal synchronisation, the coding and decoding, the interleaving and de-interleaving, the mapping and de-mapping, the composition and decomposition of the physical frame, and the modulation and demodulation. The modem is also responsible for conversion of digital to analogue and vice-versa at the interface with the RF equipment.
	5	Router	Routers manage data flows between the different devices in the SATCOM network, connecting terminals, modems, and other networks (such as LAN-Local Area networks or WAN-Wide Area networks) to the satellite network. They are the essential components of the distribution layer.
ANCILLARY SUBSYSTEM	6	User Management System	This system ensures that the user has the proper authorisation to access the system. It controls the authentication and accounting of users accessing the SATCOM system. This system is of high importance for secure SATCOM terminals, highly linked to the integrity of the system.
	7	Operations Support Systems	This system monitors the system's performance, identifying and resolving any issues. This system is of high importance for secure SATCOM terminals, highly linked to the availability of the system.

Secure SATCOM user technological factors and the digitalisation trend

The current user technological factors for secure SATCOM, their evolution, and their impact on the secure SATCOM principles are key to understand the consequences that there may be for the secure SATCOM users. One of such technological factors is digitalisation, which led to Software-Defined Satellite (SDS) and Software-Defined User Terminal (SDUT). These have become in recent years important technologies for the provision of secure SATCOM, as they clearly ease the field operations and enhance the end user terminal management.

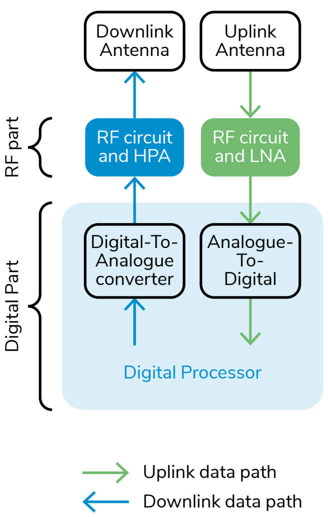
A major trend in the overall SATCOM sector: digitalisation

The increasing use of software-oriented solutions is one of the major trends in the overall SATCOM sector. Secure SATCOM systems are logically impacted by this trend, which is not only digitalisation, but it can be considered as the main one. It implies that the secure SATCOM systems (ground, space, and user terminal) are evolving from legacy hardware-centred concepts and systems toward new software-oriented solutions. Among these new solutions, Software-Defined Satellites and Software-Defined user terminals, along with their features, have a significant impact on the user segment.

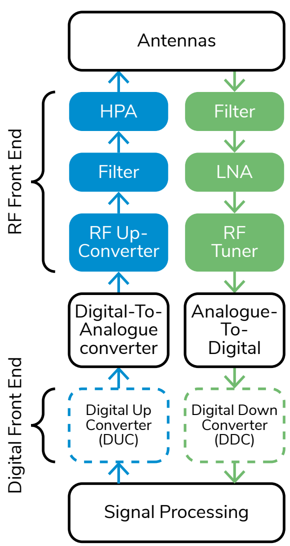
Software-Defined Satellites

SDS are satellites with a single design that can be configured for different types of missions, depending on the satellite operator's needs throughout the satellite's lifetime. SDS reduce the need to tailor the design of the satellites and define the mission several years in advance. In addition, SDS allow the satellite to be adapted to the demand in real time. They also gave operators the option to reconfigure their satellites over their lifetime. A SDS can adapt to the evolving needs and requirements of the different user market segments.

SDS Payload schematics



SDUT logical schematics



SDS are capable of optimising capacity or being adapted to minimise interference or jamming, making the overall secure SATCOM systems more resilient, available, and reliable throughout their lifespan.

SDS have key benefits to the end user with more optimised capacity available and easiness of end user specificities integration.

SDS state-ot-the art: flexibility in coverage, power allocation, and frequencies

This flexibility allows **for modifications to coverage, power** (which is generally closely related to bandwidth allocation), and frequency (with flexible channeL-bandwidth and centre frequencies); such flexibility is possible thanks to **Electronically Steerable Antennas** (ESA), digital beamforming, beam hoping, and Digital Processors (DPs). The ESA allows the satellite to dynamically reconfigure its coverage, power, and frequency in real-time by combining large arrays of smaller antenna feeds and pairing them with Digital Signal Processors (DSP) that control the amplitude and phase of each channel. Dynamic channelisation and routing between beams, enabled by DPs, allow the satellite to be adapted across various coverage areas. This flexibility enhances secure SATCOM systems with features like interference or jamming avoidance and assured access when high capacity is needed in a specific geographic area.

SDS future capability: flexibility to accommodate many air-interface protocols

This flexibility is mostly defined as the ability of a satellite to use different protocols such as Digital Video Broadcasting second-generation satellite extension (DVB-S2X), or 5G. This feature is essential for the interoperability of the space segment with user terminals or ground networks. In the case of secure SATCOM, this flexibility enables the SDS to maintain a highly reliable and secure communication protocol over the satellite's lifespan. The key equipment hosting this feature is the Regenerative On-Board Processor (OBP).

Software-Defined User Terminal

SDUT is based on software-defined wireless protocols that support various features and functionalities. SDUT can be updated and upgraded without change to the user terminal hardware. Today there are user terminals that are partially or completely SDUT based. SDUT enables network interoperability, adaptability to future updates and protocols, and lower hardware development costs. These qualities make SDUT a relevant component for the secure SATCOM user segment. The SDUT architecture can be divided into three main parts:

- **RF front end**: This is an RF circuit used to transmit and receive signals. It typically operates at various frequencies and links different antennas (to cover a broader range of frequencies) with the Analogue-to-Digital and Digital-to-Analogue converters. In this part, the signal is analogue and follows the traditional processes of amplification, modulation, and conversion in RF transmission and reception paths.
- **Analogue-to-digital or digital-to-analogue conversion**: This process converts analogue (continuous-time) signals into digital (discrete-time, binary-coded) signals. Converters are continuously advancing, focusing on optimising energy consumption and improving conversion performance.
- **Digital front end**: This part performs two primary functions: Sample Rate Conversion (SRC) and channelisation. SRC synchronizes communications, while channelisation includes up/down conversion, channel filtering, and interpolation or low-pass filters for the transmitter and receiver sides, respectively. The digital front end links the RF front end with the signal processing units. New SDRs employ Direct RF Sampling (DRFS), which moves signal processing entirely to the digital domain, eliminating the need for mixers, local oscillators, or filters in the hardware.

Multi-orbits, multi-constellations, multi-frequencies and interoperability

The use of multi-frequencies – e.g. Ku- and Ka-band – improves the user segment security, and especially its availability. Multi-orbits and/or multi-constellations connections can further improve the secure SATCOM characteristics. These capabilities multiply paths for the flow of secure SATCOM information and data. Those concepts are still at their early stage.

To support multi-connectivity, the user terminal should offer flexible features. RF flexibility (with flat panel antenna technologies such as passive analogue, active analogue or active digital) enables multi-frequency band, multi-orbit and multi-constellation operations, while flexible modems can support the multiple waveforms that could be required by different constellations. These flexible user terminals would be designed to work within new advanced architectures, allowing terminal providers to extend their core capabilities to meet the emerging challenges of satellite communications: delivering transparent secure SATCOM services using multiple space assets integrated into different space networks. These capabilities are made possible through the development of interoperability and standardisation within the user segment and ground-to-space interfaces.

Multi-orbits: available today

The driving force behind the concept of ‘multi-orbits’ is that **operators can provide their customers with the advantages of all orbits in a transparent way**. From an end-user perspective, multi-orbit is defined as the ability to work concurrently (simultaneously or not) with space assets from different orbits and/or move seamlessly from satellites flying in one orbit to satellites flying in another. Non-Geostationary orbit (NGSO) constellations offer low latency, which is necessary for low latency applications (e.g. videoconferencing), while GEO satellites provide greater capacity in specific geographical areas than a constellation alone. Several geostationary (GEO) satellite operators have indicated that they have a strategy for NGSO constellations, where GEO satellites are combined with NGSO systems to deliver services that leverage the strengths of both GEO and NGSO satellites.

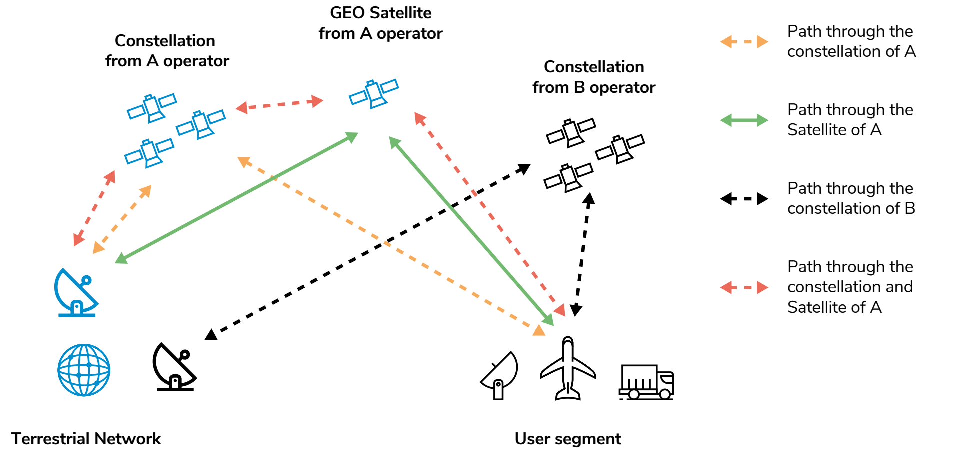
Multi-constellations: emerging capability

The multi-constellation capability is similar to multi-orbit but focuses on taking advantage of the different secure SATCOM services offered by various constellations rather than different orbital characteristics. Multi-constellation capability relies on the user terminal's **ability to switch between constellations based on any performances trigger** of the transmitted traffic or as a resilience measure. For instance, if constellation A is suitable for a certain secure SATCOM traffic with specific security requirements, but the traffic changes and requires additional security measures, constellation B may be selected to handle the new traffic and meet the enhanced security needs. Alternatively, if constellation A experiences low service availability due to attacks on its network, the user terminal can switch to constellation B to maintain service availability. Secure SATCOM user terminals designed for multi-orbit/multi-constellation operations enable the use of different space networks with seamless handovers between satellites in different orbits or constellations, This improves the availability of service for user terminals operating within a single, unified multi-orbit and multi-constellation network.

Multi-frequencies: the holy grail

The ability to use different frequencies within a single user terminal is essential **not only for enabling multi-orbit and multi-constellation capabilities** (since these systems typically operate on different frequencies) but **also as a resilience measure to avoid jamming and interference**. Techniques such as frequency hopping require the capability to operate across multiple frequencies within the same secure SATCOM system. Versatile antennas capable of operating at different frequencies are essential for enabling multi-frequency capabilities in secure SATCOM terminals.

SECURE SATCOM MULTI-PATHS CONNECTIVITY USING MULTI-ORBITS, MULTI-CONSTELLATIONS AND/OR MULTI-FREQUENCIES CAPABILITIES



Standardisation for interoperability

In a multi-vendor and multi-network environment, standardisation to ensure interoperability is crucial. According to ETSI, interoperability is "the ability of two (or more) systems or components to exchange data and use information“. When referring to user terminals for secure SATCOM systems that may be multi-orbits, multi-constellations, or multi-frequencies, interoperability is therefore a requirement. This interoperability can only be ensured if the following aspects are considered:

- **Interfaces and architectures definition** must be fully defined to allow interoperability. The hybrid space architectures, which are proposed by these new secure SATCOM approaches, are a system of systems whereby each segment needs to be coordinated with the others, with integration at subsystem, components, and even human operators level.
- **Specifications are to be properly designed**. The specifications associated with the architecture and interfaces should be designed along with them.
- **Robust, flexible, and efficient protocols** should be favoured so that they are capable to evolve and adapt to changing communications and data. The specified data format and encodings should be unambiguous allowing for better integration with the communication protocols.
- **Specifications are maintained and used in a fully understood context**. The stability of specifications is also a key factor in interoperability. This stability is tied to a clear understanding of the context in which the specifications are being designed. Ensuring that the requirements capture essential parameters that remain stable will facilitate interoperability.

High Throughput Satellites and micro/small satellites

High Throughput Satellites: high level advantages and drawbacks

Emerging around the mid-2000s, High Throughput Satellites (HTS) are designed to **offer large capacities (up to dozens or hundreds of Gbps) for bidirectional broadband communications using small user terminals**, making them **well-suited for broadband internet access**. HTS systems provide greater throughput capacity compared to traditional Fixed Satellite Services (FSS) for the same amount of allocated frequency in orbit. This enhanced performance is achieved by dividing the service area into multiple smaller spots, allowing for higher frequency reuse across the service area and utilising the resulting satellite gain to deliver more capacity from a given satellite resource. HTS are typically following a star network architecture, where the satellite facilitates direct connections between user beams and gateway beams. This configuration might require a dual-hop for user-to-user communications (i.e. from the first user to the satellite, then to the ground station, and from the ground station back to the satellite and second user).

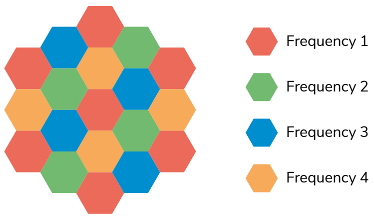
The multi-spot system in HTS enables the use of **smaller satellite antenna spots to increase antenna gain**, which improves the gain-to-noise temperature ratio (G/T) and Equivalent Isotropically Radiated Power (EIRP) over larger bandwidths and service areas, while also reducing user terminal size. This facilitates the implementation of smaller user terminals that can achieve high throughput capacity with the satellite. The high throughput of these smaller user terminals enhances the availability and resilience of secure SATCOM systems, making them more adaptable to various use cases and scenarios. The system's ability to handle traffic peaks and increased demand for secure SATCOM is also improved.

The HTS's multi-spot system has **two main features** which are **the frequency reuse factor** and **the number of beams**. Both allow HTS to have more capacity per beam and total system capacity. However, there are a few considerations to take:

- **Spot beams and co-channel Interference**: While spot beams enhance spectral efficiency, adjacent spot beams operating on the same frequency can cause interference, reducing efficiency.

- **Frequency reuse factor**: This term refers to how often a frequency is reused to generate high power cells to generate a wider beam/coverage. The goal is to maximise the overall capacity usage with frequency re-use, typically denoted as "colour" (see right schematic). A common value is 4, which avoids overlapping of the same colours, though some antennas require a higher number to reduce inter-beam interference.

FOUR-COLOUR FREQUENCY RE-USE EXAMPLE



HTS technological evolution

HTS technologies will benefit from advancements in digitalisation and artificial intelligence (AI), particularly for optimising HTS payload processes. Flexible payloads, combined with AI, can enhance processes such as beam hopping, traffic handling, capacity optimisation, beamforming, anti-jamming, and interference avoidance. The impacts of AI on secure SATCOM are discussed in more detail on page 65 of this report.

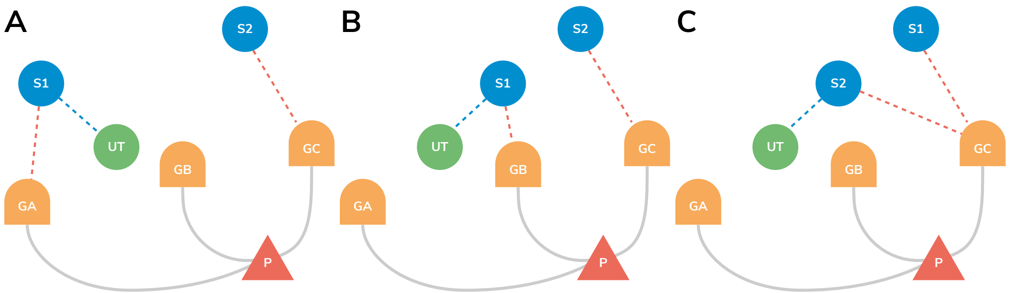
Micro/small satellites in mega-constellations: managing space mobility

Mega constellations use a large number of satellites to form a star network. They can be configured to also support mesh for some very specific users. **Traditionally, terrestrial mesh networks were employed for governmental applications** to establish ad hoc local base stations. The advent of massive Low Earth Orbit (LEO) constellations introduces new topological requirements and opportunities. A star space network enhanced by Inter-Satellite Link (ISL) is an efficient way to minimise the ground segment footprint, enabling secure communications without requiring a direct line of sight to a gateway or returning to the ground. Additionally, it can provide lower-latency communications due to the constellation's geometry and the ability to create more direct paths between two points.

Micro satellites or small satellites are integral to mega constellations and star networks with ISL, **serving as network nodes that can route data and traffic**. In large mega constellations networks using optical ISL, regenerative processors are essential for routing capabilities. Unlike transparent processors, which are limited to spectrum and beam management, regenerative processors demodulate and decode uplink signals towards the satellite before encoding and remodulating them to route the traffic towards the users/gateways or a neighbour satellite.

The primary challenge for mega constellations is ensuring seamless data transmission throughout the network (as illustrated in the schematic below), **which is influenced by ISL and roaming aspects**. Details on ISLs are discussed on page 64 of this report. Roaming and satellite movement involve handovers, which must be seamless to maintain secure SATCOM availability and data flow integrity. Handovers can be executed in 'break-before-make' mode (link interruption with the need to establish the next link within a few tens of milliseconds) or 'make-before-break' mode (preparing the next link in advance).

ROAMING CONCEPT ILLUSTRATION



In Step A, the user terminal (UT) is served by Satellite 1 (S1), which is connected to Gateway A (GA) and, via ground fibre, to Point of Presence (PoP) P. In Step B, Satellite 1 moves closer to Gateway B (GB) and roams to it. In Step C, the UT roams from Satellite 1 to Satellite 2 (S2), which is now in a better position. All these events occur within a span of a few seconds. The blue line represents the connection between the serving satellite (indicated by blue dots) and the UT (marked by a green dot). The red lines depict the link from the satellites to the gateways (marked by orange).

Cyber and signal threats

SATCOM systems and infrastructure are facing an exponential increase in the number of attacks

Of the three Secure SATCOM pillars, integrity and availability are **the primary targets of cyber and signal threats but confidentiality is becoming more and more at risk with increasing complexity of attacks profiles**. Since the 1970s, cyberattacks against the space sector, especially SATCOM systems and infrastructure, have increased sharply. Signal threats to GEO SATCOM systems began in the 1980s and 1990s with incidents of signal hijacking. **Signal jamming** emerged in the late 2000s and early 2010s for GEO SATCOM services. Concurrently, cyber threats evolved, with Distributed Denial-of-Service (DDoS) and Advanced Persistent Threat (APT) attacks becoming prominent. Since early 2020, both signal and cyber threats have intensified, with incidents such as In-Orbit Eavesdropping (IOE), LEO jamming, and malware attacks. **The year 2022 marked a significant milestone, as military conflicts highlighted the convergence of signal and cyber threats to space SATCOM systems**, exemplified by the Ka-Sat cyberattack and the Starlink jamming. Since then, the frequency of cyberattacks against space systems has doubled annually, a trend likely to continue amid growing geopolitical tensions. The major threat trends from 2022 onward include the diversification of targets and increasing complexity of attacks. Attackers now tend to launch more complex and widespread attacks against various assets and stakeholders, including secure SATCOM systems.

The difference between cyber threats and signal threats are the following:

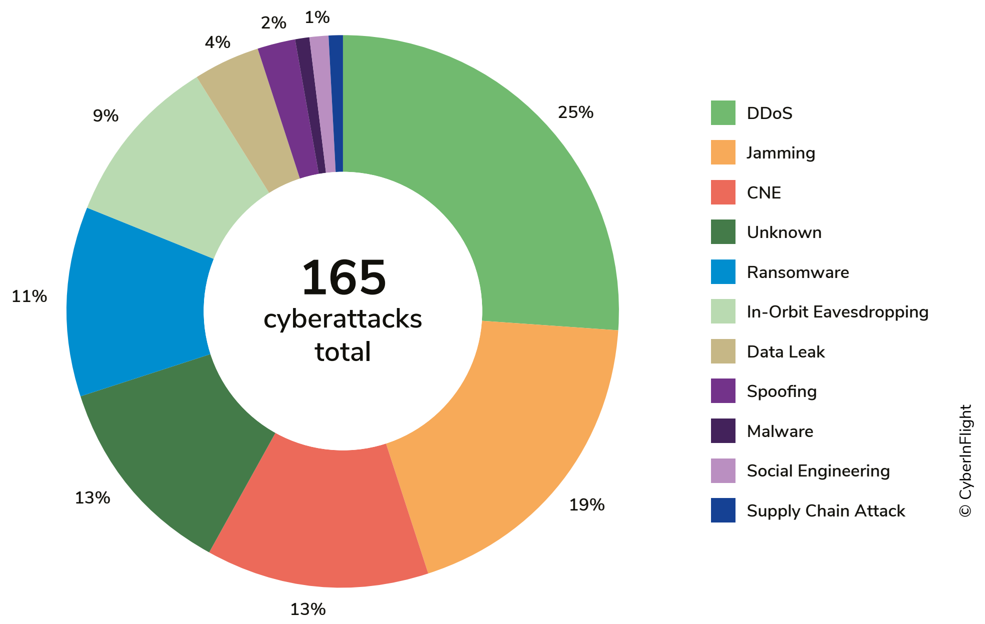
- **Cyber threats** involve **malicious attempts to disrupt computer systems or networks by stealing data, disrupting communication links, or compromising systems**. For secure SATCOM, cyber threats target the software of user, ground, and space segments. Common cyber threats include Advanced Persistent Threats (APT), Computer Network Exploitation (CNE), Distributed Denial-of-Service (DDoS) attacks, data leaks, malware, phishing, ransomware, social engineering, supply chain attacks, and wipers.
- **Signal threats** refer to threats **targeting the RF ground-to-space and space-to-space links used between space, ground, and end-user segments**. In secure SATCOM, signal threats affect the system's confidentiality integrity and availability. Common signal threats include eavesdropping, hijacking, In-Orbit Eavesdropping (IOE), In-Orbit Spoofing (IOS), jamming, and spoofing.

Key takeaways of the threat evolution

Three main reasons can explain the rapid growth of attacks against SATCOM systems and infrastructure since the 1970s. First, the New Space approach has brought new SATCOM players into the market, expanding the attack surface with more potential systems to target than before. Moreover, the increasing integration of SATCOM players into the cloud allows for more connectivity and potential paths for an attack. Second, from an attacker's perspective, SATCOM systems and infrastructure tend to be more targeted due to a democratisation of hacking skills and techniques. Third, attacks are more visible to the general public due to increased tracking and monitoring capabilities and also due to more open communication from hacker groups, notably on social media such as X or Telegram. Since the 2020s, many public and private actors, civilian and military, have been closely monitoring and tracking the evolution of the threat landscape. These reasons can also explain the sudden increase of observed cyberattacks since 2022-2023.

Since the onset of the war in Ukraine, there has been **a notable increase in ground-based jamming and spoofing targeting LEO SATCOM services. The complexity of these interference attacks has significantly risen**. The deployment of new generations of intelligence satellites in GEO has accelerated incidents of In-Orbit Eavesdropping and In-Orbit Spoofing, threatening the data confidentiality and integrity of GEO SATCOM systems. To combat these threats, secure SATCOM systems must develop and deploy anti-jamming and anti-spoofing techniques and technologies, such as power limiters, automatic level control loops, frequency hopping, nulling antennas, spread spectrum techniques, and tactical modulation methods.

EVOLUTION OF THE NUMBER OF ATTACKS AGAINST THE SPACE SECTOR (JANUARY 2022 – JULY 2024)



From detectable to insidious consequences for users

Threats targeting the availability of the Secure SATCOM service to the end user are a detectable situation since the effect is a **decrease in service quality up to a complete loss** of it (including incapacity to connect without changing the hardware).

Threats targeting integrity and/or confidentiality are more insidious to the end user. In those situations, **the user may not detect that his system is under attack**. He may collect data that has lost its integrity with potential consequences related to the associated use of this data. Also, its system may have been corrupted and confidential information are collected by a third party seamlessly.

Technologies improving resilience to cyber and signal threats

The table below presents a list of cybersecurity technologies and signal techniques that secure SATCOM systems can use to become more resilient to cyber and signal threats. The applicability of these technologies and techniques to the different SATCOM segments (ground, space, and user) depends on various factors. Some technologies may be relevant to certain segments but will need further development as threats evolve. Others can be applied directly from other domains (such as computing and terrestrial telecommunications) without technical adaptation to secure SATCOM systems. This table is not an exhaustive list of cybersecurity technologies and signal techniques; rather, it serves as an example of how secure SATCOM systems can address these threats. More details and a complete list of these technologies can be found in the Space-Shield Framework.

APPLICABILITY PER SEGMENT

	Ground	Space	User
Applicable			
Not applicable			

Cybersecurity technologies	Cybersecurity technologies context description	Cybersecurity technologies applicability to secure SATCOM: Ground	Space	User	Related threats
End-to-end network encryption via certified cryptographic protocols with a secured key management lifecycle	There is a growing need to maintain the confidentiality of sensitive data exchanges over SATCOM networks.	Applicable	Not applicable	Applicable	Eavesdropping & in-orbit eavesdropping
Endpoint detection and response (EDR) tools	The limited resources of SATCOM organisations mean that cybersecurity operations must be rationalised. EDR tools contribute to this logic.	Applicable	Applicable	Applicable	Endpoint compromise takeover
Firewall, Access Control List (ACL), and Network Segmentation Rerouting, filtering	DDoS attacks are growing in scale, and anti-DDoS technologies are an essential requirement for maintaining high-performance SATCOM systems and infrastructures.	Applicable	Not applicable	Applicable	DDoS attacks
Hot, warm, or cold backup site implementation Storage replication, disk mirroring	Securely backing up data according to an established process helps mitigate the effects of ransomware or wiper attacks.	Applicable	Not applicable	Not applicable	Ransomware & wiper
Intrusion detection and prevention systems (IDS/IPS System)	Detection needs stem from the growing surface area of cyberattacks.	Applicable	Applicable	Applicable	CNE attacks
Robust patching and system configuration audits	To prevent the emergence of vulnerabilities, systems are updated.	Applicable	Applicable	Applicable	Malware infection
Security Operation Center (SOC)	The complexity of SATCOM operations calls for the constant unification of cybersecurity technologies and resources.	Applicable	Not applicable	Not applicable	Vulnerabilities & zero day
SIEM (Security Information Event Management)	As data flows within and outside organisations grow, so does the need to visualize potential threats.	Applicable	Not applicable	Not applicable	APT attacks & CNE
TRANSEC measures (spread spectrum, multiple frequencies, burst coding, frequency hopping)	Jamming and spoofing attacks against SATCOM systems and infrastructure make organisations slowly tend to enhance their resiliency to ensure secure data transfer and communications.	Applicable	Applicable	Applicable	Jamming & spoofing
Virtual Private Networks (VPN)	Attempted Man-In-the-Middle attacks accelerate the widespread use of VPN technologies in SATCOM operations.	Applicable	Applicable	Applicable	Eavesdropping & Man-In-the-Middle
Virtualisation, segregation, container	The development of defense-in-depth enhances overall resilience.	Applicable	Applicable	Applicable	Satellite control takeover
Future-oriented cybersecurity technologies such as Quantum Key Distribution (QKD) or Post Quantum Cryptography (PQC)	The development of threats capable of making most cybersecurity technologies obsolete calls for developing technologies such as QKD or PQC, to address these challenges.	Applicable	Applicable	Applicable	Future quantum threats

Cybersecurity ecosystem in Europe

The European space cybersecurity ecosystem

The European space cybersecurity ecosystem comprises over 150 corporate players that have publicly announced their space cybersecurity activities, along with an additional 30 institutions that complement this robust ecosystem. **The sector has been expanding steadily in recent years, driven not only by an increase in threats and attacks but also by the growing budgets of various institutions and the heightened importance of cybersecurity**. European institutions, through programmes such as Digital Europe and Horizon Europe, are fostering the development of projects to enhance the ecosystem, strengthen cybersecurity coordination, stimulate quantum integration, and standardise cybersecurity features in space systems. These efforts positively impact secure SATCOM systems, which benefit from enhanced cybersecurity and greater resilience against attacks and threats.

The European space cybersecurity regulatory ecosystem

Several European institutions, including **the European Commission, the European Cooperation for Space standardisation (ECSS), the European Union Agency for Cybersecurity (ENISA), and the European Space Agency (ESA), have started developing a comprehensive set of European space cybersecurity standards**. These key organisations have introduced several general frameworks applicable to SATCOM, such as the EU Space Strategy for Security and Defence, the European Space Law (EUSL), the EU Network and Information Security Directive (NIS) v2, and specific ECSS standards like ECSS-E-ST-80C – Security in Space Systems Lifecycles. Additionally, a new trend is emerging with space cybersecurity frameworks that focus specifically on SATCOM, such as ENISA's LEO SATCOM Cybersecurity Assessment, the METI Guideline, IT-Grundschutz, and the LOS.

Focus on information sharing in the light of secure SATCOM

Sharing information is crucial for maintaining consistent cybersecurity in secure SATCOM systems. This can be achieved through various communication channels, such as a Computer Emergency Response Team (CERT), an Information Sharing and Analysis Centre (ISAC), and an exchange group.

The EU Space Strategy for Security and Defence, announced in 2023, includes the creation of an EU Space ISAC. The EU Space ISAC aims to facilitate collaboration, awareness, and best practices among private entities to ensure the security of space systems and their dependent networks. The European Union Agency for the Space Programme (EUSPA) oversees this European ISAC and is responsible for bringing together private entities from the European space sector, along with universities and European and national institutions from member countries.

The network-based information-sharing platform **European Space ISAC** was launched on April 24, 2024, with an inaugural meeting of its 12 founding members (Airbus, CyberInflight, GMV, Infodas, Leonardo, OHB, Osmium, Priamos, Prométhée, Satlantis, Technobit and Thales Alenia Space). These founding members are required to dedicate time, resources, and expertise to the initial stages of development. The EU Space ISAC's mission is to contribute to the security and resilience of space systems and their supply chains. To achieve this, EUSPA and the European Commission have identified several information-sharing and best practice objectives, including establishing efficient and secure communication channels, facilitating feedback and experience sharing among members, enabling European collaboration, and providing resources and support to its members. The EU Space ISAC is not intended to be an incident response body. Instead, responding to security incidents will remain the responsibility of each individual member.

MAP OF THE EUROPEAN SPACE CYBER ECOSYSTEM AND MAJOR INSTITUTIONS

The map shows the headquarters of institutions and companies. Displayed institutions are those that have publicly showcased their space cybersecurity initiatives. Source: CyberInlfight

Quantum communications, optical communications and inter-satellite links

The development of powerful future quantum computers could undermine the security of current encryption methods. Encryption relies on mathematical techniques to protect information, with these problems being intractable for conventional computers. However, advanced quantum computers could potentially solve these mathematical challenges, rendering current systems protection ineffective. Protection serves three primary purposes: hashing to protect integrity; encryption to protect confidentiality; and digital signatures, which are used for identity authentication. If those protection fail, it will severely compromise secure SATCOM communications, making current protection techniques insufficient to ensure the security of these communications. To address the threats posed by quantum computers, the first solution would be to develop Quantum Resistant Algorithms (QRA), also known as Post-Quantum Algorithms (PQA). Another approach would be to implement Quantum Key Distribution (QKD).

Quantum technologies to enhance security

Encryption can be with a symmetric key algorithm or with a public key algorithm which is asymmetric. Only asymmetric algorithms are in danger from quantum computing. Symmetric and hash functions are considered more secure against quantum computing since simply increasing the key size can protect them. Therefore, QRAs cover a broad array of mathematical techniques that, while based on the same principles as existing asymmetric methods, are specifically designed to be more resistant to attacks by quantum computers. These mathematical problems are structured to be challenging for both conventional and quantum computers to solve. Multiple countries, including the France, Germany, and the US, are actively developing and testing QRAs to identify robust algorithms and establish new security standards. Digital signatures also require QRA.

In QKD, instead of relying on mathematical principles to protect the symmetric key, the key is shared openly using quantum bits (qubits) – i.e. by encoding data into the quantum mechanical properties, such as the polarisation of individual particles. QKD leverages two fundamental principles of quantum mechanics: the No-Cloning Theorem and Heisenberg's Uncertainty Principle. These unique properties of quantum mechanics are utilised to generate cryptographic key material. QKD protocols being considered:

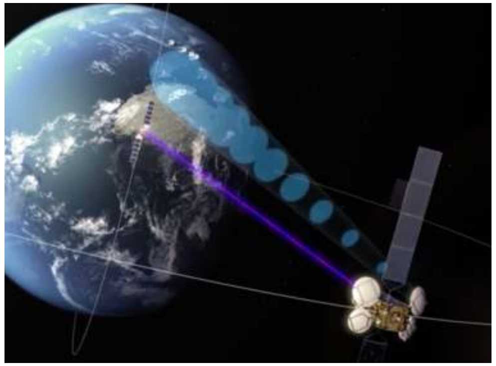
- **Discrete-Variable (DV-QKD)** relies on the direct detection of individual polarised photons, where the information is encoded. It is widely used in most current experiments.
- **Continuous Variable (CV-QKD)** encodes the information in the quadratures of randomly coherent states, which are then measured using either homodyne or heterodyne detection.

QKD has some limitations. Firstly, while it can be used for general encryption purposes, it cannot provide digital signature encryption. Secondly, since QKD is based on physical properties, it requires specialised equipment. This means it cannot be implemented as software or a network service, presenting challenges for integration into existing networks and increasing infrastructure costs. Finally, QKD is vulnerable to denial-of-service (DoS) attacks and insider risks. For satellite application of QKD, mostly two approaches are considered: "prepare and measure" and "entanglement". "Prepare-and-measure" protocols focus on measuring unknown quantum states, whereas "entanglement" uses groups of photon sources to send entangled photon pairs to the communicating parties. One European project example is OpenQKD under the H2020 framework.

Laser/optical communications and inter-satellite links to open opportunities

Optical communication links transmit data using shorter optical wavelengths of light (lasers), allowing for higher data transmission rates compared to RF communications. These optical links are also more secure against interferences, making them highly valuable for secure SATCOM systems. They can be used in space-to-space (S2S) or space-to-ground (air-S2A, maritime S2M, or ground S2G) links. Optical communications can establish connections between the user segment, space segment, ground segment, or within the space segment itself. One example of such solution where optical waveforms are used in the intersatellite link is the European Data Relay Satellite System (EDRS).

Inter-satellite Links (ISL), as a subset of S2S, provide a **direct connection within the space segment**, eliminating the need for the ground segment to relay data. The two main types of ISLs are RF ISLs (mainly in the Ka-band) and optical ISLs. RF ISLs are chosen for data rates below a few hundred Mbps due to their lower mass and simpler tracking system, making them easier to implement than optical ISLs. OISLs, on the other hand, are required to provide faster connections, up to hundreds of Gbps, but they significantly increase satellite mass (approximately 100 kg for four OISL terminals). This limits the number of optical ISLs per satellite. Typically, two ISLs for interplane connectivity and two for adjacent plane connectivity are installed in mesh networks within constellations.



© ESA

Another limitation is the total achievable capacity per link. The typical data rate is around 100 Gbps for optical units (about 800 Mbps for RF units). All traffic from satellites not within the range of a gateway must pass through a satellite that does have gateway coverage, potentially creating a bottleneck. This necessitates very tight resource planning and allocation. When a satellite supplies traffic to a high-density area without gateway visibility, it can only be supported by ISLs. The congestion effect is amplified by two factors: the number of ISL hops required to reach a ground station and the capacity available in adjacent satellites to route over this high-density area data traffic.

User terminals can incorporate **optical units to establish S2A, S2M, or S2G links**. Data transmission for all three types of links is affected by atmospheric conditions. **Optical links suffer signal loss while passing through the atmosphere due to small particles such as clouds, which can cause absorption and scattering**. This means that a large network of up to 10 optical gateway sites positioned in areas of Europe with low cloud probability is required to ensure a service availability in Europe of 99.9% served by a single operational optical gateway, with the remaining ones acting as backup sites.

In addition to these factors, atmospheric turbulence can also occur. This random phenomenon, caused by temperature and pressure variations, results in intensity fluctuations in the received signal. However, uplink and downlink paths are affected differently by atmospheric turbulence. For example, in the uplink, turbulence is primarily experienced at the beginning of the path, while in the top layers of the atmosphere. All these effects must be considered when establishing S2A, S2M, or S2G bidirectional links.

Role of AI in secure SATCOM

Artificial Intelligence (AI) aims to make machines to perform complex intellectual tasks, usually not easily manageable by humans. These tasks can be linked to classification, regression, clustering, detection, recognition, segmentation, planning, scheduling, or decision-making, among others. The concept of AI was established in the 1950s and has been developing since then. Currently, AI is in a period of significant activity, which began in the 2010s, fuelled by the evolution of computer processing power and the vast amounts of data generated by our increasingly connected societies and widespread internet usage.

Basic classification of AI

The AI field can be classified, relying on the methods used to resolve the different complex cases faced. AI can then be classified into symbolic AI, sub-symbolic AI, or in-between methods. Symbolic AI approaches pursue logical conclusions where sub-symbolic methods learn and adapt to the given data. In between methods take characteristics of both previous methods.

Machine Learning (ML), a subdiscipline of sub-symbolic AI, involves enabling machines to learn rules independently to solve complex tasks. ML frameworks usually include a training and testing process. The training enables the ML process to discover the relationships between inputs and outputs. Based on the training method, ML can be supervised, unsupervised, or reinforced learning. Inside ML there is the subset of **deep learning** (DL). DL is important for secure SATCOM systems since these types of techniques and models allow for the making of classifications, predictions, or decision-making. All of them are based on large raw datasets. DL includes models and techniques such as **neural networks** (NN), which use a composition of simple operations on neurons to extract essential features from the input data. DL and ML techniques can be applied to different prediction and pattern classification problems that current secure SATCOM systems are facing.

AI is an active field of both R&D and operations. The field of possibilities is so wide that we can say it is already present in the systems through small bricks, although its coverage will grow in the future.

AI FIELD CLASSIFICATION BY METHODS AND THEIR MAIN CHARACTERISTICS

Symbolic AI	• Logical conclusions, ability to explain the conclusion. • Human intervention is common as it is usually hard or hand-coded. • Best performed with relatively small and precise datasets as inputs. • Applicability for well-defined and static problems, and modelling of abstractions.
Sub-Symbolic AI	• Associative results with correlations between input and output variables. • Learn and adapt to given data. • They require significant computation power. • Able to handle large and not precise datasets (noisy data). • Applicability for prediction, clustering, pattern classification and recognition of objects, natural language processing.
In between methods	• Benefits from symbolic and sub-symbolic methods. • Can learn from the environment and the ability to reason the results.

AI and secure SATCOM optimisation

AI through ML and DL could help in the optimisation of secure SATCOM.

In the **payload of the space system, energy is one of the main parameters to be optimised**. AI-driven power management using adaptive power schemes can optimise energy consumption, ensuring stable and sufficient transmitting power to meet traffic demands. Thermal control for optimal working parameters of the payload can also be optimised thanks to the application of AI during the design phases.

AI, in combination with flexible payloads, will also enhance and **optimise secure SATCOM systems capacity and traffic**. AI application to techniques such as beam hopping or beam forming can optimise non-uniform and variant traffic requests from the ground and user segment. Allocation of the needed resources with the minimum mismatch between the offered and requested capacity will help to maintain high quality of service (QoS) standards. AI can also improve channel modelling for reliable high-speed communications.

User terminals can benefit from AI optimisation too. Some examples are multi-orbit handling, real-time adaptative MODCOD(s), enhanced signal detection or failure prediction (error, congestion).

AI and secure SATCOM network

AI, through ML and DL, can greatly enhance network and resource management, orchestration, and integration with external networks in secure SATCOM systems.

Network traffic forecasting and resource management are proactive methods for ensuring reliable and secure SATCOM communications. Congestion control, dynamic routing, dynamic channel allocation, network planning, and network security all depend on accurate traffic forecasts. However, SATCOM network traffic presents two main challenges for traffic modelling and managing resource: its **self-similar long-range dependence and the limited computing capacity** available on the payload. The **self-similar nature of network** traffic means that bursts of increased traffic appear similar across various time scales (seconds, minutes, hours). **The long-range dependence** implies that traffic and therefore the resource usage are correlated over time (what happens at time "t" is related to what happens at time "t-1"). These characteristics necessitate **robust computing capacity to implement traffic models that can predict future traffic accurately as well as resource usage scheduling**.

AI can also enhance the integration of secure SATCOM networks with other communication networks (see pages 66 and 67 on network management).

AI and secure SATCOM defence against threats

Anomaly detection in telemetry, tracking and command (TT&C) data, interference detection and classification, and anti-jamming techniques are all aspects to be impacted by AI and ML.

TT&C is used for control and monitoring of the space segment components. Traditionally, the telemetry analysis is based on limit checking, where the value of the parameters is monitored against predefined limits to detect out-of-range events. However, an attacker or an anomaly has the possibility of impacting a value without reaching these limits and not becoming an out-of-range event. This problem can be addressed by applying the generic ML problem of anomaly detection in a large number of variants over time. ML methods can be used to detect anomalies that might be out of the probabilistic values of operations, and lower than the prefixed traditional limits. AI enables a more efficient, dynamic, and precise health monitoring of our system.

Interference and jamming can also be detected and characterised by ML methods for aberrant comportments. In both cases, the correct identification can trigger system response to anti-jamming or interference isolation as frequency hopping, power limiters, or level control loops to protect the payload and the secure SATCOM service.

Space networks as a seamless complement to terrestrial networks

5G enabling the terrestrial network and non-terrestrial network integration

5G non-terrestrial networks (NTN) purpose is to enable the integration of space-based systems or High-Altitude Platform Systems (HAPS) connectivity and cellular networks/terrestrial networks (TN) under the same interoperable standard umbrella.

In 2017, the standardisation body 3GPP decided to adopt 5G broadband New Radio (NR) as well as 4G narrowband IoT (NB-IoT) and machine-type LTE (LTE-M) standards to permit connectivity from space. In 2022, Release 17 of the 3GPP standard included the essential features allowing the first NTN configurations. The Release 18 version introduced enhancements to NTN in June 2024, with work on Release 19 expected to be published at the end of 2025 or early 2026. The 3GPP's approach involves using frequencies selected by regulatory bodies for space communications. These frequencies are distinct from TN frequencies. In Release 17, some L and S-band frequencies were considered for IoT applications and direct 5G NR communication with smartphones. In Release 18, the possibility to offer VSAT communications in the Ka-band was introduced, while in Release 19 additional satellite frequency bands could be added. Release 20 will soon be initiated with two parallel tracks: further development of the 5G standard and preparatory studies for introducing the 6G standard, which will strive for a full unification of TN and NTN networks.

For NTN the impact of **transmission delay and possible frequency Doppler shift from the satellite are some of the main challenges**. The solution to these challenges is to require the user terminals to compensate for delay and Doppler shift before accessing the network. To this end, the satellite broadcasts its ephemeris corresponding to its position and velocity. The user terminal usually has a GNSS module to determine its position before accessing the network. With these elements, the user terminal calculates the distance and relative velocity of the satellite and uses that information to compensate for the delay and frequency Doppler shift.

Potential 5G security and flexibility features based on 3GPP standard

5G also offers **advanced security features designed to enhance communication security and data privacy**. Some concrete examples of security aspects implemented by 5G standards are:

- **Enhanced Authentication Mechanisms** to ensure that only authorised users and devices can access the network. Additionally, the authentication framework ensures that only authorised network functions can access services offered by another function.
- **High Level of Subscriber Privacy Protection**, using a concealed identifier instead of directly transmitting the permanent subscriber identifier over the air.
- **Strengthened Encryption Algorithms** to ensure that all communications are secure.
- **Improved Signalling Protection** to enhance the security of signalling messages between the network elements.
- **Optional network slice-specific authentication and authorisation between a user terminal and a server** which may be owned by an external third-party enterprise.

These comprehensive security features ensure that satellite networks based on the 3GPP 5G standard will be able to support secure SATCOM requirements and provide mission-critical services.

In addition, key design concepts of 5G networks include network slicing as well as Mobile Edge Computing (MEC), Network Function Virtualisation (NFV), and Software-Defined Networking (SDN) capabilities. These concepts can provide a ubiquitous, flexible, and extensible infrastructure for all types of secure SATCOM user needs and requirements. The standard also ensures the interoperability between NTN and TN.

NTN CONNECTIVITY CHARACTERISTICS

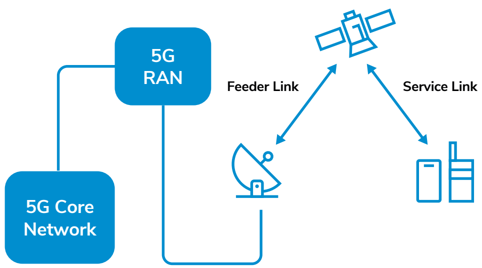
	Direct mobile connectivity		Fixed & Backhauling mobile connectivity
Frequencies	< 7 GHz (L, S-band)		>10 GHz (Ku, Ka-bands)
User terminals	Internet of Things (IoT)	Smartphones & car mounted	VSAT & mobile VSAT
Services	Narrowband (hundreds of kbps)	Wideband (few Mbps)	Broadband (hundred Mbps)
Satellite orbits	All	LEO	All
3 GPP radio interfaces	4G Narrow Band IoT/ LTE-M	5G New Radio	5G New Radio
Example of applications	Smart grids, water distribution, oil and gas, agriculture...	Automotive, public safety, defence, utilities, agriculture...	Telecom Networks, video service providers, transport, public safety, defence...

Direct-to-device and the move towards regenerative payload

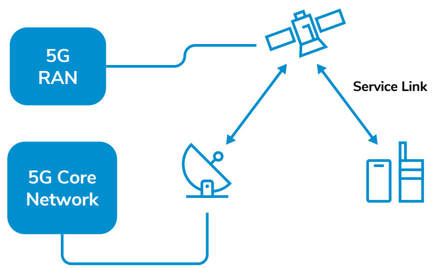
The direct-to-device 5G in NTN is already integrated, with the future possibility of direct-to-smartphone communications. The objective is to create enhanced mobile broadband (eMBB) for users of smartphones and the Internet of Things (IoT).

In the Release 17 and Release 18 NTN versions, it is assumed that the satellite (or HAPS) platform payload is transparent. Accordingly, a 5G base station ("gNB", including the Radio Access Network - RAN) and a Core Network (CN) are located on the ground behind the gateway, and the satellite's main purpose is to act as a repeater – **transparent** configuration. The only processing that it can perform is radio frequency processing such as frequency conversion, amplification, and beam management. Starting with Release 19, **regenerative** payload configurations will also be described. In such architectures, the satellite (or HAPS) carries a gNB or at least a radio unit able to decode and process packets. In such a case, the feeder link is comparable to a terrestrial backhaul/fronthaul link. Such regenerative architecture provides more flexibility, and better performance.

TRANSPARENT PAYLOAD
NTN ARCHITECTURE



NON-TRANSPARENT PAYLOAD
NTN ARCHITECTURE



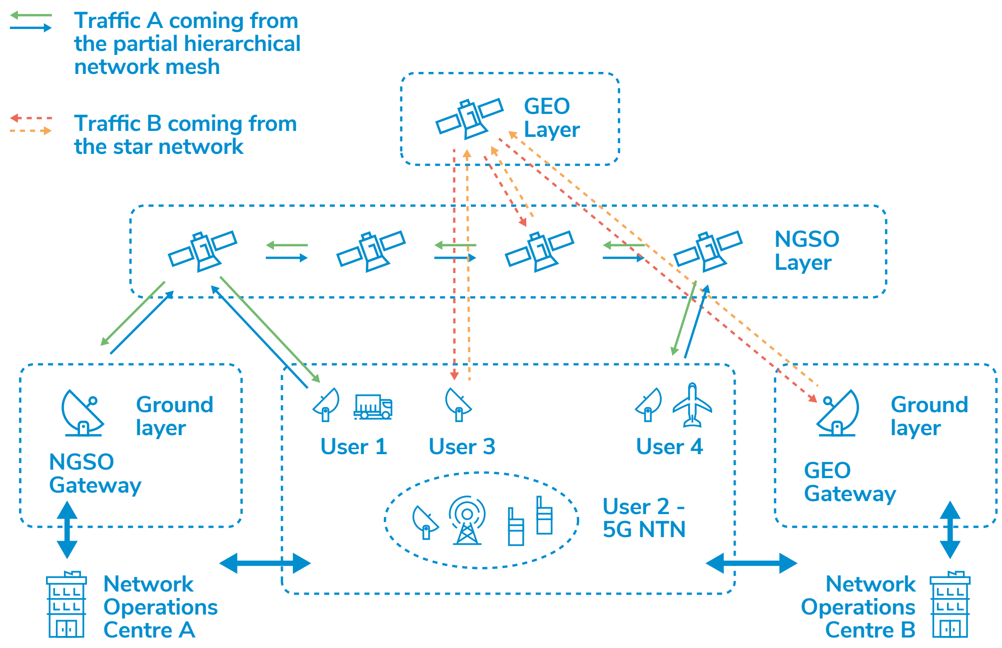
Secure SATCOM network management and 5G NTN Quality of Service

Hybrid networks management: an opportunity for the users

Secure SATCOM network management systems (NMS) are important to ensure **reliable, resilient, and available services**. Traditional network layouts (like star and mesh) already require NMS to ensure their service. Currently, due to the possibility of multi-orbit and multi-constellation, these networks are being combined into new hybrid mesh networks that incorporate GEO and NGSO systems. This increases the complexity and criticality of NMS. In these hybrid secure SATCOM networks that combine different network topologies, the Network Operations Centres (NOC) becomes a fundamental part of the overall SATCOM network architecture. Cyber threats, QoS, interference, traffic routing and load balancing, incident resolution, and service support are all functions provided by the NOC. These functions can be grouped into different categories, such as fault management (for monitoring and resolving all faults and failures), configuration management (overseeing the installation of new devices into the network to ensure they are correctly configured), performance management (tracking aspects like throughput, packet loss, and latency to manage optimal network performance), security management (protecting the network against intrusions, cyber threats, or signal threats), and accounting management (network usage, traffic, and resource allocation). All these functions executed by the NOC incorporate a high level of automation and AI tools to allow the correct management of large networks. **For user terminals, access to these large hybrid networks enables them to establish auto PACE** (Primary, Alternate, Contingency & Emergency) communication paths using different parts of the network. Coordination between the user terminals and the NOC is also important to maintain proper service.

Another trend on the user side is **the use of software-defined networks** (SDN). SDNs aim to unify and provide optimal traffic and capacity to users who are integrating different independent SATCOM sub-networks. For example, different SATCOM user terminals are located on a ship for different levels of security, traffic, and services. SDNs attempt to unify these user terminals into a more efficient routing and balancing network, where LAN users on the ship will have an intelligent traffic network that will ensure their access to the service. SDNs represent a new trend in the development of the user segment.

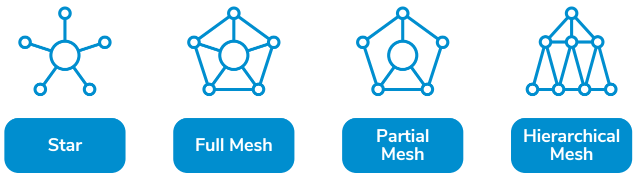
REPRESENTATION OF A HYBRID MESH WITH THE DIFFERENT LAYERS (NGSO, GEO, NGSO GATEWAY, GEO GATEWAY AND USER)



Space SATCOM networks topology

The traditional star topology is characterised by a **central node** (in SATCOM, this is usually the GEO satellite). **Mesh networks** linked to **large or mega-constellations** can have different configurations. The full mesh has all the nodes connected to each other. However, SATCOM mesh networks (i.e. NGSO constellations) can't implement a full mesh due to physical and operational constraints (earth obscuration, high number of nodes, limited number of ISLs in each satellite). That's why SATCOM mesh networks follow partial mesh topologies. In this partial mesh, each node is connected to a certain number of other nodes. This partial mesh can also be a hierarchical mesh, whereby the connections are organised by layers. These layers can be within the same NGSO constellation (based on altitude, inclination, etc.) or for multi-orbit systems based on their orbits (GEO, MEO, LEO). **Hybrid mesh networks are combinations of mesh networks with other topologies**, and in the case of SATCOM systems, it usually involves legacy GEO star topologies being incorporated into new NGSO mesh networks.

SECURE SATCOM POSSIBLE NETWORK TOPOLOGIES



5G Quality of Service (QoS)

As network management and load balancers are essential for QoS in secure SATCOM networks, the introduction of 5G NTN also offers new opportunities to improve QoS for 5G NTN. The 3GPP 5G cellular standard includes features to ensure that different types of traffic receive appropriate levels of service, meeting the application requirements. The standard introduces the following features that can benefit secure SATCOM users:

- **QoS flows** are used to manage the quality of individual data streams. Each flow has its own QoS parameters (such as latency, bandwidth, and priority). The objective is to ensure that different types of secure SATCOM traffic are handled appropriately according to their respective secure SATCOM requirements.
- **Core network slicing** allows the creation of multiple virtual networks within a single physical infrastructure, each tailored to specific secure SATCOM user needs.
- **Dynamic resource allocation** enables the network to adjust resources live based on current demand and network conditions, enhancing network resilience.
- **Support for the definition and enforcement of service level agreements** ensures that network operators can guarantee specific performance levels and availability requirements for different services.

Additionally, the standard allows advanced traffic steering and load balancing capabilities to distribute traffic efficiently across the network.

Cloud computing significantly influences secure SATCOM networks

Cloud computing is opening new area of services for secure SATCOM

Cloud computing represents a significant technological evolution across various industries. It affects business results and models in the information and communication technology sector. The cloud allows IT resources such as computing power, storage, and applications to be provided over the Internet. Instead of relying on local servers and infrastructure, companies can access cloud services from providers, enabling them to flexibly scale and adapt their IT infrastructure. The three primary cloud service models – **Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS)** – offer tailored solutions for different organisational needs. These models are increasingly being implemented in space systems. Cloud computing has started to be integrated into various space segments. For instance, the integration of cloud technology with the ground and user segments has led to the creation of new services such as Ground Segment as a Service (GSaaS).

Overall, the incorporation of cloud services into IT infrastructures impacts space systems and SATCOM satellite operators and their networks, reflecting a growing trend towards cloud integration. The opening to cloudification is part of a wider trend that encompass virtualisation and also concepts such as Space Edge Computing.

Cloud computing in secure SATCOM

Secure SATCOM networks are significantly influenced by advancements in cloud computing. The flexibility, scalability, efficiency in network management, and reliable connectivity provided by the cloud favour its integration. Hybrid network solutions combining terrestrial networks (TN) and non-terrestrial networks (NTN) will benefit from cloud usage, enhancing network reliability and performance through edge computing and cloud integration. This integration enables the creation of hybrid networks tailored to various user needs.

For example, cloud direct connectivity via satellite allows organisations to establish a private, dedicated network connection to their cloud resources through satellite communications. This type of connectivity is especially advantageous when traditional terrestrial network infrastructure is unavailable, unreliable, or inadequate. Increasingly, satellite operators and service providers are partnering with cloud service providers. For instance, SES Networks offers cloud-based applications for its mining customers, while Marlink implements a digital enablement strategy for shipping using Microsoft's Azure Stack. Hardware providers are also transitioning some gateway functionalities to the cloud. Intelsat's FlexEnterprise service, for example, provides cloud-managed satellite connectivity solutions with optimised and scalable network services via cloud-based management tools. Similarly, Thales Alenia Space integrates cloud computing to manage satellite gateways and network services, aiming to enhance operational efficiency and reduce reliance on on-premises hardware. Some cloud providers are pursuing all-in-one solutions, where their cloud services are complemented by SATCOM systems. For instance, Amazon Kuiper plans to deploy over 3,200 LEO satellites to create a global broadband network, providing high-speed Internet access to remote and underserved areas while linking users with their cloud services.

Brief market overview of cloud providers

The current cloud computing market is dominated by three major hyperscalers: **Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP)**. These companies offer a broad array of managed services and global infrastructure that cater to a wide range of industries and applications. However, alongside these dominant players, several smaller cloud providers focus on specific regional markets or niche sectors. In Europe, several cloud providers have emerged to address the region's unique regulatory and business requirements. German companies such as Open Telekom Cloud, IONOS, and STACKIT, as well as other European providers like OVHcloud, exemplify this trend. These providers often emphasise compliance with stringent European data protection regulations and offer localised support.

SOME CLOUD TRENDS AND THEIR IMPACT ON SECURE SATCOM

Cloud trends		Impact on secure SATCOM
Automation / Platform engineering	Setting up an infrastructure based on secure satellite communication is technically possible and can offer many advantages. However, it requires significant investment, specialised technological knowledge and careful planning to manage the technological complexity and security requirements.	**High**
Central data fabrics	Central data fabrics play a critical role in transforming how satellite communication (SATCOM) data is managed, integrated, and utilised. By providing a data management framework, they enhance data accessibility, improve operational efficiency, and support advanced analytics. Integrating SATCOM data into central data fabrics enables new insights, optimises resource utilisation, and drives innovation across various sectors.	**High**
Sovereign clouds	Independence from global cloud vendors and control over data are crucial for future workloads managed on digital infrastructures. Cloud and SATCOM providers must address how data is handled and secured through legal control mechanisms beyond encryption.	**High**
Hyperconnectivity	Satcom provides worldwide coverage, which is crucial to ensure hyperconnectivity even in remote and rural areas where terrestrial networks are often unavailable.	**Medium**
Cybersecurity	Satellites provide secure communication channels that are protected from cyber attacks and ensure the integrity of sensitive data. Using satellites as part of a distributed network increases resilience to attacks and outages.	**High**

Secure SATCOM R&D projects in Horizon Europe

EUSPA stimulates the market development of the EU space downstream sector and supports the uptake of space-based solutions through Horizon Europe (HE) space calls inside the programmes' second pillar. The third EUSPA Horizon Europe (HE) call, with a budget of €34.5 million, closed on February 2024. One of the topics was the EU GOVSATCOM that aims for a safer and more secure EU with an indicative allocation of €10 million. Other topics were related to GNSS, Copernicus, and downstream applications with international partners. Under the previous call, the GOVSATCOM-related topic had an indicative budget of €9.1 million and financed the following four projects: 5G-GOVSATCOM, GEXTRECS, S5LECT and SIGMA.

5G-GOVSATCOM

5G non-terrestrial networks (5G-NTN) satellite networks will soon be able to handle all types of applications and provide service to a vast number of users. In this complex and dynamic network ecosystem, and end-to-end adaptation of 5G-NTN towards the EU-GOVSATCOM services, requirements and use cases are of capital importance to efficiently deploy European governmental satellite services. To enable such a vision, 5G-GOVSATCOM targets the development and evaluation in a natural user environment of different key enabling technologies that aim to provide full integration of 5G-NTN in the EU-GOVSATCOM framework. In the radio technologies domain, 5G-GOVSATCOM targets the **development of necessary adaptions and enhancements of radio access procedures to attend to geostationary mobile terminals in the exclusive governmental X-band**. Furthermore, the integration of 5G-NTN user equipment with an **antenna operationally focused on on-the-move and on-the-pause scenarios** are planned. In parallel, in the internetworking segments, 5G-GOVSATCOM aims to provide a **seamless handover between terrestrial networks and NTN via a smart gateway**, while enhancing core-network functionalities. Finally, all project developments are planned to be first validated in a controlled lab with satellite connectivity and, posteriorly, experimentally tested in close collaboration with final users. These latter tests will constitute the first 5G-NTN trials with final users devoted to i) ubiquitous telemedicine in maritime areas, and ii) the crisis management connectivity bubble.

More information can be found on the 5G-GOVSATCOM page of the EUSPA website.

S5LECT

The S5LECT (SatCom and 5G Link, Edge and Cyber secuiriTy) project, led by SNCF, will test a solution for **seamless handover between 5G TN, satellite links, and Global System for mobiles-Railways (GSM-R)** communications system. The project studies the **hybridisation of TN and NTN for railway-critical applications**. The project aims to define and develop an innovative solution for seamless handover between NTN-TN, assess cybersecurity risk and propose solutions, propose innovative architecture for edge computing, and provide a **proof of concept** of all the bricks developed in the project thanks to an original laboratory testing platform. The S5LECT project will directly contribute to the development of solutions for the **use of GOVSATCOM satellite communications in the railway domain**. It also contributes to the development and testing activities for delivering more reliable and robust wireless communication prototypes. This should help to enhance the testing activities and minimise time and efforts to deliver the next generation of adaptable wireless communications for all railway segments.

More information can be found on the S5LECT info page.

SIGMA

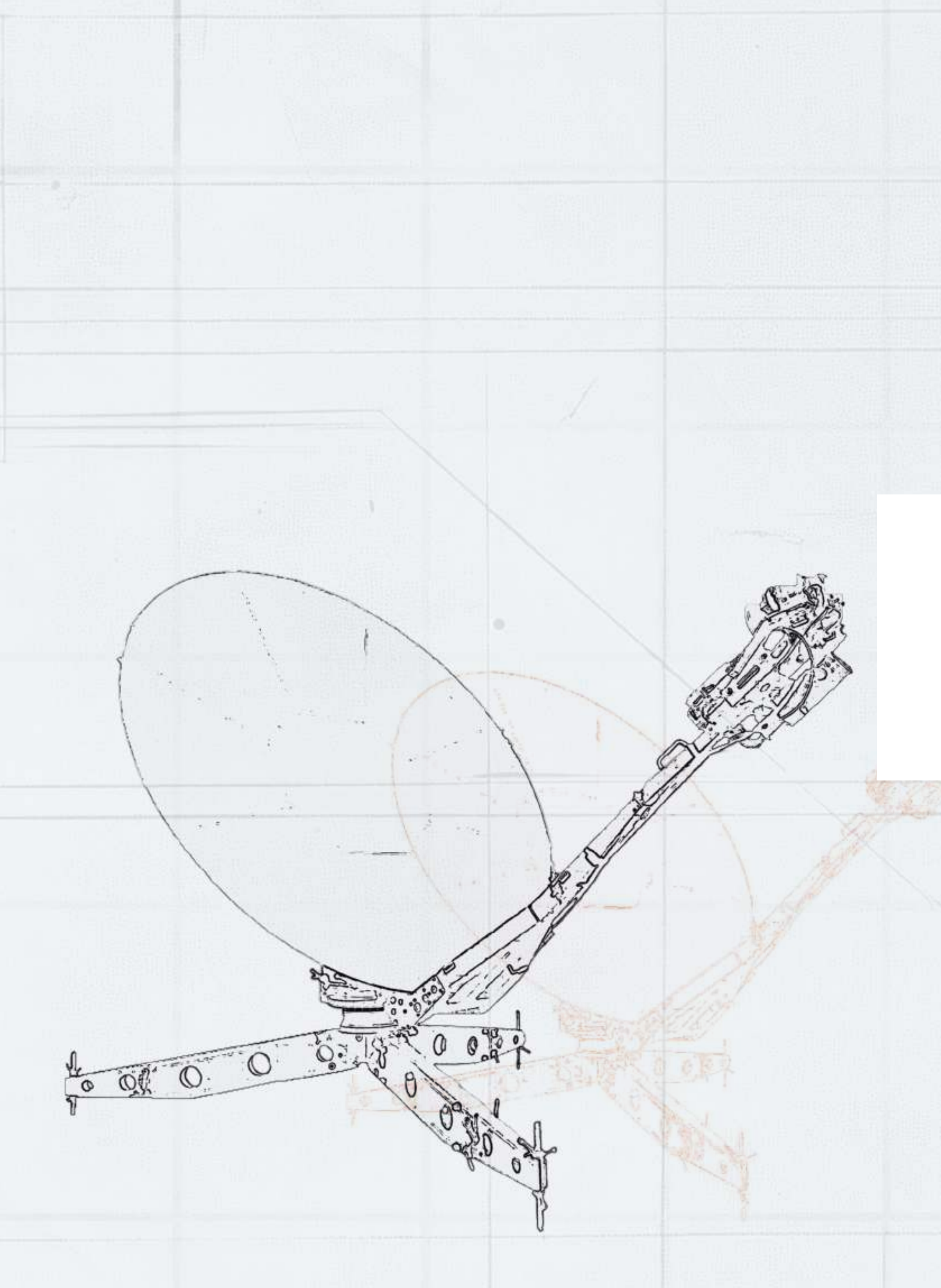
The SIGMA (Satellite-enabled Interoperable system ensuring GOVSATCOM services' reliability, optimal traffic Management, security and long-term Availability for EU and national public authorities" project) will develop and demonstrate a technical solution for **GOVSATCOM capability and 5G interoperability with seamless handover between military/civilian satellites and terrestrial 5G networks**. The consortium, made up of five companies and a research centre from four different countries, will integrate Satcom-On-The-Move operating in military X- and Ka-bands as well as civilian Ka-band with 5G Terrestrial Network into a robust solution that provide **interoperability, security, and seamless operational capabilities**. The solution will integrate existing hardware with routing of traffic managed by a **completely new traffic management software and a software-defined wide area network router** including full end-to-end security by an encryption module that incorporates the advanced encryption standard algorithm. The new solution will be demonstrated in real user environments in three use cases specified by national end users of three EU countries: Luxembourg (emergency response during a major flood crisis); Germany (search and rescue operations in isolated Alpine regions); and France (responding to a terrestrial network outage during a cultural/sporting event).

More information can be found on the SIGMA info page.

GEXTRECS

The GEXTRECS (GOVSATCOM Extreme Events Crisis Management Service) project, aims to demonstrate an end-to-end GOVSATCOM service supporting **extreme events crisis management**. In the event of natural or manmade disasters, it is essential to ensure an adequate level of action in terms of provision of proper SATCOM services and response time. During such crisis management situations, multiple and simultaneous requests from different end users are typically addressed to SATCOM resources, with a high risk of network saturation. The GEXTRECS end-to-end solution plays a **crucial role in preserving the security of the EU citizens** in such conditions. To address this, the project is developing and will be demonstrating an innovative component called the Dynamic Planner, which will **dynamically, optimally, and continuously allocate resources during the crisis**, assigning each service request to the most suitable SATCOM resource. This will be integrated with a Network Balancer, which will enable the required interoperability, ensuring that secure communication is maintained when using different communications networks. Two scenarios will be demonstrated (land natural disaster and maritime emergency) in real end user environments, also exploring the GOVSATCOM synergies with other EU space programme components.

More information can be found on the GEXTRECS page of the EUSPA website.



SECURE SATCOM USER TECHNOLOGY TYPES

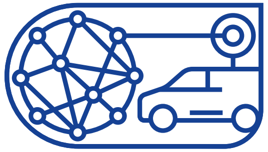
Back to main table of contents | Back to secure SATCOM user technology overview page

Three secure SATCOM user technology types used to simplify categorisation

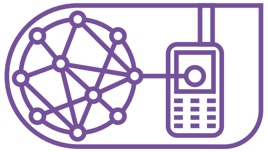
In the preceding sections, the key components of a secure SATCOM terminal and their associated technological evolution trends were introduced. When looking at the actual market offer, **available secure SATCOM (user) terminals differ in several aspects** including performances, frequency bands, antenna type, GSO/NGSO compatibility and/or transportability of the device.

To help navigate the diverse range of options available on the market, the authors have defined three primary categories of secure SATCOM terminals starting from terminology widely recognised within the SATCOM industry. This classification organises secure SATCOM terminals according to their operational scenarios, with a specific emphasis on the mobility requirements of the terminals.

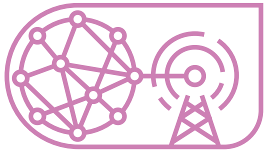
In the subsequent sections, secure SATCOM terminals have been categorised into three distinct **user technology types**:



1. OTM/OTP user technology type is based on one major constraint, which is mobility (i.e. non-fixed connectivity). Therefore, OTM/OTP (On-The-Move/On-The-Pause) should meet the following requirement: the capability to connect to a network at a location that is rarely the same to the last connection. To fulfil this requirement, the terminals are usually integrated into a moving/transport platform (airplane, ship, or land vehicle). **OTM** is required when the user communicates with a GEO/NGSO constellation while installed on a moving platform, whereas **OTP** is required when the user must stop to allow the pointing of the terminal's antenna and must remain immobile during communication.



2. Deployable, handheld and secure IoT user technology type is mainly characterised by the capability of communicating and deploying its terminals in a more compact and easier way. **The deployable** user terminals (fly-away or manpack) share characteristics with the OTP terminals. However, the key difference is that they are more compact and easier for users to deploy and install. Fly-away user terminals are equipped with directional parabolic or flat panel antennas. Manpacks are deployable terminals that bridge the gap between fly-away and handheld units. They allow secure SATCOM users to carry the antenna and terminal components (such as a more robust power source) in a backpack, offering better performance and functionality than a simple handheld terminal. **Handheld** terminals, typically lightweight, use omnidirectional antennas that can be integrated into the terminal or carried in backpacks or held by the operator. **IoT** terminals are uniquely identifiable connected devices that can process data and communicate with each other with or without human involvement. They are usually characterised by low throughputs and periodic transmissions at regular or event-driven intervals, while they are installed either at fixed locations or at moving platforms, such as trains, and ships.



3. Fixed and backhauling user technology type is not constrained by the mobility requirement as the other two previous technology types. As such, the user installs the terminals in a stable place, where the secure SATCOM service will be needed for long periods of time or even permanently. **Fixed** user terminals are traditionally designed to allow for higher throughput than e.g. OTM/OTP and they have a simplified architecture since the antenna doesn't need tracking systems as it usually does in other cases. Meanwhile **backhauling** terminals allow the communication between the core network, for instance cellular base stations, and local terrestrial networks usually located in remote locations and/or unavailable via terrestrial links, by aggregating and backhauling via satellite all the data required.

For each specific user technology type, the following sections delves further into its specific characteristics both from operational and technical point of view providing details on the typical targeted use cases; terminal components and architecture; characteristics of the main used signals; technological factors and trends or security and standardisation efforts.

OTM/OTP user technology type: overview

The OTM (On-The-Move) and OTP (On-The-Pause) user technology type is addressing mobility needs (i.e. non-fixed connectivity) and thus the capability to connect to a network at a location that is rarely the same to the last connection. To fulfil this requirement, the user terminals are usually integrated into a moving/transport platform (airplane, ship, or land vehicle, including all connected and automated/unmanned vehicles for air, sea surface, underwater, and land). It should be noted that OTM and OTP can also rely on isotropic and omnidirectional antennas, for instance, when it is in L-band for Broadband Global Area Network (BGAN) on airplanes, or ships (e.g. INMARSAT C safety services).

OTM/OTP difference of usage

OTM terminals are required when the user communicates with a GEO/NGSO constellation while installed on a **moving platform**. The user terminal must be able to track the satellites in continuous movement through air, ground, or sea. The challenge is to keep pointing to the satellite whatever the movement of the vehicle – for instance, with large waves at sea and car manoeuvres, but also the obstructions from the vehicle body and physical infrastructure. The **antenna's technological response** to this need can range from mechanically having actuators to steer the antenna to more electrical components or fully electrical parts that can perform these pointing functions (as in Electronic Steerable Antennas).

OTP terminals are active when the user stops to allow the pointing of the user terminal's antenna (generally large). The OTP user terminal is not able to track the satellites while the terminal is moving, which eliminates the complexity of the OTM tracking systems.

In both cases, the secure SATCOM applications usually involve **traffic** with throughputs of few Kbps to up to 40 Mbps, where voice, data, and video/images are transmitted. User terminals are incorporating all the elements necessary to establish and maintain the connections. In both cases, OTM and OTP, the handover of the connection from one satellite to another (especially in the case of NGSO constellations, but also in cases of crossing beam boundaries in GEO satellites) and the capability to have multi-orbit and multi-constellation access are key challenges for today's user terminals. These **transitions** need to be properly **secured and seamless** through the user **terminal** to allow secure SATCOM services. The seamless handover between satellites is not such a big challenge anymore thanks to flat panel electric antennas with beamforming capabilities. However, the cost of these flat panel antennas is still high and a limiting factor for the end-users.

OTM/OTP integration as the main challenge

From a **user's point of view**, the main **challenge** for the adoption of OTM terminals is the **integration with the mobile platform**, not only in terms of physical integration but also in interfaces and connections to internal networks and systems of the platform. These **connections and integrations are crucial for maintaining the secure SATCOM properties** and not introducing vulnerabilities or access points for attackers. For example, vulnerabilities can arise when secure SATCOM traffic and commercial traffic are mixed in the local networks, such as on a ship. Routing and channelling the different traffic on these platforms are the main challenges for the OTM terminal integration. However, integration is not only a challenge in these situations. It is also a challenge when integrating with other non-SATCOM user networks – e.g. in the case of railway infrastructure, where the OTM terminal must interact with a dedicated railway terrestrial network in charge of specific railway traffic management tasks. Railway infrastructure managers in particular intend to benefit in the future from "multi-bearer" solutions, providing the capability to reduce the infrastructure-related cost associated with deployment and maintenance of the terrestrial networks. In the case of OTP terminals, integration remains important, but the deployment of the user terminal becomes more challenging, requiring users to have specific training on how to deploy, operate, and integrate the OTP terminal in the area of interest.

OTM terminals can be further **categorised according to the type of moving platform on which they are installed** (i.e. land, air or maritime). The user terminals usually come with domes (in the case of parabolic antennas) or covers (in the case of flat antennas) to protect them and allow seamless integration with the mobile platform structure.

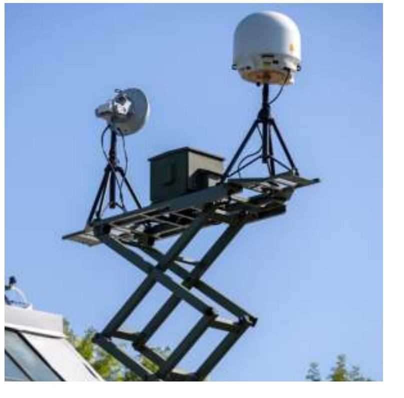
OTP terminals are **land-based** and can either be integrated into **a mobile platform** or a **transport platform**. In both cases, the user terminal must be deployed to the area of interest, where trained personnel are needed to deploy and install these user terminals. OTP terminals integrated into transport platforms are meant to be mobile but stay for longer periods in the area of interest. In contrast, OTP terminals integrated into mobile platforms are meant for dynamic and frequent deployments.


© dani3315/istockphoto.com

OTM terminal (white antenna radome) installed on a navy ship. Integrating an OTM terminal into platforms like ships, where different types of communications traffic, networks, and systems coexist, is one of the main challenges to maintaining secure SATCOM guarantees for the end user.


© AdrianHancu/istockphoto.com

OTP terminal integrated with a vehicle. These user terminals offer high mobility while integrating all secure SATCOM functions and parameters into the moving platform, enabling quick connection to, or deployment in, local networks.


© Karolis Kavolelis/shutterstock.com

OTP terminal integrated with a moving platform that can be transported and deployed. These user terminals, while not being integrated into a moving vehicle, still offer mobility for their deployment. The main difference with deployable fly-away user terminals is their size and the complexity of installation, requiring support assets and trained personnel.

Main characteristics of OTM/OTP terminals

	On-The-Move	On-The-Pause
Main capabilities	• Use of Directional antennas (VSATs or ESA) or isotropic and omnidirectional. • Throughputs of few Kbps up to 40 Mbps, for voice, data, and video/images. • Terminals usually operate in one or two bands, including L, X, Ku, Ka-band.	• Use of Directional antennas (large aperture, VSATs or ESA) or isotropic and omnidirectional. • Throughputs of few Kbps up to 40 Mbps, for voice, data, and video/images. • Terminals usually operate in one or two bands, including L, X, Ku, Ka-band.
Deployment/installation of the terminal in the field	**The terminal needs integration with the vehicle and vehicle systems:** • Aero-installation and accommodation of the terminal must be done in line with ARINC standards including aerodynamics, air operations and structural aspects. • Maritime/installation and accommodation of the terminal must be done mainly with terminal operational capacities in mind.	**The terminal needs a deployable space or integration with the transport vehicle:** • Vehicle-installation must be done with terminal operational capacities in mind. • Deploy in terrain – Line of sight will be the main concern to deploy the terminal.
General experience to operate the terminal	• **Operation of the terminal, integrated in the vehicle remains simple, with a basic level of training.** • Installation, malfunctions or maintenance, however, might imply the need for more qualified personnel and terminal/platform system experts.	• **Operation of the terminal, once set up and configured, remains simple to manage with a basic level of training.** • Installation, malfunction, or maintenance might imply the need for qualified expert personnel on the terminal.
Time to deploy and set-up connectivity	• Installation and integration with the moving platform of the terminal may take up to days or hours. • Initial configuration might take 10-30 minutes. • **Connectivity once the terminal is configured and on-the-move should remain stable with access to the service in the order of a few seconds.**	• Installation and integration with the moving platform may take hours. • Deployment and set-up of the terminal may take minutes to hours. • Initial configuration might take 10-30 minutes. • **Connectivity once the terminal is configurated and on-the-pause should remain stable with access to the service in the order of a minute.**
Considerations about operational environment	• Terminal must be on the upper part of the platform, with clear line of sight to the satellite while the platform moves. • **Weather, aerodynamics loads, thermal environment and structural integration with the platform are aspects to consider while installing the terminal.**	• Terminal must be on upper part of the platform, with clear line of sight to the satellite once the platform stops. • **If deployable, terrain might be as flat as possible to facilitate a consistent reference for terminal pointing and acquisition operations.** • **If deployable, terrain must have a clear line of sight and be free of obscuring elements.**
Future trends	• Multi-orbits, multi-constellations. • Multi-frequencies. • Virtualisation of the integration with local network. • **Standard installation procedures for generic platforms (UAVs, ships, vehicles).** • **Miniaturisation.**	• Multi-orbits, multi-constellations. • Multi-frequencies. • Virtualisation of the integration with local network. • **Miniaturisation.**

Typical use cases

Use cases of OTM/OTP user technology type are those where mobility is a major driver. Indeed, the users need to stay connected while their position is constantly changing (OTM) or while the location might change from connection to connection (OTP). Among many, these use cases can be highlighted: maritime emergency and surveillance, border surveillance (land, air, and maritime), forces deployment, and crisis/emergency intervention or transport infrastructure.


© KITTIKUN YOKSAP/shutterstock.com

Example of OTM terminal mounted on an aircraft.

Maritime OTM use cases

Connectivity at sea is critical, either in maritime emergencies, maritime surveillance, or forces deployment scenarios. Operations within the framework of the Common Security and Defence Policy (CSDP), such as EUNAVFOR ASPIDA (Red Sea, Indian Ocean, and the Gulf), MED IRINI (Mediterranean near Libya), or ATALANTA (near the Horn of Africa), are excellent examples of these cases, where secure SATCOM is needed to conduct surveillance, force deployment, and respond to maritime emergency missions. These secure SATCOM services are used for communications between different ships or between ships and mainland HQ, and to coordinate other maritime surveillance assets such as **coast patrol airplanes or drones**.

Emergency at sea, with the **Global Maritime Distress and Safety System (GMDSS) service**, can benefit from secure SATCOM OTM terminals to maintain connectivity in remote or polar sea regions, where normal radio coverage might be insufficient.

Air OTM use cases

Sensors mounted on Unmanned Air Vehicles (UAVs), especially for very long operations, need secure SATCOM data traffic. **Images and video from surveillance, or only telemetry and operational data** to keep the UAV operator connected to the asset, make up the traffic that secure SATCOM OTM terminals must ensure on these air platforms. In surveillance, border control, or forces deployment use cases, the operations of UAVs and other unmanned vehicles (surface, underwater, etc.) require secure SATCOM connectivity to operate them.

In civil aviation, secure SATCOM OTM services can improve the safety services for air traffic management, airline operations, and information services, as well as autonomy services (linked with UAV remote piloting). The **Aeronautical Mobile Satellite (Route) Service (AMS(R)S) can support oceanic or polar data link and voice safety services through OTM L-band secure SATCOM user terminals**.

© Obatala-photography/shutterstock.com

Example of an OTP terminal mounted on a trailer for firefighter operations in France.

Land OTM use cases

Land OTM use cases are, among others, related to **transport infrastructure**, with a special interest in secure SATCOM OTM terminals for railways. In Europe, within ERTMS (European Rail Traffic Management System), the Global System for Mobile Communications-Railway (GSM-R) is currently used as a radio-communication system, offering a wide range of voice and data services needed for the daily operations. GSM-R is expected to be obsolete by 2035, with railways planning to replace it with Future Railway Mobile Communication System (FRMCS), which is based on 5G NR. Studies to incorporate secure SATCOM OTM terminals into FRMCS evolutions are in progress at present, with involvement of several EU railway infrastructure managers. On top of railways, satellite connectivity is already the reality for the **automotive** industry. User terminal products, mainly based on flat panel antenna technology, are available in the market both for NGSO and GEO connectivity. In addition, connected and automated cars is one of the use cases of 5G NR and it is planned to be addressed in the future also via non-terrestrial networks.


© Mariusz Bugno/shutterstock.com

Example of **OTM flat panel antenna** mounted on board of big container ship.

Land OTP use cases

OTP terminals are related to **force deployment** or similar deployments (emergency, crisis management, remote areas connectivity), where secure SATCOM services can be enabled in a remote zone thanks to the OTP terminals. OTP terminals are designed to be mobile, but to enable use cases that need connectivity in a region for variable periods of time (hours, days, weeks, or months). OTP terminals mounted on vehicles are easier to move and deploy than OTP terminals mounted on transport platforms, which usually require an additional deployment process.

Back to main table of contents | Back to secure SATCOM user technology overview page

Terminals' main technology considerations

The mobile nature of the OTM/OTP user technology type implies two main technical specificities that must be taken into account in the design of such equipment: the changing of the relative position of the satellite and the user and the satellite/beam handover.

Changing of relative position of the satellite and/or the terminal

Regarding **changing of relative position of the satellite and/or the user terminal when directional antennas are considered**: in the case of OTP, antenna pointing must be done once at start-up if using GSO or done dynamically in the case of a moving satellite (NGSO). In the case of OTM, since the user terminal is potentially also in movement, antenna steering must always be dynamically maintained. The tracking antenna subsystem first needs to know in which direction to point, then apply this parameter to the antenna beam steering. The following steps are performed:

1. Using external orbit data (e.g. ephemeris or Two-line Element sets (TLE)), the **satellite orbit determination subsystem** determines the position and the trajectory of the satellite to predict its evolution.
2. Sensors, such as a **GNSS receiver**, determines the location and the velocity vectors of the user terminal (it also provides a precise time/frequency reference which can be crucial in certain operations such as make-before-break concept).
3. The **terminal attitude determination module** uses different sensors (compass, gyroscopes, accelerometers) to derive the position in Roll, Pitch & Yaw of the user terminal relative to a reference frame.
4. The beam is either steered mechanically (parabolic dish) or electronically with direct radiating arrays (flat panel antennas).
5. Some user terminals can be equipped with an **antenna tracking receiving chain**, which can be used in closed-loop to keep tracking by locking on the received signal (e.g. mono-pulse tracking, step-track).
6. The **Antenna Control Unit** (ACU) compiles all these inputs to derive the steering direction of the antenna beam. Note that the elevation visibility mask around the user terminal may also be entered as an input parameter to the ACU.

This process is very much simplified when omnidirectional or isoflux antennas are considered, as antenna pointing is unnecessary and therefore all the related equipment can be dispensed with.

Satellite handover/beam handover

Regarding **satellite handover/beam handover** in particular when the link is to be established with an NGSO constellation, the need for a satellite handover is mandatory as spacecraft are moving in and out the visible field of the user location. This may imply (in the case of the "Make-Before-Break" strategy) the use of two parabolic antennas to keep seamless communication. Electronically Steerable Antennas provide a solution to this as they can directly form two distinct beams, whereas mechanically steered antenna only have a single main beam. For OTM, the terminal may travel through different satellite ground beams. While adjacent beams will most likely use different frequencies/polarisations, the terminal will need to use two data carriers (two in transmission and two in reception) at the same time to ensure seamless communication. This is managed at the modem and RF front-end level. Both these handover types also need to be managed at the network level to define the data routes. On the other side, the terminal shall also manage these handovers (traffic plan can be received through the satellite link). The terminal will also need to have feeds that allow both polarisations to be received to allow the handover between beams of different polarisations. In case of omnidirectional or isoflux antennas the challenge of satellite handover is not applicable given that the single user terminal antenna is able to see multiple satellites with almost the same user terminal EIRP and G/T.

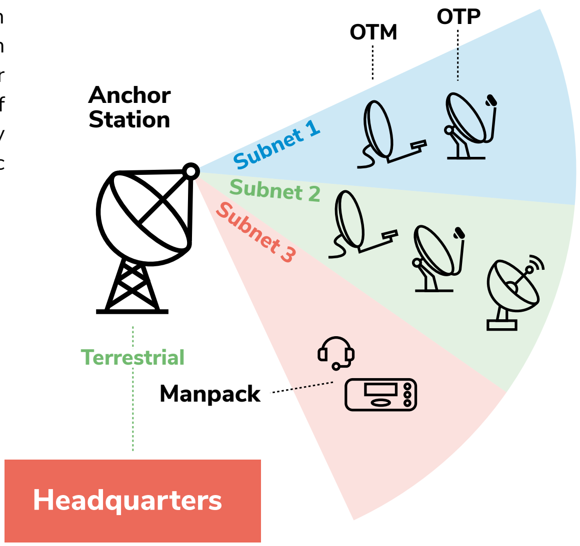
While all OTM/OTP systems share similar components and architectures, they vary in size and performances depending on their operational role and the deployment scheme. For example, **OTP or OTM terminals for first-line command centres or highly mobile units** utilise small size deployable directive antennas (below 2.4m), whereas **larger OTP for field headquarters** feature larger size antennas to gain high-throughput (above 2.4m).

The secure SATCOM network is structured to ensure optimised operations and resources allocation for each of these systems, tailored to their operational requirements and performance capabilities. The Quality of Service (QoS) parameters include link availability, committed information rate, latency, security, and robustness.

A major trend in secure SATCOM networks is the separation of different terminals and **QoS levels into dedicated subnetworks** (as shown in the figure). Data transmission in these subnetworks can occur either on separate RF carriers (enabling different MODCOD(s) and thereby affecting spectral efficiency) or using waveforms that allow different MODCOD(s) for various users within the same carrier (e.g. DVB-S2X). These considerations are critical for both Forward (gateway stations to users) and Return (users to gateway stations) links.

While traditional SATCOM systems typically utilise a star topology, secure SATCOM networks can also implement mesh topology, where users can communicate directly with each other. This enhances communication reliability in case of anchor station failure or disaster, as it eliminates the single point of failure and single point of target for security attacks associated with ground-based traffic centralisation.

USERS SPLIT IN DIFFERENT SUBNETWORKS BASED ON THEIR TERMINAL TYPE



Architecture of OTM/OTP terminal

As shown on the previous page, the architectures of OTM/ OTP user technology type remain traditional, except for the hardware required to adapt the antenna steering, manage handovers, and enable multi-orbit capabilities. Their main components are the following:

- **Antenna**: Transmits and receives data (parabolic dish or electronically steerable flat panel, or omnidirectional, or isotropic). A multi-orbit user terminal must be capable to remain connected with satellites of multiple altitudes during their movement. In case of directional antennas, this requires various tracking speeds and beam steering accuracy, while ensuring sufficient gain to maintain the link budget and the committed information rate. In addition, in case of directional antennas and for secure SATCOM, the secondary lobes should be particularly low to minimise the risks of eavesdropping or interference with the user terminal.

- **Tx/Rx frequencies & polarisation diplexer**: Separates the transmitted from the received signals at the antenna input/output.

- **Antenna Control Unit** (not applicable for omnidirectional and isoflux antennas): Includes the steering direction computation (when applicable), the antenna tracking receiving chain (optional) to lock on the received signal, and the beam forming network (in the case of an electronically steerable antenna), or the antenna motor unit with its power supply (in case of mechanical steering). Antenna locking on the signal can be achieved either using the satellite beacon (which requires a specific beacon receiver) or the modulated signal (which avoids the need for a beacon receiver but makes tracking capability dependent on the modulation/waveform technology). In the case of an NGSO system or multi-constellation, seamless connectivity during satellite handover will require two mechanical steering antennas. Electronically steerable antennas can mitigate this issue.

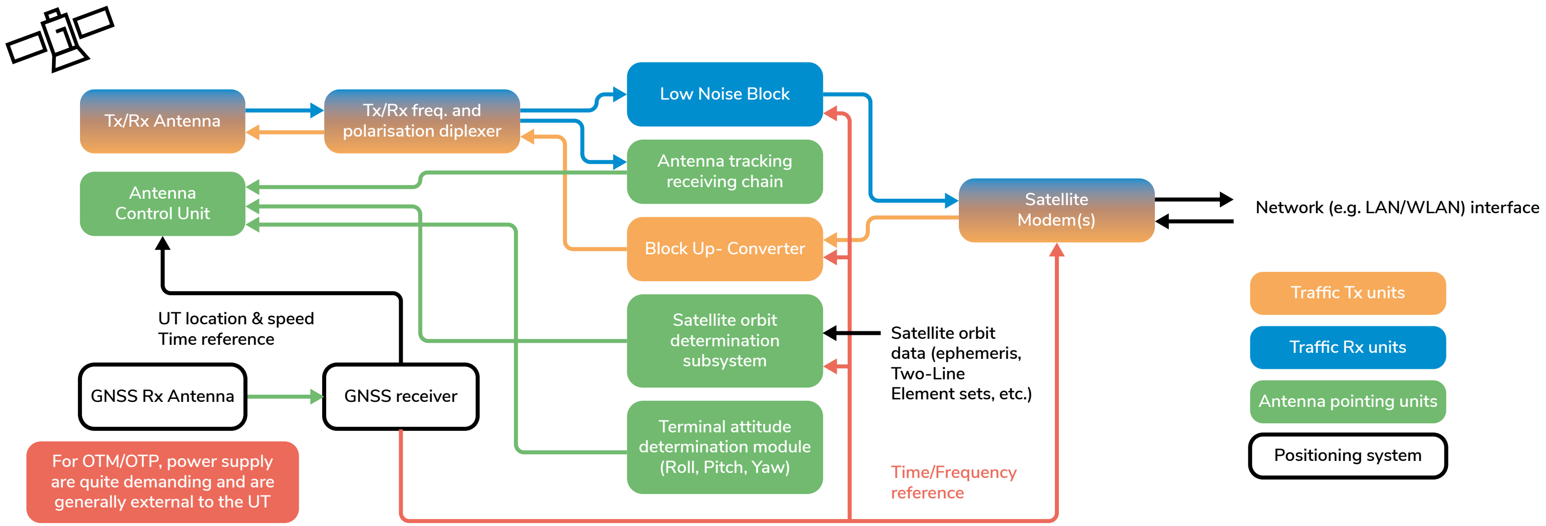
- **Low Noise Block (LNB)**: Includes a frequency downconverter and an LNA to receive the signal.

- **Block Up-Converter (BUC)**: Includes a frequency upconverter and a High-Power Amplifier (HPA), either Travelling-Wave-Tube Amplifier (TWTA) or Solid-State Power Amplifier (SSPA), to transmit the signal. The BUC's RF output power, combined with the antenna gain, is the one of the main performance factors of a user terminal and determines the achievable throughput in data transmission.

- **Satellite Modem(s)**: The modem performs the signal synchronisation, the coding and decoding, the interleaving and de-interleaving, the mapping and de-mapping, the composition and decomposition of the physical frame, and the modulation and demodulation. The modem is also responsible for conversion of digital to analogue and vice-versa at the interface with the RF equipment.

- **GNSS antenna and receiver**: Computes the user terminal's geolocation and velocity. This geolocation, along with the knowledge of the satellite's orbit and the user terminal's attitude (Roll, Pitch, Yaw), enables the determination of the azimuth and elevation to be pointed at.

GENERIC LOGICAL ARCHITECTURE OF AN OTM/OTP USER TERMINAL (SINGLE ANTENNA)



Characteristics of signals used

Secure SATCOM for OTM/OTP utilises specific signals, both in terms of frequency and waveform, to enhance security and robustness.

OTM/OTP compatible with all frequency bands

The OTM and OTP terminals in secure systems can theoretically operate across all **MSS/BSS/FSS-dedicated frequency bands**. However, the mobile nature of such terminals imposes some limitations in terms of footprint (volume, mass, DC power), particularly affecting antenna size, although truck-transportable units now offer comfortable antenna apertures of several metres. This, in turn, directly impacts link budget performance and, consequently, achievable data throughput. Depending on the mission and its requirements – whether broadband, narrowband, low throughput or voice communications only – the choice of frequency becomes crucial.

Secure OTM and OTP terminals may use military SATCOM frequency bands such as X-Band (also known as SHF, 8-9 GHz) or Military Ka-Band (also known as EHF, 20-21 & 30-31 GHz) for broadband, which typically require directional antennas.

COMSEC & TRANSEC to protect the data transmissions

By nature, SATCOM transmissions are “observable” by any user directing their user terminal toward a space asset, provided the terminal is within the same ground coverage area. Similarly, uplink communications (transmitted) may be intercepted by monitoring the electromagnetic environment near a ground station or through high-altitude assets (aircraft or platforms over operational theatres). In this context, OTM/OTP concepts increase security by making it difficult for an attacker to determine the user terminal's location. However, strategies must be developed to prevent transmissions from being compromised.

The general strategy for protecting secure SATCOM communications relies on the following pillars:

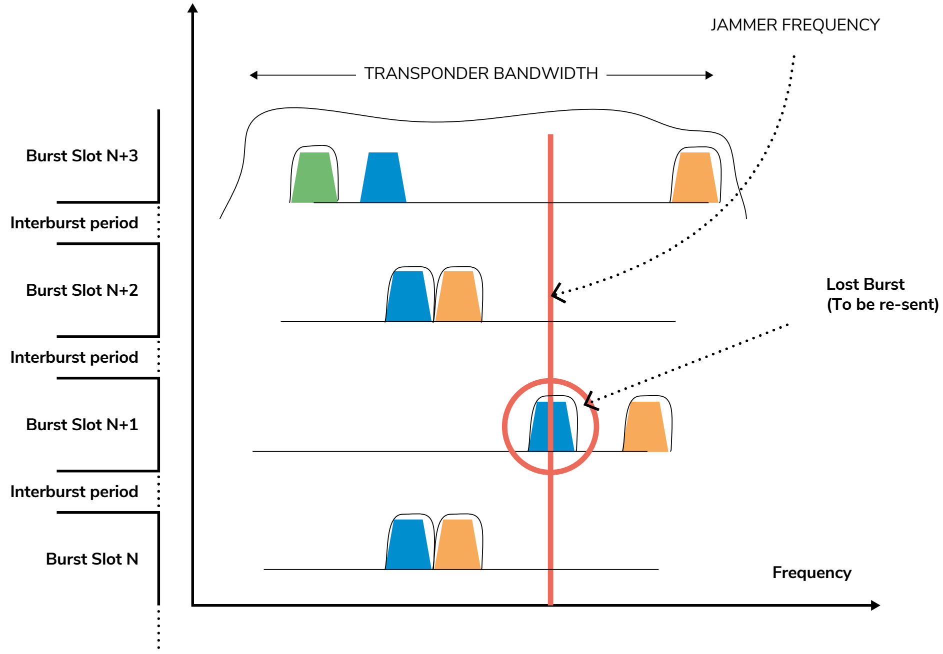
- **Encryption of space communication data** is using **COMSEC algorithms**, generally based on traffic encryption keys and counters that may be synchronised with a satellite reference.
- **Dissemination of traffic encryption keys** is employing various methods at the operation field level, including pre-configured terminals, ruggedised modems designed to prevent key compromise, over-the-air distribution using key encryption keys systems, quantum key distribution, and the use of complementary crypto-officers (each holding part of the keys to avoid compromise).
- Use of specific signal characteristics to **prevent detection, interception, or jamming** (TRANSEC), as described hereafter.

The TRANSEC techniques rely on specific data formats, network protocols, waveforms (modulation & coding – e.g. Link 16, NATO UHF Modcods, European Protected Waveform), and signal processing techniques, to increase robustness and protection, such as:

- **Direct Sequence Spread Spectrum** multiplies binary data with a pseudo-random spread sequence, resulting in a signal that appears random and occupies a broader frequency range than the original signal. This helps ‘hide’ the signal within thermal noise and provides protection against narrow-band jammers.

- **Frequency hopping** uplink and/or downlink (hop & dehop) technique relies on a consistent time versus frequency allocation for uplink (transmitted) and downlink (received) signals, which are rapidly changing. Such hopping sequences are generally done upon time-based beacons radiated by the satellite and an encrypted traffic key. Synchronisation between remote users and the master satellite shall then be done upon the specific algorithm. Certain systems do also have a re-hop function on the downlink to enhance the protection on this link as well.

EXAMPLE OF FREQUENCY HOPPING PROTECTION AGAINST RF JAMMING



Frequency hopping concept with a single fixed narrow band jammer in red. The blue carrier is jammed at slot N+1 but avoids interference on slots N and N+2.

Technological factors and trends

OTM technological characteristics, current practices & challenges

OTM SATCOM terminals now offer **broadband connectivity**, allowing for the transmission of high data throughputs. The SWaP (Size, Weight, and Power) factor of the user terminal has been significantly improved over the past years, with miniaturised terminals of high power being available on the market. Due to the mobility of the terminals, full-time dynamic antenna steering, satellite/beam handover management, robustness to fast Doppler shift changes, and robustness to **propagation conditions** are required.

The precise knowledge of the satellite's **orbital position and velocity** through recent orbital data and accurate orbit propagation algorithms is crucial. Furthermore, precise location/velocity and attitude (Roll, Pitch, Yaw) of the moving terminal must be known in real-time thanks to GNSS and local sensors. In case of directional antennas, the antenna must be able to track the satellite while keeping its beam steered in real time, dynamically compensating for both the satellite and the user terminal movements. Depending on the terminal and the satellite's relative velocities, the antenna must have tracking speed and accuracy characteristics that can exclude certain types of technologies.

For instance, a ship with an OTM terminal tracking a GEO satellite will not need an antenna robust to sudden changes in the user terminal's direction. In this case, a **motorised mechanically steered parabolic antenna** under a radome is sufficient. On the other hand, an airplane cannot rely on such antenna technology and must use an **Electronically Steerable Antenna** (ESA) for two main reasons: **fast steering** and **antenna aerodynamics**. The use of ESA is becoming more frequent, enabled by the cost decrease in producing such advanced technology, such as Digital Beam Formers and associated signal processing units (FPGA, ASICS). The flexibility and reliability of ESA must be balanced by generally lower antenna performance (directivity, cross-polarisation discrimination, and level of side lobes). On top of that, terminal movements imply a necessary loss of **beam pointing precision** (compared to fixed), which could increase interference on adjacent satellite systems. Specific ITU regulations were put in place to address this issue for MSS systems.

An OTM terminal will also face possible satellite and/or beam handover. **In secure SATCOM, a 'make-before-break' satellite handover strategy is recommended, but this implies two spacecraft tracked simultaneously**. This will require a modem capable of dealing with both links simultaneously, and in case of directional antennas, a dual-antenna terminal system (or an ESA). From a network management standpoint, the challenge is to adapt the satellite and the beam through which the traffic should be routed for the user terminal in real-time. The process requires the Network Management System (NMS) to know the terminal location and moving direction at all times, as well as the satellite positions and beams. This is done through signalling messages exchanged between the NMS, the communication hubs (at the anchor station), and the user terminal, through the current satellite link, to prepare the task of the upcoming handover. The terminal then can anticipate the next satellite to be pointed at, and the next frequency/polarisation on which to expect the link to be established. As SATCOM systems become more complex in terms of topology and the number of spacecraft, the orchestration of OTM traffic becomes challenging.

The current **state of the art of OTM terminal technology** includes the use of multi-orbit systems that integrate different constellations at different altitudes. This can provide enhanced redundancy for a more secure SATCOM system, as well as increase capacity and flexibility. Until recently, this was a technical challenge since the different systems used different frequencies, waveforms, etc., requiring multiple antennas, frequency converters, and compatible modems. **Software-Defined Radios (SDR)** now make the user terminals more agnostic to the different constellations' signal characteristics.

OTP technological characteristics, current practices and challenges

OTP terminal faces most of the technical challenges OTM terminal must address, especially when dealing with NGSO constellations or multi-orbit systems. However, the fact that the terminal is static for the OTP terminal greatly simplifies the tracking/handover issues, as well as the network management and data traffic orchestration.

The use of parabolic dishes with greater diameters than OTM (e.g. 2 m versus 0.5 m typically) ensures higher performance and beam directivity capabilities, although they are not capable of the fast change of pointing direction that are needed by Communications On-The-Move.

The current trend is to make sure OTP terminal is easier to transport, faster to mount/dismount (from a SUV-type size to a truck's trail size), and that secure SATCOM communication is established quicker (user terminal location and orientation fix, orbital data recovery, and orbit propagation, automatic antenna pointing and tracking, SATCOM system logon, traffic signalling, etc.).

The electronical beam forming advantages appear less obvious than for OTM uses, but the deployment of secure SATCOM NGSO constellations, as well as the multi-orbit approach, may impose such technology in the OTP, over classical parabolic dishes.

Future trends for OTM/OTP

These are the future directions that OTM and OTP user technology type will move towards:

- **Reduced SWaP**: the mobility required for OTM/OTP pushes the engineering towards smaller (miniaturisation), energy-efficient equipment while ensuring the same level of performance and security, for the development of lighter communication units for highly mobile operational needs.
- **Improved MODCODS**: future advances in secure OTM/OTP technology will focus on increasing bandwidth capacity and network availability. Innovations will include more robust, more energy-efficient and spectrum-efficient waveforms, as well as the development of waveforms specifically designed for security, and robustness to eavesdropping, jamming, or spoofing.
- **Improved cybersecurity**: such improvement is done through TRANSEC & COMSEC, through specific hardening of the hardware, especially encryption keys or frequency hopping random sequence management.
- **Software-Defined Radios**: this upcoming trend is the generalisation of SDR for signal processing functions, very soon after the RF antenna interface. This will enable more flexibility, and adaptability to future signal characteristics, and improve compatibilities to multiple satellite systems, in the multi-orbit environment that the secure SATCOM is aiming towards.
- **Enhanced systems integration and automation**: OTM/OTP will likely involve greater integration with other tactical networks and infrastructures, along with more automated network management tools to handle the growing complexity of the SATCOM systems as well as the increasing importance of NGSO constellations.

Focus on security and standardisation efforts

General considerations about OTM/OTP user technology types availability

Mobile secure SATCOM terminals, particularly OTM, allow ground personnel to maintain continuous communication while in transit. This capability is crucial for modern, highly mobile scenarios or dynamic operations (e.g. search & rescue operations during large scale natural disasters). Their bigger size compared to other mobile units, like manpacks, enables them to provide better throughput performance and better spectral efficiency and to increase the satellite link availability, making them well suited for field headquarters or advanced command posts. On top of that, a larger antenna aperture will yield a narrower beam, which is more difficult for a possible opponent to intercept or to jam.

The OTP terminals, although quite powerful, are relatively bulky and heavy and cannot be carried by a human being. Hence, they must rely on a specific platform for transportation (e.g. vehicle roof, truck trailer). Consequently, there is no more mobility advantage, compared to user terminals such as the fly-away terminal. The relatively higher RF power in both transmission and reception also comes with the need for electrical power supply, a separate unit which also needs to be transported. Electronically Steerable Antennas (ESA) have become a game-changer for OTM applications, even if they are still very expensive for the average user. Their ability to rapidly steer their beam, or even form multiple beams to handle satellite handovers, is allowing seamless tracking even during high-speed user terminal movements. This technology alone has permitted the availability of the link during those move phases to increase. In addition, ESA technology is decreasing both the risk of failure and the need for maintenance, since less mechanical parts are used (and mechanical parts are sensitive to harsh environments such as sand or heavy humidity). These antennas are also a powerful technology for the terminal to provide **flexibility and adapt to multi-SATCOM systems and multi-orbits**, offering an increased resilience to threats by having more possible backup solutions in-orbit.

Finally, modern OTM/OTP user technology types can support **multiple frequency bands, including Ku-, Ka-, and X-bands** particularly used for broadband SATCOM. This multi-band functionality provides greater flexibility in selecting satellite networks and enhances availability.

Considerations over upgradability

Here are some elements to consider to quantify the need of upgradability associated to improved resilience:

- **Situational awareness**: OTM/OTP user technology types enable, from an advanced outpost, real-time information sharing, tactical maps and data, command and control capabilities for vehicles, aircraft, UAV, and naval vessels, significantly improving situational awareness.
- **Ruggedisation**: Modern OTM/OTP user terminals are designed to withstand extreme environmental conditions and to meet high standards such as MIL-STD-810, undergoing rigorous testing (e.g. shock and vibration, dust and sand infiltration, extreme temperatures, electromagnetic interference, salt spray and corrosion for maritime environments) to ensure field readiness and combat durability.
- **Electromagnetic signatures recognition**: Despite efforts to reduce observable signatures, the electromagnetic emissions from OTM/OTP user technology types can potentially reveal the position of military units. Ongoing research focuses on developing low-profile and low-observable antenna designs. Electronically steerable antennas, which for these terminals are often used as flat panels/direct radiating arrays, are excellent candidates to comply with such requirements.
- **Low Probability of Intercept/Detection (LPI/LPD)**: Some advanced systems are designing specific antennas, guaranteeing higher main lobe gain, and lower antenna side-lobes to add an RF protection, while implementing frequency hopping and spread-spectrum waveforms (TRANSEC), thereby making communications harder to detect or jam.
- **Cybersecurity robustness**: As OTM/OTP user technology types become more software-defined and network-integrated, they may become more susceptible to cyber-attacks. Ensuring robust cybersecurity, in particular within a military environment, is a top priority.

Standardised SDRs and end-to-end interoperability capabilities

Software Defined Radios (SDR) technology applied to OTM/OTP user terminals offers significant advantages. Firstly, the SDR technologies can eliminate the need for multiple physical modems, reducing the SWaP factor, to increase mobility and length of remote off-the-grid operations. Secondly, SDR technologies enhance interoperability as they allow terminals to adapt to different existing communication protocols and frequencies through software updates rather than hardware changes. Thirdly SDR offer a faster adaptation of the terminal to innovative air interfaces: as new communication standards emerge, such as 5G, SDR-enabled terminals can be updated to support them without requiring complete hardware replacements and associated complex logistics.

Licensing and compatibility challenges

In order to fully leverage the SDR possibilities and avoid modems duplication, several elements must be considered: **standardised SDR frameworks** – developing common SDR frameworks across different manufacturers and military branches could enhance interoperability; **flexible licensing models** – implementing more flexible licensing models for SDR software could allow military units to adapt their communication capabilities as needed without excessive costs; and **security considerations** – ensuring that SDR-enabled terminals maintain robust security measures is crucial, as software-based systems may introduce new vectors for cyber attacks.

Deployable, handheld and secure IoT user technology type: overview

Deployable and handheld terminals

The **deployable user terminals** share characteristics with the OTP terminals presented earlier. However, the key difference is that they are **more compact** and **easier for users to deploy** and install. **Deployable fly-away terminals** are equipped with directional antennas and can include parabolic antennas ranging from 0.5 m to 2.4 m in size. ESA antennas can also be used with fly-away terminals. Fly-away terminals are **transportable, small-sised units** that can usually be installed and operated by one or two people. Their VSAT or ESA antennas tend to be smaller than those used in OTP systems. These terminals generally support C-, X-, Ku-, and Ka-bands and are used for demanding data transmissions of voice, images, video, and data. Aside from their size and focus on rapid deployment, these terminals can be ruggedised to varying degrees depending on the secure SATCOM user needs and operational environment.

Manpacks are deployable terminals that **bridge the gap between fly-away** and **handheld units**. They allow secure SATCOM users to carry the antenna and terminal components (such as a more robust power source) in a backpack, offering better performance and functionality than a simple handheld terminal. These terminals are also heavily ruggedised in order to operate in harsh environments. These terminals carry either small directional antennas operating at higher bands such as X, Ku and Ka, or operate at low frequency bands such as L-band, usually equipped with omnidirectional and isoflux antennas.

Handheld terminals are lightweight, with weights ranging from hundreds of grams to a few kilograms, depending mainly on the weight of the batteries. For a compact design, handheld terminal are typically equipped with an omnidirectional antenna that can be integrated into the terminal or carried in backpacks or held by the operator.

The power sources are batteries with variable usage times, typically ranging from 4 to 10 hours of continuous usage. These terminals transmit voice and data (Kbps) and usually operate in L, UHF, and VHF frequency bands. Secure SATCOM users can incorporate encryption and various waveforms. They tend to be highly ruggedised to withstand harsh conditions, including extreme temperatures, water immersion, and shock impacts. Handheld terminals may also connect to external support infrastructure, such as hand-supported antennas, larger antennas, power sources, and other equipment installed in vehicles.

Secure IoT terminals

The Internet of Things (IoT) is an evolution of Machine-To-Machine (M2M) technologies. Compared to system architectures that were built for M2M connectivity, **IoT technologies are cheaper, more flexible**, and **less rigid** architecturally, which enables brand-new applications. Within the secure SATCOM section of this report, we will refer to the IoT as a wired or wireless network of uniquely identifiable connected devices that can process data and communicate with each other with or without human involvement. In other words, it is a network of devices that enables objects to exchange information. There are two types of IoT: the terrestrial and the space one which accordingly rely either on the terrestrial network or on the space one. This report focuses on the space IoT, which covers more areas and has greater availability in remote locations than terrestrial ones.

The concept of secure IoT comes from the vulnerabilities that IoT and its connectivity can introduce into a system. As it happens to the secure SATCOM concept, secure IoT addresses the availability, confidentiality and integrity of the IoT.

Secure IoT devices and networks must also be designed with robustness to withstand the different operational scenarios of secure IoT. As IoT is usually designed and used with components not fitted to withstand harsh conditions, secure IoT must be hardened to consider the associated operational burdens.

It is worth highlighting that IoT terminals are usually compact and have very low SWaP with low cost. They also have a low data rate and low frequency (in most cases at L- and S-band).

IOT SECURITY MEASURES

	Measures
Securing IoT devices	• Hardware temper resistance. • Hardware protected with firmware that can be updated/patched. • Ensure hardware performance through dynamic testing to establish baseline security. • Ensure data protection on the device disposal (proper sanitation of device and data to avoid usage).
Securing IoT network	• Strong user authentication such as context-aware authentication (CAA). • Strong encryption and secure protocols, such as IPSec Transport Layer Security or Secure Sockets Layer (TLS/SSL). In cases where encryption is not applicable for safety messages, digital signatures can be employed. • Minimise device bandwidth, limiting the amount of network traffic IoT generates. • Division of the network into smaller local networks using Virtual LANs (VLANs), IP address ranges, or a combination of both.

Main characteristics of deployable terminals

	Deployable fly-away	Deployable directional manpack	Deployable omnidirectional manpack
Main capabilities	• **Use of directional antennas (VSATs or ESA).** • **Throughputs of ~1 to 40 Mbps**, for voice, data, and video/images. • Terminals usually operate in one or two bands. Including C, X, Ku, Ka-band.	• **Use of directional antennas (VSATs or ESA).** • **Throughputs 1 to 5 Mbps** using mainly for voice and data. • Terminals usually operate in one or two bands. Including X, Ku, Ka-band.	• **Use of omnidirectional and isoflux antennas.** • **Throughputs of ~15 kbps to 1.5 Mbps** mainly for voice and data. • Terminals usually operate in one or two bands. Including L-band, S-band.
Deployment/installation of the terminal in the field	• Terminal deployment and set ups remain simple for a low level of training. • Pointing and non-blocking line of sight are the main challenges while deploying the antenna. • Set up of power source and connections with the local network are simple aspects.	• Terminal deployment and set ups require none to very low level of training. • Small-size and easy connections to facilitate the deployment of the installation. • Line of sight remains an important parameter. • **Plug-and-play philosophy.**	• Terminal deployment and set ups require none to very low level of training. • Small size and easy connections to facilitate the deployment of the installation. • Line of sight remains an important parameter but pointing of the antenna is not so critical. • **Plug-and-play philosophy.**
General experience to operate the termi-nal	• Some level of training is needed to install and connect the terminal. • Operation of the terminal remains simple and once the connection is established, even personnel with no training can operate the terminal.	• **Easiness of terminals to operate in the field.** • Very low level of training required to operate once the connection is established.	• Easiness of terminal to operate in the field. • A low level of training is needed to configure the terminal. The terminal can be pre-configured to ease or eliminate this. • **Operation with the terminal remains simple and very basic concepts should be needed to operate.**
Time to deploy and set up connectivity	• **Deployment might take from 5 to 30 minutes.** • Initial configuration and signal acquisition from 5 to 10 mins. • Connectivity once the terminal is configured and working should remain stable with instant access to the service.	• **Deployment and setting-up of the terminal take few minutes.** • Initial configuration and signal acquisition take less than five minutes. • Connectivity once the terminal is configurated and working, should remain stable with instant access to the service.	• **Deployment might take few minutes.** • Initial configuration and signal acquisition can be almost instant, especially if the terminal is pre-con-figured. • Connectivity should remain stable while using the terminal.
Considerations about operational environ-ment	• **Terrain might need to be as flat as possible to fa-cilitate a consistent reference for terminal pointing and acquisition operations.** • Terrain must have a clear line of sight and be free of obscuring elements. • Weather and wind might be a consideration depend-ing on the size of VSAT, so the terminal will remain stable.	• Terrain must have a clear line of sight and be free of obscuring elements. • **Power autonomy might be limited.**	• Line of sight and be free of obscuring elements. • **Omnidirectional antenna is easier to jam and/or to listen to.** • Power autonomy might be limited.
Future trends	• Multi-orbits, multi-constellations. • Multi-frequencies. • Virtualisation of the integration with local network. • Auto tracking technologies (both mechanical and electrical).	• Multi-orbits, multi-constellations. • Multi-frequencies. • More efficient power source. • Auto tracking technologies (both mechanical and electrical) in case of directional antenna.	• Multi-orbits, multi-constellations. • Multi-frequencies. • Smaller terminal SWaP factor. • 5G integration. • More efficient power source.

Main characteristics of handheld and secure IoT terminals

	Handheld	Secure IoT
Main capabilities	• Use of omnidirectional antennas. • **Throughputs of ~15 kbps to 500 kbps**, for voice and data. • Terminals usually operate in one band. Usually VHF, UHF, L-band.	• Use of directional antennas (VSATs or ESA) or omnidirectional. • **Throughputs of ~15 kbps to 1.5 Mbps** in narrowband, for data. • Terminals usually operate in one band. Including VHF, UHF, X, Ka, Ku, L-band.
Deployment/installation of the terminal in the field	• Terminal configuration might need some level of expertise. Terminals can be pre-configurated to ease the deployment in the area of interest. • **Users don't need specific training.** • Basic usage is meant to be easily and quickly teachable. Thus any user can operate this terminal with minimum formation and time.	• **Installation must be planned and designed in order to minimise security vulnerabilities**, such as physical access and tempering with the terminal, RF interference and possible jamming. • Installation must consider the design of the IoT network. • Installation must take care of the interface with other networks/systems.
General experience to operate the terminal	• A low level of training is needed to configure the terminal. The terminal can be pre-configurated to ease or eliminate this hurdle. • **Operation with the terminal remains simple and very basic concepts should be needed to operate it.**	• User knowledge on the installation operation varies depending on the complexity of the IoT network and interfaces with its surrounding systems and/or another network. • **Basic level of knowledge of network architecture, set up and configuration needed.**
Time to deploy and set up connectivity	• **Deployment might take from 5 to 15 minutes.** • Initial configuration and signal acquisition can be almost instant, especially if the terminal is pre-configured. • Connectivity should remain stable while using the terminal.	• **Deployment and setting-up of the terminal takes minutes.** • Set-up of the IoT network and terminals might take minutes, hours, or longer periods depending on the complexity of the network. • IoT design and planning time for the secure IoT network remains non-negligible.
Considerations about operational environment	• Line of sight and be free of obscuring elements. • **Omnidirectional antenna is easier to jam and/or to listen to.** • Power autonomy might be limited.	• Terrain must have a clear line of sight and be free of obscuring elements. • **RF environment, as the terminal is easy to jam or listen to.** • Physical environment, specifically to avoid tampering or manipulation by non-authorised personnel.
Future trends	• Multi-orbits, multi-constellations. • Smaller terminal SWaP factor. • 5G integration. • More efficient power source.	• **Integration in Broadband, 5G or 6G ecosystem.**

Typical use cases

Deployable and handheld use cases

Similar to the OTM and OTP use cases, deployable fly-away and handheld terminals target situations where a secure SATCOM connection needs to be established in areas or zones that typically do not require such a service, or where traditional communication networks are absent or down (e.g. terrestrial networks after a natural disaster). The main advantage of deployable fly-away and handheld terminals is that they offer a more flexible and cost-effective solution compared to OTM/OTP user technology type. While OTM/OTP systems usually require integration with a mobile platform, deployable fly-away or handheld terminals can be used directly without the need for any additional platform, simplifying their deployment. Deployable user terminals can quickly adapt to the user's needs without the burden of maintaining equipment integrated into mobile assets, as is the case with OTM/OTP systems. This flexibility is particularly useful in scenarios such as humanitarian aid, civil protection, law enforcement, or, in the EU-specific context, the EU External Action Services (EEAS).

Secure IoT use cases

For secure IoT, the use case scenarios differ. IoT can be either installed on mobile platforms (e.g. trains and ships) or can be fixed (e.g. powergrids, pipelines or tsunami prevention).

Secure IoT pertains to more critical functions where applications must be both reliable and secure. It is associated with critical infrastructures, including energy, industrial, financial, cyber, and space sectors. Uses of secure IoT range from monitoring the health status of infrastructure to anomaly detection and alerts, logistics, maintenance, and security features. Overall, secure IoT provides a reliable and guaranteed network for monitoring and tracking the evolution of various parameters and functions, or the status of specific infrastructure, assets, or areas of interest.

Three existing operational examples

To illustrate use cases associated to the deployable and handheld user technology type, three operational examples are detailed below:

- **Humanitarian Aid and Civil Protection** – The EU's humanitarian action embodies the principle of solidarity, which ensures that the EU provides assistance, relief, and protection to disaster victims. Humanitarian aid missions encompass both civil protection and humanitarian assistance within Europe and globally. Civil protection overlaps with humanitarian aid, addressing the needs of EU civilians concerning disaster prevention and preparedness. Disasters, whether natural or man-made, can occur anywhere and at any time. This makes deployable fly-away and handheld secure SATCOM solutions particularly suitable for humanitarian aid and civil protection. These solutions enable connectivity in disaster areas, facilitating coordination among humanitarian and civil protection teams, restoring connectivity services in affected regions, supporting telemedicine or similar remote-assisted aids, and enabling critical data flows for situational awareness and crisis management. Deployable secure IoT plays a crucial role in situational awareness and crisis management, allowing for the establishment of sensors and networks to monitor evolving situations (e.g. sensors to detect structural integrity in damaged buildings or to monitor food distribution and storage).
- **Law enforcement** – As demonstrated with OTM/OTP systems, law enforcement interventions benefit from mobile assets. Handheld and fly-away terminals also support secure SATCOM services for various law enforcement operations. Real-time monitoring and in-the-field communication and coordination benefit from the portable and compact nature of these user terminals. Unlike OTM/OTP systems, these deployable solutions offer greater flexibility and discretion in deploying secure SATCOM services. Law enforcement missions typically involve policing, investigations, emergency measures, and support services aimed at enforcing the law, preventing and controlling crime, maintaining peace and order, and ensuring public safety.
- **EEAS delegations and missions** – The EEAS relies on an extensive network of the EU's diplomatic presence worldwide, including European civil servants, diplomats from EU Member States' foreign services, and local staff in host countries. The EEAS is responsible for the CSDP, which implements military and civil assistance operations. The EEAS uses secure SATCOM as a primary connectivity source worldwide, with services provided not only by OTM/OTP user technology type but also by deployable fly-away and handheld terminals. The latter offers flexibility depending on the scenario and communication needs of different EEAS actors.

Civil protection can benefit from secure SATCOM connectivity through fly-away and handheld terminals that enable response teams to access independent secure connectivity for coordination of their activities in any scenario. The pictures depict examples from the Emergency Response Coordination Centre in Brussels.

Terminals’ main technology considerations

The deployable fly-away, the handheld, the manpacks and the secure IoT terminals could be considered as a subset of the OTM/OTP, even though IoT terminals can also be “fixed”. As such, they have a similar general architecture. Moreover, this mobile nature implies that the technical specificities shown for the OTM/OTP are also present, but they need to be balanced with the specifics of these small-sised user terminals.

Changing the relative position of the satellite and/or the terminal

When directional antennas are considered, and in the case of a deployable fly-away (or a fixed IoT terminal), the pointing must be done once at start-up if using a GEO satellite or done dynamically for a LEO satellite. **In the case of a moving IoT terminal** with a directive antenna, since the terminal is potentially also in movement, antenna steering must always be maintained dynamically. The tracking antenna subsystem first needs to know in which direction to point, then apply this parameter to the antenna beam steering. The following steps are performed:

1. Using external orbit data (e.g. ephemeris or TLE), The **satellite orbit determination subsystem** determines the position and the trajectory of the satellite to predict its evolution.
2. The **GNSS receiver** determines the location and the velocity vectors of the terminal (it also provides a precise time/frequency reference, which can be crucial in certain operations).
3. The **terminal attitude determination module** uses different sensors (compass, gyroscopes, accelerometers) to derive the position in Roll, Pitch & Yaw of the terminal with respect to a reference frame.
4. The beam is either steered mechanically (parabolic dish) or electronically with direct radiating arrays (flat panel antennas).
5. Some terminals can be equipped with an **antenna tracking receiving chain**, which can be used in close-loop to keep tracking by locking on the received signal (e.g. mono-pulse tracking, step-track).
6. The **Antenna Control Unit (ACU)** compiles all these inputs to derive the **steering direction** of the antenna beam. Note that the elevation visibility mask around the terminal may also be entered as an input parameter to the ACU.

As a **deployable fly-away** terminal uses a smaller antenna than a typical OTP terminal, it will have **fewer beam pointing accuracy constraints**, due to the wider main beam. Therefore, the antenna control sensors and actuators do not need to show the same performance. In addition, **handheld, some manpacks, and most IoT** (fixed or mobile) terminals will implement an **omnidirectional or isoflux antenna** (typically a whip antenna), which means that the throughput performance is drastically decreased, but that antenna pointing is unnecessary. It therefore allows all the related equipment to be dispensed with, and the **UT’s overall architecture becomes much simpler**.

Satellite handover/beam handover

When using **NGSO SATCOM constellations**, the need for a satellite handover is mandatory as spacecraft are constantly moving in and out of the visible field of the user’s location. This may require, in the case of a ‘make-before-break’ strategy, the use of two parabolic antennas to maintain seamless communication. Electronically steerable antennas provide a solution for deployable terminals as they can directly form two distinct beams, while mechanically steered antennas have only a single main beam (which is not suitable for deployable fly-aways because the entire equipment would need to be duplicated).

In addition, for **handheld or moving IoT secure users**, the terminal may travel through different satellite ground beams. Since adjacent beams will likely use different frequencies or polarisations, the terminal will need to use two data carriers (two in transmission and two in reception) simultaneously to ensure seamless communication. This is managed at the modem level. Both of these handover types also need to be managed at the network level to define the data routes. On the other side, the terminal must also manage these handovers (the traffic plan can be received through the satellite link). The terminal will also need to have feeds that allow both polarisations to be received to allow the handover between beams of different polarisations.

For the **handheld, manpack and IoT** (fixed or mobile) terminals using omnidirectional or isoflux antennas, the **satellite handover constraint is not present anymore**, although the beam handover is still a possibility. The need for a full-time, seamless, real-time communication link in the case that IoT is not always present, as **the IoT device can re-transmit its data packets on a regular basis**, and that typical IoT-constellations are LEO satellite practice on-board data storage until they pass over an ‘anchor’ station. This **reduces the operational and technical constraints** on these particular IoT links.

Very low SWaP constraint

Required to be portable by a human being, these types of secure SATCOM terminals are constrained by their SWaP factor, which will impact the usable equipment (e.g. power supply/batteries and antenna size/thermal control), which will impact the performance. Unless this is partially compensated by the gain and power of the antenna, these will be limited to low-to-medium throughputs, which may not be an issue for some use cases such as IoT narrow-band. The size constraint will also push towards more integrated equipment (e.g. SATCOM modems already including LNB or BUC), with the limit being the handheld that can encompass all the functions into a single box. However, the terminal performance is much higher than low-to-medium throughputs with the planned dedicated direct-to-handheld constellations, despite still the low SWaP of such user devices, but thanks to the large antennas on board the satellites of such systems.

Architecture of deployable, handheld and IoT terminals

By essence, a simpler architecture and integration

The deployable fly-away and directional manpack user technology type has similar characteristics as the OTP terminals. The main difference is a lower SWaP factor, due to the **size reduction of the antenna** (parabolic or electronically steerable) diameter, smaller and less powerful RF amplifiers, and a first level of integration of RF equipment such as the **Tx/Rx Antenna, BUC, LNB, GNSS antenna and receivers in a same unit**, with an easy-to-transport or even integrated power supply unit. The reader may refer to the OTP terminals to get information regarding their general architecture and components.

IoT terminals can use an electronically steerable antenna (ESA) to enhance the link performance with respect to omnidirectional antennas. However, since the **IoT is by nature narrow-band and low-power satellite links, the use for ESA remains quite limited**.

Regarding handheld, omnidirectional manpack or IoT terminals using omnidirectional or isoflux antennas, the architecture is much simpler, as **antenna pointing is not required**. However, most of these terminals keep a GNSS receiver, which can be useful to send the location of the terminal through the satellite link, as well as to provide time and frequency reference to the frequency converters and the modem.

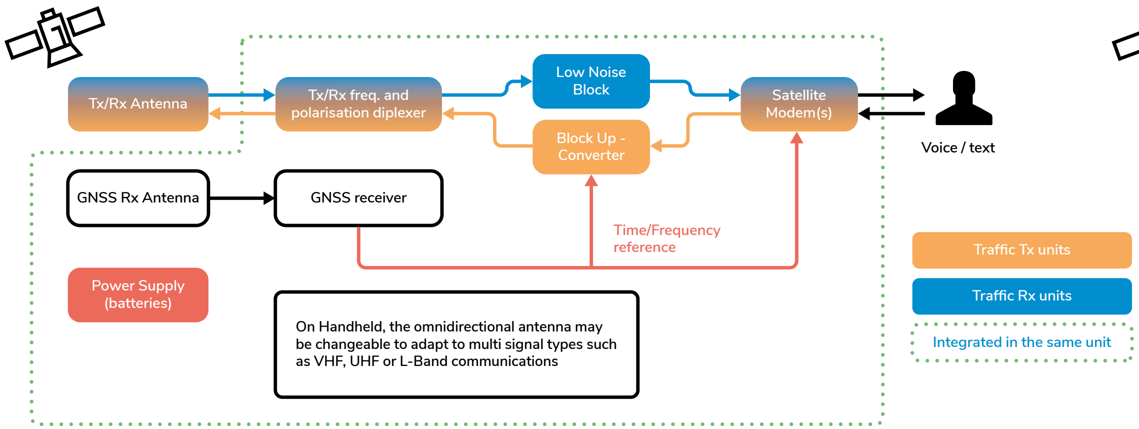
Nevertheless, the classical transmit/receive architecture is kept (with a real effort especially on IoT) **to rely on cheap (COTS), lightweight, small, and low power** (a few Watts) **consumption units** (small omni antennas, optimised electronic chips for demodulation and modulation). **In secure SATCOM, these units are ruggedised to withstand difficult environmental conditions**.

For IoT terminals, in case of the (optional) presence of a GNSS receiver, the GNSS antenna might be directly integrated within the unit. The power supply might be directly integrated in the form of batteries, especially for moving IoT terminals.

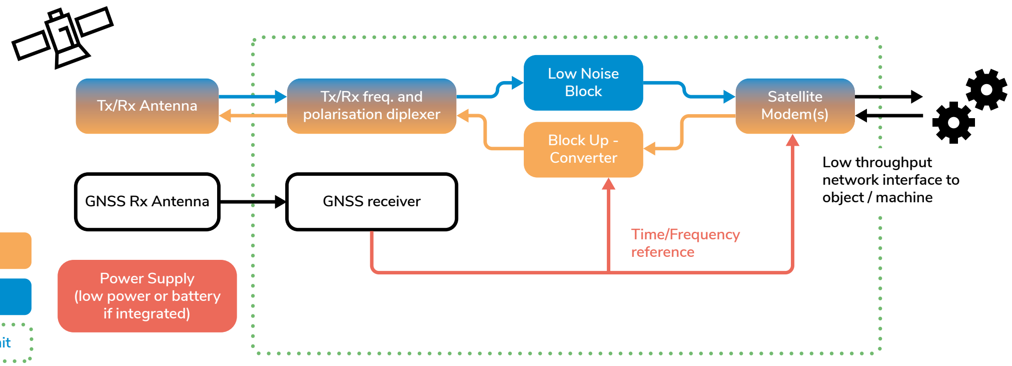
Most of the IoT units do not have a receiving chain but are designed to transmit only (e.g. for monitoring purposes): the architecture becomes even simpler. In such a scenario, the elements for the Rx in the antenna, in the diplexer, in the modem, but also the LNB, are not needed.

	SATCOM system orbit	
UT type	**GSO**	**NGSO**
Deployable fly-away	Single tracking dish antenna or single ESA	Dual tracking dish antenna or single ESA
Directional manpack	Single tracking dish antenna or single ESA	Dual tracking dish antenna or single ESA
Fixed IoT	Omni or single ESA antennas	Omni or single ESA antennas
Moving IoT	Omni or single ESA antennas	Omni or single ESA antennas
Handheld	Omni antenna	Omni antenna
Omnidirectional manpack	Omni or isoflux antenna	Omni or isoflux antenna

GENERIC ARCHITECTURE OF A HANDHELD/OMNIDIRECTIONAL MANPACK TERMINAL



GENERIC ARCHITECTURE OF AN IOT TERMINAL



Characteristics of signals used

Secure SATCOM deployable, handheld and secure IoT terminals all utilise specific signals, both in terms of frequency and waveform, to enhance security and robustness and to meet their operational requirements.

Favouring use of low frequencies for availability reasons

Similar to OTP terminals, deployable terminals with directional antennas, although smaller and less powerful, can be considered as "temporarily fixed" for communication, thus behaving similarly to fixed terminals. Depending on the required service (broadband, narrow-band, voice/e-mail/text) and the SATCOM system used (satellite distance, proprietary waveforms, etc.), they will be compatible with various frequency bands, from L-Band (~1-2 GHz) to Ka-Band (~20-30 GHz). Higher frequencies can achieve greater throughput, but performance at these frequencies can be limited by antenna size and amplifier power, particularly for communication with geostationary satellites. In such cases, the service will have low throughput, and fly-away deployable terminals will rely on lower bands where propagation losses are more manageable, thereby closing the link budget.

Conversely, deployable terminals with omnidirectional antennas, handheld and IoT terminals using omnidirectional antennas must operate in the lower part of the spectrum, historically dedicated to mobile services. The omnidirectional nature of these terminals is considered for the regulation of adjacent SATCOM system interference, and they typically offer relatively low throughput to manage the link budget. Handheld devices generally use VHF/UHF (180-1000 MHz) for tactical military radios, L-Band (satellite phones), or even S-Band (2-3 GHz) for voice/text/low throughput links. For IoT terminals with omnidirectional antennas, state-of-the-art practice involves using UHF/VHF in dedicated IoT SATCOM systems. Standardised 4G NB-IoT allocates spectrum resources with more than 25 channels within UHF and L-Bands. IoT terminals with directional antennas (ESA) can achieve better performance, with some terminals using frequencies up to Ku-Band (~12-14 GHz). IoT terminals typically use narrow-band carriers (a few dozen kHz wide), specifically designed for low power consumption, while deployable fly-away user terminals use more traditional wideband carriers (a few MHz wide).

The **use of lower spectrum bands**, even with limited throughput, provides significant **robustness against propagation impairments**, which is crucial for secure SATCOM. Lower bands, such as L-Band or UHF, are **less affected by rain fade or other weather conditions** as compared to higher frequencies like Ka-Band.

Adverse transmission environments

A key characteristic of tactical secure SATCOM is its robustness in adverse propagation conditions, such as non-direct Line of sight with the satellite or environments that cause RF multipath interference (e.g. trees, overpasses, urban canyons). This is especially true for terminals using omnidirectional antennas, which are more vulnerable to multipath issues. These challenges can be mitigated using specific waveforms and signal processing algorithms, often derived from techniques initially developed for ground cellular networks (e.g. Orthogonal Frequency Division Multiple Access - OFDMA).

COMSEC & TRANSEC to protect the data transmissions

SATCOM transmissions are inherently 'observable' by all users directing their terminal towards a space asset, provided that the terminal is within the same ground coverage area. Similarly, uplink communications can be intercepted by monitoring the electromagnetic environment nearby a ground station or through high-altitude assets (aircraft or platforms over operational theatres). Like OTM/OTP terminals, deployable, handheld and secure IoT terminals must be robust against attacks such as eavesdropping, RF jamming, or spoofing.

Deployable fly-away terminals enhance security as compared to fixed or OTM/OTP user technology types. Being smaller and more mobile, they are easier to evacuate from threat zones and harder for attackers to locate. However, their smaller antenna apertures tend to increase beamwidth and the presence of secondary lobes degrades protection against jamming or eavesdropping. Conversely, handheld or IoT terminals with omnidirectional antennas are particularly vulnerable to eavesdropping (as they transmit in all directions) and jamming (as they receive from all directions). These threats can be mitigated using COMSEC and TRANSEC techniques, such as advanced encryption key distribution, Direct Sequence Spread Spectrum, or Frequency Hopping techniques, as described in the OTM/OTP section.

Note that **IoT terminals**, being non-human-operated, are **more susceptible to direct physical threats**. All these terminals can also be affected by **GNSS jamming or spoofing**, which can hinder the embedded GNSS receiver from computing a reliable geolocation. For terminals with automatic antenna tracking subsystems, spoofing **could render the device unusable**. Mitigation of GNSS spoofing can be achieved by implementing multi-GNSS constellation receivers, augmented/differential geolocation techniques, terrestrial geolocation systems, or additional PNT sensors/systems.

Technological factors and trends

Deployable fly-away and manpack driven by SDR and ESA

Deployable fly-away and **manpack** terminals are becoming increasingly compact, lightweight, and easy to set up for rapid deployment with high mobility in crisis areas, while remaining robust in difficult environments. These rely on several key technological factors:

- **Software-Defined Radio** at the modem level makes it easier to include multi-bands and multi-orbits capabilities, compatible with various waveforms/TRANSEC techniques, and adaptable to future advances. These are made possible by advances in electronics SWaP factors, the increased computational power of signal processing chips, and the reduction in costs.
- **Electronically steerable antennas** accelerate the acquisition and tracking. They are also lighter, easier to handle, and enable (to the extent of their capability due to limited antenna aperture) multi-orbits capabilities. These are made possible by advances in RF signal processing for Beam Forming Networks (BFN).
- **Ruggedised designs** are definitively a must for harsh environments (shock, dust, sand, extreme temperatures, water, electromagnetic fields, etc.).
- **Integrated power systems** are needed for extended off-grid operations.

SWaP is at stake for handheld devices

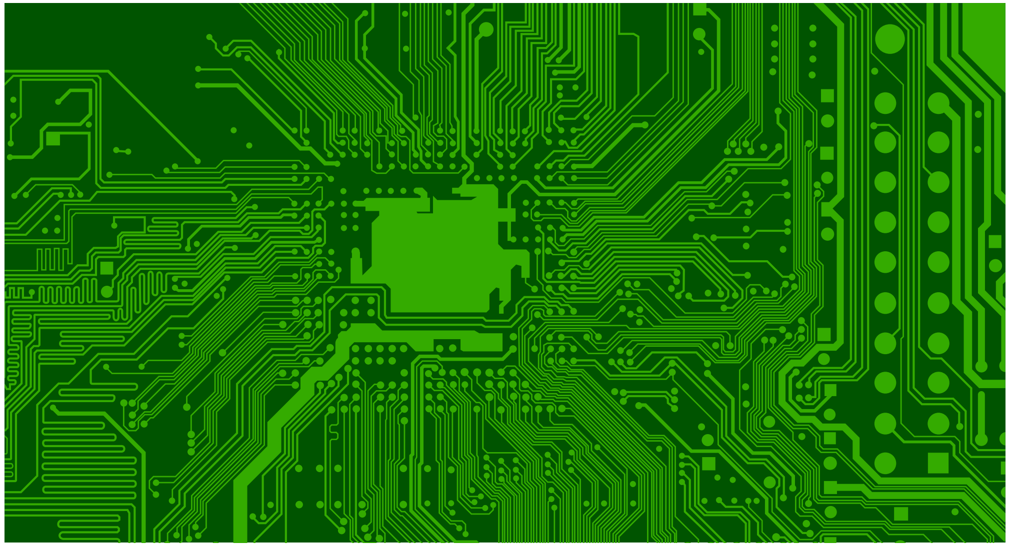
Handheld satellite phones, satellite tactical radios, and data devices are evolving to provide more capabilities in smaller SWaP factors by targeting:

- **Advanced chipsets** enable more processing power with less electric power consumption (increased energy efficiency).
- **Improved antenna** designs for better signal reception.
- **Hardened security features** like encrypted communications (COMSEC) and anti-jamming (TRANSEC), along with ruggedised equipment are vital for usages that are generally of key importance for the life and the mission of its holder.

IoT as a key node accessible via satellite network

Satellite-enabled IoT devices are becoming an important part of secure SATCOM networks, especially for remote monitoring and asset tracking. The main technological factors addressed are:

- **Low-Power Wide-Area Network** (LPWAN) technologies are well suited for satellite links and for objects that are not supposed to be easily operated.
- **Miniaturised satellite modems and antennas** reduce the SWaP factor of these terminals.
- Edge computing capabilities are generally mandatory for local data processing, which reduces the data volume that needs to be transported through the satellite link and therefore the time to transmit.
- Advanced encryption and authentication protocols (COMSEC/TRANSEC) help to avoid any signal interception.



Future trends

The following **deployable** terminals major trends have been identified: (1) increased automation and simplified user interfaces – these terminals are getting usable with very limited knowledge of SATCOMs; (2) integration of AI for predictive maintenance and optimised performance; and (3) support for higher throughput and lower latency communications (compatibility with LEO satcom constellations' signals such as Starlink).

The **handheld** terminals future highlights will probably be: (1) in the case of satellite phones, convergence with smartphones for dual-mode terrestrial/satellite operation (in particular in the frame of 5G NTN advances); (2) enhanced location services and situational awareness features (e.g. notification of natural disasters or other nearby threats; and (3) higher throughputs capabilities.

The development of the **secure IoT** terminals rely on: (1) terminal integration with emerging LEO satellite constellations (e.g. either IoT-dedicated such as Sateliot or Kinéis, or SATCOM generic such as Starlink) for global coverage; (2) hybridisation of these devices for terrestrial/satellite connectivity to improve link reliability; and (3) development of industry-specific IoT solutions (e.g. maritime, agriculture, energy, security), optimised for their own use cases.

Focus on 5G NTN secure SATCOM integration

5G NTN integration as a major opportunity for lightweight terminals

The main **standardisation** effort at the telecommunication level is focusing on RF (frequencies, MODCOD(s), waveforms, antenna techniques, multiple access schemes), lower layers of network protocols, and cyber-security protocols. One of the main efforts has been the 5G NTN standardisation and integration led by the 3GPP. Since Release 17, the focus has been on the integration of SATCOMs within the terrestrial 5G eco-system. This integration aims to enhance global connectivity by enabling interconnectivity between systems, particularly for secure SATCOMs, increasing reliability and resilience by providing backup solutions in case of failures, crises, threats, or disasters.

The core network now differentiates between various satellite systems' orbits (LEO, MEO, GEO) and 5G NR (New Radio) radio access types (WB-EUTRAN, NB-IoT, LTE-M, etc.). Release 18 studies focused on management aspects of IoT NTN, including network resource models and performance measurements. Some ongoing research aims to develop a unified air interface for both terrestrial and NTN in the 'after 5G' telecommunications era, going beyond the modified 5G NR air interface currently used for NTN. The integration of the terminals within the 5G NTN framework presents both **advantages** and **drawbacks** for secure SATCOM applications.

5G NTN BENEFITS AND DRAWBACKS

5G integration advantages	5G integration drawbacks
Global coverage: 5G NTN will allow for seamless connectivity in off-the-grid and hostile environments, crucial for secure SATCOM operations.	**Interoperability**: integrating proprietary telecommunication systems (e.g. waveforms, COMSEC, TRANSEC) with standardised 5G NTN protocols may create vulnerabilities or compatibility issues.
Resilience: The combination of terrestrial and non-terrestrial networks will provide redundancy and increased survivability of communications.	**Increased attack surface**: The convergence of terrestrial and satellite networks could potentially expand the attack surface for adversaries, creating more potential vulnerabilities.
Higher data rates: 5G NTN will enable faster data transmission, supporting advanced applications like real-time situational awareness and tactical telecommunications (e.g. unmanned aerial vehicles).	**COMSEC algorithm vulnerability to quantum computing**: As quantum computing progresses, current encryption methods used in secure terminals may become vulnerable.
	Artificial Intelligence/Machine Learning: While AI/ML offer enhanced security capabilities, they also introduce new complexities and potential vulnerabilities if not properly implemented.

© Vladimir Kazakov/shutterstock.com

Future research and development opportunities in 5G NTN

Future research and development for critical and emergency response applications will capitalise on the opportunities presented by 5G NTN integration that will mostly focus on:

- The developments of **quantum-resistant encryption methods** through PQC (Post-Quantum Cryptography) algorithms, along with Quantum Key Distribution techniques and technologies.
- The enhancement of the network's **physical layer security** in conjunction with Integrated Sensing and Communications capabilities.
- Implementing **AI-driven security measures** that can help the terminal to adapt to evolving threats in real-time.
- **Standardising security protocols** across different types of SATCOM terminals which can ensure interoperability without compromising security.

Fixed and backhauling terminals user technology type: overview

Fixed and backhauling user technology type eliminates the mobility constraints on OTM/OTP and deployable user terminals. As such, the user installs the terminal in a stable place, where the secure SATCOM service will be needed for long periods of time or permanently.

Fixed terminals

Fixed terminals are traditionally designed to allow for higher throughput than OTM/OTP and deployable terminals. They have a **simplified** architecture since the antenna **does not need a tracking system as it usually does in other cases**. Once the terminal is installed and configured, it rarely needs readjusting or reconfigurations. Traditionally, fixed terminals operate with GEO satellites. **However, the emergence of NGSO constellations is posing challenges** to the handover procedure of the fixed terminal. The multi-orbits, multi-constellations capabilities are real challenges that affect modems and antennas, among others. In this aspect, ESA and flat-panel antennas are demonstrating their capacity to solve these challenges and work with NGSO constellations.

An example of SATCOM fixed antennas installed on a house roof

Backhauling terminals

In this case, the fixed terminal **creates networks that are used to provide backhaul** to cellular base stations. Backhauling terminals allow for the communication between the core network, for instance cellular base stations, and local terrestrial networks usually located in remote locations and/or unavailable via terrestrial links, by aggregating and backhauling via satellite all the data required. Current solutions are based on DVB-S2X implementations. As mentioned on the NTN networks page, backhauling uses the secure SATCOM system to extend terrestrial coverage or as a backup network in case of failure of terrestrial networks. **Traffic routing and channelling, in addition to scalability capacities**, are the main parameters for backhauling operations. Integration of the terminal with the terrestrial network remains also one of the main challenges for backhauling users.

In addition to extending the coverage of terrestrial networks, secure SATCOM backhauling can also be used as a primary or contingency strategy for connectivity routing and associated communication plans.

SATCOM backhauling supporting a terrestrial network cell antenna

Main characteristics of fixed and backhauling terminals

	Fixed	Backhauling
Main capabilities	• **Use of directional antennas (including ESA).** • Throughputs of ~5 Mbps to even more than 100 Mbps, for voice, data, images, and video. • Terminals usually operate in one band. Including L, X, Ku, Ka-band.	• **Use of directional antennas (large aperture, VSATs or ESA).** • Throughputs of 5G backhauling can reach approximately 1800 Mbps for voice, data, images, and video. • Terminals usually operate in one band. Including Ku, Ka-band.
Deployment/installation of the terminal in the field	• **Terminal deployment and set up is performed only once.** • Pointing and non-blocking lines of sight are the main challenges when deploying the antenna. • Set up of power source and connections with the local network tend to be simplified aspects.	• Installation must be planned and designed to be integrated with the terrestrial network. • **Installation is usually complicated since it is usually in remote areas with difficult access.** • **Installation must take care of the interface with the terrestrial network and additional equipment is needed to ensure this function.**
General experience to operate the terminal	• **Some level of training is needed to install and connect the terminal the first time.** • Operation with the terminal remains simple and even personnel without training can operate the terminal. • Self-pointing and self-installing fixed terminals exist and do not require any user intervention.	• Training and formation on installation, configuration, and integration with **the terrestrial network is needed.** • **Knowledge of terrestrial networks might be needed.**
Time to deploy and set up connectivity	• Installation might take from 10 to 40 minutes. • Initial configuration and signal acquisition from 5 to 15 minutes. • Connectivity once the terminal is configured and working should remain stable with instant access to the service through all the life of the terminal.	• Deployment and set-up of the terminal are variable. They might take from minutes, if the terrestrial infrastructure already exists and integration is easy, to hours and days if the terrestrial infrastructure has also to be installed and/or the integration is complex.
Considerations about operational environment	• Terrain might be as flat as possible to facilitate a consistent reference for terminal pointing and acquisition operations. • Terrain must have a clear line of sight and be free of obscuring elements. • Antenna can also be directly installed on a mast. • Weather and wind might be considered depending on the size of the antenna and the structure in which the antenna is fixed (possible use of radome).	• Terrain must have a clear line of sight and be free of obscuring elements. • Terrestrial network integration with the terminal must be always considered and evaluated. • Antenna can also directly be installed on a mast.
Future trends	• Multi-orbits, multi-constellations. • Multi-frequencies. • Virtualisation of the integration with local network.	• Non-terrestrial network integration, 5G. • 6G and full integration of SATCOM networks and terrestrial networks.

Typical use cases

Fixed secure SATCOM solutions have a role in ensuring connectivity for EU critical infrastructures, such as space, financial, industrial, and energy infrastructure or data centres. They also provide connectivity for institutional (EU or member states) use cases. Among the most relevant use cases are communications with embassies or consulates around the world, allowing EU member states to have an independent, secure, reliable, and available communication channel with these assets. In fixed secure SATCOM use cases, fixed secure IoT can also be considered. As explained in the deployable, handheld and secure IoT section, fixed secure IoT has a role to play in supporting connectivity needs, especially with limited data rates. For the rest of the traffic, fixed secure SATCOM ensures the exchange of higher throughput traffic that usually encompasses data, voice, and video.

EU critical infrastructure

Ground segments of space systems that are not SATCOM can be connected with each other by exploiting secure SATCOM fixed connectivity terminals. For instance, already today **Copernicus data are channelled down to SATCOM fixed terminals via the European Data Relay System (EDRS)**, thereby ensuring a faster delivery to the user. Similarly, EGNOS and Galileo ground segments already use SATCOM to connect their remote sites and could use secure SATCOM fixed terminals in their upgraded versions.

Space Situational Awareness (SSA) systems rely on a wide range of ground sensors and can also use secure SATCOM fixed terminals to interconnect these sensors. They can also be used to access future space-based SSA sensors and connect them to ground sensors and other SSA infrastructures.

Financial infrastructure requires reliable and secure connectivity. The European Central Bank, EU Member States' national banks, and stock markets can use secure SATCOM fixed terminals to improve their connectivity, data share and exchange, either for critical traffic transmission paths or as backup systems in case of TN failure. This can be also applied to **critical industries, energy, and data centres**. They can use fixed secure SATCOM and secure fixed IoT to also create secure communications networks to exchange critical data or to backup communications systems, in case of failure of the principal communication channel.

EU institutional communications

The **diplomatic activities of the EU and EU Member States** need secure SATCOM to coordinate, exchange, and implement suitable foreign policy. Diplomatic communications are also the **first channel to prevent, alert, or coordinate international crises, crisis management implementation, and EU foreign policy**. Thus, fixed secure SATCOM allows for independent, reliable, and available diplomatic communications all around the world, enabling the EU and Member States' foreign policy and foreign actions.

EU institutions and agencies (e.g. the European Commission, the European Parliament, the European Council, and European agencies) can also benefit from fixed secure SATCOM services. Such services can be used to communicate with missions, delegations, or deployments of forces of these institutions and agencies worldwide, coordinating their activities and missions. They can also be used **to secure exchange of data and information among them** (regardless of their geographical position). And, of course, similarly to the other use cases, fixed secure SATCOM services can be used to direct critical information traffic or as a backup communication channel.

Fixed secure SATCOM services can also be used to provide connectivity to remote areas, where TN is limited. This can be done by either deploying secure SATCOM fixed terminals or by enabling larger areas to have NTN through secure SATCOM backhauling.

Satellite antenna of small observation station

And what about backhauling?

Secure SATCOM **backhauling can benefit remote areas or areas with poor TN connectivity**. For example, the use of NGSO backhauling services in polar regions (i.e. European regions above 60° North) can be easier than TN deployment, enabling European citizens living in these areas not only to access connectivity services, but also to **have access to critical services such as specialised health care through telemedicine**. Secure SATCOM backhauling can be deployed as a backup service to critical TN, taking over the connectivity in case of emergency or when the terrestrial network is down, thus ensuring availability. Backhauling services can also be used **to enlarge the reach of institutional communication networks**, enabling EU institutions to deploy their communication networks in remote areas, improving the institutional reach even in remote or poorly connected areas. Backhauling can also be used for recreational connectivity in remote operational camps.

Terminals' main technology considerations

Fixed terminals were the first to be used extensively in SATCOM. In fact, in the case of a GEO satellite (the first ones used on a large scale for SATCOM systems), the advantage of such terminals is that satellite handover or beam handover will not occur, which implies a much simpler architecture (an antenna tracking system is not needed) while keeping high performances with a directive antenna. It is worth noting that backhauling terminals are a subset of fixed users with a higher SWaP factor, as they are meant to carry more traffic than more conventional small terminals (Very Small Aperture Terminals – VSAT). Their specificities include also the interface with the backhauled network, rather than offer an interface to a WLAN or a LAN. These fixed and backhauling terminals have more relaxed SWaP constraints as compared to the mobile terminals, although they must still comply with the ITU regulations to limit interference to other systems, but also not to saturate the satellite transponder.

Less size and weight constraints

The fixed terminals can go from **VSAT antenna size (0.45 metre to 1.2 metre typically)**, to much larger in the case of **backhauling (up to 3-4 metres antennas)** enabling higher performance and throughput. Increasing the antenna diameter at higher frequencies will increase the achievable throughput performance, but it will reduce the antenna beamwidth and possibly result in the need for a tracking system, even for GEO satellites that are never perfectly still in the sky.

Since the terminal does not need to be transportable, it means that the terminal equipment is not required to have an advanced level of integration. It can be bulkier, heavier, stored in shelters or use racks in a dedicated server room, for instance. It eases the **RF Front-End and Base-Band equipment integration**. This absence of integration needs often leads to them being separated as **Outdoors Units (ODU) and Indoors Units (IDU)**. **At RF level**, the use of bigger equipment can drastically enhance the performance in signal transmission and reception.

Less power constraints

The fixed/backhauling users are generally directly connected to a land power grid, which means that the amount of electrical power consumption is not a strong constraint as compared with mobile units; this allows for more powerful and less energy-efficient equipment to maximise the link performance. The thermal control of such devices is not as critical, as the integration level is lower.

Satellite handover/beam handover

However, with the expansion of the SATCOM NGSO constellations, the **need for a satellite/beam handover is still present**, even for fixed terminals, as spacecrafts are moving in and out of the visible field of the user location. This may imply (in the case of the 'make-before-break' strategy) the **use of two parabolic antennas to maintain seamless communication**. Electronically Steerable Antennas provide a solution to this as they can directly form two distinct beams whereas mechanically steered antennas only have a single main beam. The terminal requires the use of two data carriers (two in transmission and two in reception) at the same time to ensure seamless communication. This is managed at the modem level. Both handover types also need to be managed at the network level to define the data routes. On the other side, the terminal shall also manage these handovers (traffic plan can be received through the satellite link). **The terminal will also need to have feeds that allow both polarisations to be received to enable the handover between beams of different polarisations**. For fixed and backhauling, the number of different sensors used by the Antenna Control Unit (e.g. with respect to OTM/OTP or deployable user terminals) may be reduced, as:

- The terminal geolocation is fixed and thus GNSS subsystem can be discarded. However, it can be kept to provide time/frequency reference to the equipment (frequency converters, models, Network Time Protocol servers, etc.);
- No more terminal "attitude" (Roll, Pitch, Yaw) to consider since the antenna is generally built on a roof or a pedestal that is supposed to be horizontal and stable. Gyroscopes, compass or accelerometers are useless, with only pointing calibration during installation stage.

Backhauling network connectivity

One of the specific challenges of a backhauling terminal is the connectivity it must provide to the backhauled network. In a SATCOM backhauling scheme, the system needs to implement the satellite interface (e.g. using standards like DVB-S2X and DVB-RCS2, similarly to a classical SATCOM terminal), but in case of backhauling of a cellular 5G network it also needs to implement the "conversion" from/to the 5G ecosystem to address the cellular traffic, implementing the protocols, the 5G NR modems and the specifics of antennas used in 5G networks, such as MU-MIMO technologies (Multiple Users - Multiple antennas Input, Multiple antennas Output). The N3IWF is defined and standardised by 3GPP exactly for this purpose. This is the module that ensures the interfacing between a non-3GPP air interface with the 5G core. However, the integration of a backhauling user terminal to the backhauling network is straightforward, without the requirement for adaptors, in case the satellite air interface is already 5G NR.

Architecture of fixed and backhauling terminals

The **fixed terminals** show the classical transmission/reception architecture that was described in the previous sections for the OTM/OTP, deployable or handheld terminals. **The main differences are generally a simpler and less integrated architecture** (for example the antenna pointing units are not required for GEO terminals), **a much higher SWaP factor** that is reached by the increase of the antenna size (parabolic or electronically steerable), **bigger and more powerful RF amplifiers**, and base band equipment.

For **bigger fixed backhauling units**, some items of equipment that are traditionally integrated at the terminal level can be separated to increase the performance, including:

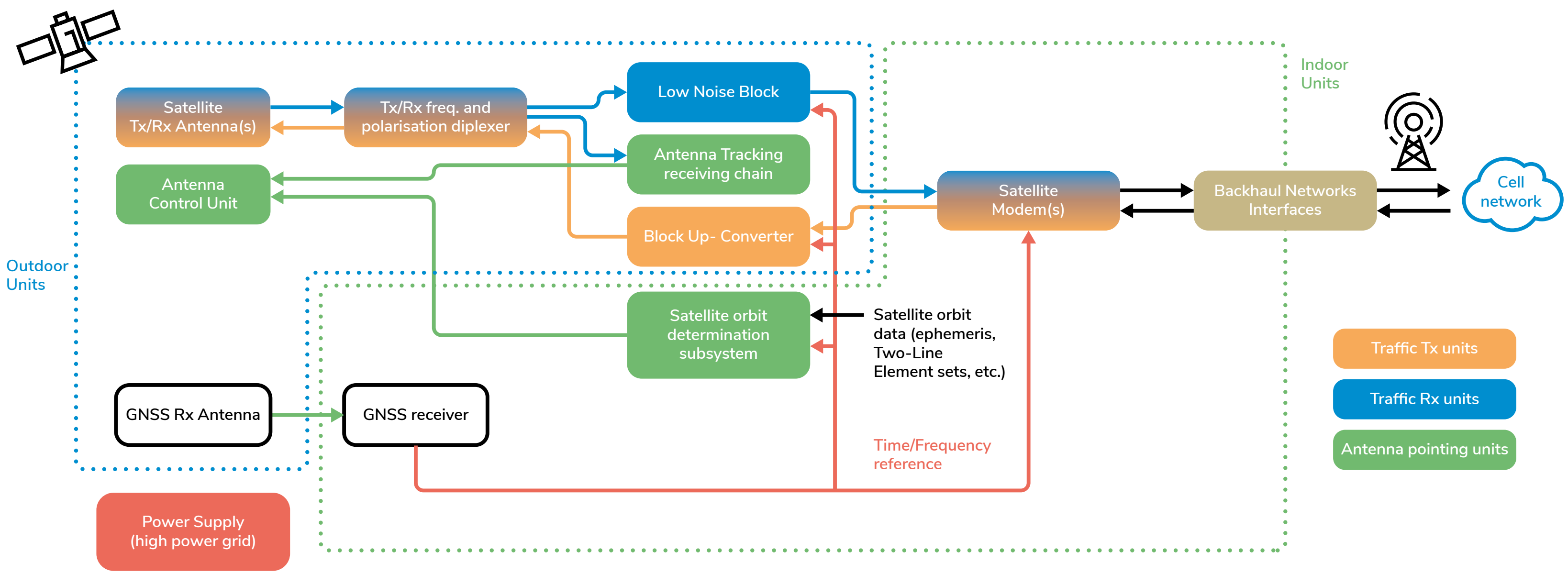
- The low noise block downconverter can be separated into a frequency down converter (DOCON) and a low noise amplifier.
- The BUC can be separated into a frequency upconverter (UPCON) and a high-power RF amplification stage (SSPA or TWTA typically).

As previously stated, depending on **the type of satellite** followed, the **antenna subsystem** will either be single fixed parabolic (GEO only), single parabolic dish tracking (GEO only in the case of large diameter at high frequency), dual-parabolic tracking (NGSO constellation with a 'make-before-break' strategy), or single ESA (recommended for NGSO only, as performance with GEO might be insufficient). In the case of tracking antennas, an antenna control unit is still needed, but with only two main inputs: the satellite orbit determination unit (with an orbit propagation algorithm fed by external orbital data such as two-line element sets or constellation ephemeris) and a possible (but optional) feedback loop from an antenna tracking receiving chain (step-track or mono-pulse techniques).

Depending on the satellite system, the backhauling equipment at the terminal level will have different functions:

- If the satellite system and the backhauled network are sharing the same protocols at lower levels of the protocol stack (i.e. down to the physical layer), then the need of data/packet processing at the interface is minimal.
- If the satellite system and the backhauled network use different set of protocols, then complex packet processing and air interface adaptors will be needed, at different levels of the protocols stack.

GENERIC ARCHITECTURE OF A BACKHAULING TERMINAL (WITH OPTIONAL ANTENNA TRACKING FUNCTIONALITY)



Characteristics of signals used

In the context of secure SATCOM, fixed and backhauling user technology type utilises specific signal characteristics to ensure reliable and secure communications. This section discusses the key characteristics of these signals.

Frequency bands of fixed and backhauling user technology type

Fixed terminals (and by extension, backhauling terminals) may be used in any frequency bands where FSS or BSS SATCOM services are allowed by the regulations. In detail, the exploitable bands are:

- **In sub-bands of C-band** (4-8 GHz): Historically used for BSS (direct-to-home satellite communications) and FSS services. It has been favoured in very rainy areas due to limited propagation losses (rain fade). However, it requires a larger antenna diameter for the user terminal, making the implementation of an electronically steerable antenna unfeasible. Spectrum availability (and consequently, total achievable throughput) has recently decreased, as some C-band spectrum has been reallocated to terrestrial 5G systems. The number of achievable spot beams by a C-band satellite is limited, preventing modern HTS (high throughput satellite) systems from using it; instead, they prefer Ku and Ka-band. Current and upcoming NGSO constellations do not implement C-band at all. While C-band remains useful for its propagation advantages, its future use in satellite systems appears to be more limited.

- **In sub-bands of X-band** (8-12 GHz): ThiS-band shares similar characteristics with C-band, particularly regarding the propagation of electromagnetic waves. However, X-band has been largely reserved for military and governmental use, significantly reducing the risk of interference. Additionally, thiS-band has enabled for the development of more anti-jamming units and equipment.

- **In sub-bands of Ku-band** (12-18 GHz): Widely used for FSS and BSS for decades, Ku-band offers a good compromise between available spectrum and propagation impairments. User terminal antennas can be reduced to VSAT size (0.45 metre), and the implementation of ESA is possible. NGSO constellations like Starlink and OneWeb use Ku-band for their user links. However, the extensive use of thiS-band in both GEO and NGSO orbits is making the spectrum resource-scarce, creating an increasingly challenging RF interference environment.

- **In sub-bands of Ka-band** (17-40 GHz): Developed since the mid-2000s, Ka-band is now the preferred frequency band for modern HTS systems, including NGSO constellations. Although it is vulnerable to rain fade, the narrow beamwidth with reasonably-sised antennas (parabolic dishes or ESA) makes it appealing for secure SATCOM with frequency reuse schemes and high throughput. However, increased use of thiS-band demands constant coordination and regulatory efforts to avoid severe interference. The use of military Ka-band, more protected for military and government use, helps mitigating this issue.

- **In sub-bands of higher frequency bands**: The trend in SATCOM is moving towards higher frequency bands (e.g., Q, V, W, E-bands, and optical near-infrared), though their use has been limited so far. These bands offer large spectrum resources with low interference, but they are extremely vulnerable to rain fade (a single cloud can disrupt an optical signal), necessitating, for example, the set-up of backup stations under different locations. For these reasons, these bands are generally unsuitable for user links in secure SATCOM, although some implementations exist for backhauling applications. Quantum Key Distribution, a now emerging technology, is implemented using infrared lasers.

Particularly for Europe, details of all sub-bands allocated to satellite services are available in the European Table of Frequency Allocations and Applications for the frequency range 8.3 kHz to 3000 GHz (ECA Table) which is frequently updated to reflect frequency allocation modifications. For some European countries national regulations and limitations also apply on top of the ECA Table.

DVB and its derivates heavily used today

Terminal falling under the fixed and backhauling user technology type typically use classical protocols designed for direct line of sight communication with a satellite and a non-mobile user terminal. Modulation and coding standards such as DVB-S2X in the forward link and DVB-RCS2 (or more often proprietary waveforms using multi-frequency time division multiple access MF-TDMA techniques) in the return link are widely used. Most communication satellite payloads are engineered to handle these types of waveforms optimally. Additionally, DVB-S2X implements adaptive coding and modulation (ACM), which adapts the throughput for each individual user to fit propagation conditions, improving link reliability. However, backhauling use cases may require the satellite system to adopt other waveforms, such as 5G NR. In secure SATCOM, the use of more robust waveforms (TRANSEC) might also be necessary.

COMSEC and TRANSEC to protect the data transmissions

SATCOM transmissions can be intercepted by any user directing their user terminal toward a space asset, provided the user terminal is within the same ground coverage area. Similarly, uplink communications may be intercepted by monitoring the electromagnetic environment near a ground station or through high-altitude assets (aircraft or platforms over operational theatres). Similar to other secure SATCOM user technology types, fixed and backhaul user terminals must be robust against threats such as eavesdropping, RF jamming, or spoofing. These threats can be mitigated using COMSEC and TRANSEC techniques, such as advanced encryption key distribution, direct sequence spread spectrum, or frequency hopping techniques, as discussed in the OTM/OTP section.

Fixed user technology type can employ various antenna diameters. The larger the diameter (e.g. for backhauling user terminals), the smaller the antenna beamwidth, reducing the risk of uplink eavesdropping. Additionally, since the fixed terminal location is constant, it increases the possibility of an attacker eavesdropping on downlink signals from the satellite or RF jamming the satellite.

Technological factors and trends

Characteristics and state of the art

The fixed and backhauling user technology type offers a relatively straightforward architecture that delivers efficient performance. When used with GEO satellites, the simple design of this user technology type only requires initial configuration, such as antenna pointing and SATCOM system log-on (including line-up with the satellite operator), during installation. Without the need for complex pointing mechanisms, this user technology type is cost effective and has **minimal maintenance requirements**.

This user technology type is particularly well-suited to **HTS systems**, which are designed to handle **growing traffic demands** over satellites. They benefit from a well-established history of use, fine-tuning, and feedback over decades, which has contributed to their maturity in both hardware and protocols.

With the advent of SATCOM **LEO and MEO constellations, satellite and beam handovers** have become necessary. To ensure seamless connectivity during such events, dual mechanically steerable parabolic dishes can be an effective but costly solution, due to the doubling of RF equipment.

In the context of current and upcoming **NGSO constellations**, the **electronically steerable antennas**, now maturing in commonly used FSS frequency bands (Ku and Ka-bands), provide a solution, as they can directly form more than one distinct beam, contrary to the mechanically steered antennas which have only a single main beam. They also offer **increased flexibility** and **easier maintenance** due to fewer mechanical components.

The need for satellite and beam handovers presents challenges from a network perspective, including **adaptive real-time dynamic data routing** to address traffic congestion and atmospheric propagation considerations. The DVB-S2X standard includes mechanisms to handle these issues effectively. The fixed position of these terminals simplifies network management system (NMS) tasks as compared to OTP or OTM terminals. Through signalling messages exchanged among the NMS, communication hubs (at the anchor station), and the terminal via the satellite link, the system prepares for upcoming handovers. This enables the terminal to anticipate the next satellite, frequency, or polarisation for establishing the link. As SATCOM systems become more complex with increased spacecraft and intersatellite links acting as space data routers, managing traffic even for fixed terminals becomes increasingly challenging.

The current state of the art for the fixed and backhauling user technology type involves the **integration of multi-orbit systems** that combine different constellations at various altitudes. This approach enhances **redundancy, security, capacity, and flexibility**. Previously, integrating these systems was a technical challenge due to differing frequencies, waveforms, and equipment requirements. However, **Software-Defined Radios (SDRs)** now allow terminals to adapt to various constellation signal characteristics more seamlessly.

The dedicated satellite relay station in Aflenz (Austrian Alps)

Future trends

These are the main evolution trends of the fixed and backhauling user technology type:

- **Adaptation to upcoming VHTS (very high throughput satellite) systems** is key since the associated development in GEO and NGSO orbits significantly increases the capacity available for the fixed and backhauling user technology type, meeting the growing demand for secure, high-bandwidth communication.
- **Software-Defined Radios** is an upcoming trend for signal processing functions. This will enable more flexibility and adaptability to future signal characteristics, and it will improve compatibilities to multiple satellite systems in the multi-orbit environment the secure SATCOM is aiming towards.
- **Integration within the 5G ecosystem** is one trend of the cellular backhauling towards the ‘direct-to device’ capability. It goes through the integration of satellite communications to 5G ecosystem through the 5G NTN advances, since the 3GPP’s Release 17 (reinforced after Releases 18 & 19). On this path, more and more of the responsibility for 5G network processing is placed on the satellite system, first by the anchor station, then by the spacecraft itself. Therefore, it reduces the processing task of the backhauling terminal and shrinks the vulnerable surface of attack (up to the extreme where the satellite becomes a 5G radio tower).
- **Advanced cyberthreats countermeasures** are linked to the increase of threats, and fixed and backhauling user technology type will therefore increasingly incorporate sophisticated cybersecurity mechanisms. Among these are advanced encryption (new COMSEC algorithms which will be robust to quantum computers, implementation of QKD), intrusion detection systems, and real-time threat monitoring capabilities. AI and ML technologies are also expected to play a growing role, enhancing threat detection, network optimisation, and adaptive resource allocation.
- Even though they are very sensitive to atmospheric conditions, the rise of **optical communication** technologies (also supported by the QKD raise) is expected to enhance the security and capacity of satellite links for fixed terminals. This technology offers the potential for significantly higher data rates (dozens of Gbps) and improved resistance to eavesdropping (narrow ‘pencil’ beams difficult to intercept) and jamming.

Focus on security and standardisation efforts

Resilience and vulnerabilities of fixed and backhauling secure SATCOM user technology type

The **fixed** secure SATCOM user technology type provides stable, high-efficiency and high-throughput performance capabilities to the network. Properly positioned and within good protection, it will offer a high level of reliability and availability for satellite communication, even though it is not suitable for rapid deployment scenarios. Satellite **backhauling** terminals, per nature, provide a backup solution to a terrestrial communication network if it is compromised or set in a failure mode. As modern fixed secure SATCOM user technology type now aims to offer multi-systems/multi-orbit capabilities, the SATCOM link's resilience towards disasters or threats is even higher.

The fixed nature of these terminals needs to be considered: an attacker, once having the knowledge of the terminal's location, will be able to target it, either with RF (jamming, spoofing, eavesdropping), cyber threat or by physical access to the equipment itself (e.g. physical damage to the equipment, access to data storage). This can even be increased by the low level of integration of the equipment, the human operator often being remotely located from the terminal itself. This should be mitigated through proper physical security measures, for instance through sealed restricted areas. The backhauling terminals also represent a particular risk. Indeed, acting as 'gateways' between a satellite network and a terrestrial one, they may represent a single point of failure, making them preliminary targets in cases where the primary terrestrial network is also down. Additionally, similar to all secure SATCOM user technology types, ensuring the terminal's equipment supply chain security is a challenge, as compromised hardware could introduce backdoors.

In addition, the 'conversion' functions of a backhauling terminal should also be addressed. Indeed, to ensure the connectivity between the satellite network and the backhauled one, some data should be processed in the protocols stack. First, some demodulation must be performed, as well as de-encapsulation of some data packets (may be up to IP layer), which may compromise the cybersecurity. For that reason, it is important for the system designers to define the level of the network protocol stack to which the security is ensured, and which is the domain of confidence in the system.

Standardisation efforts

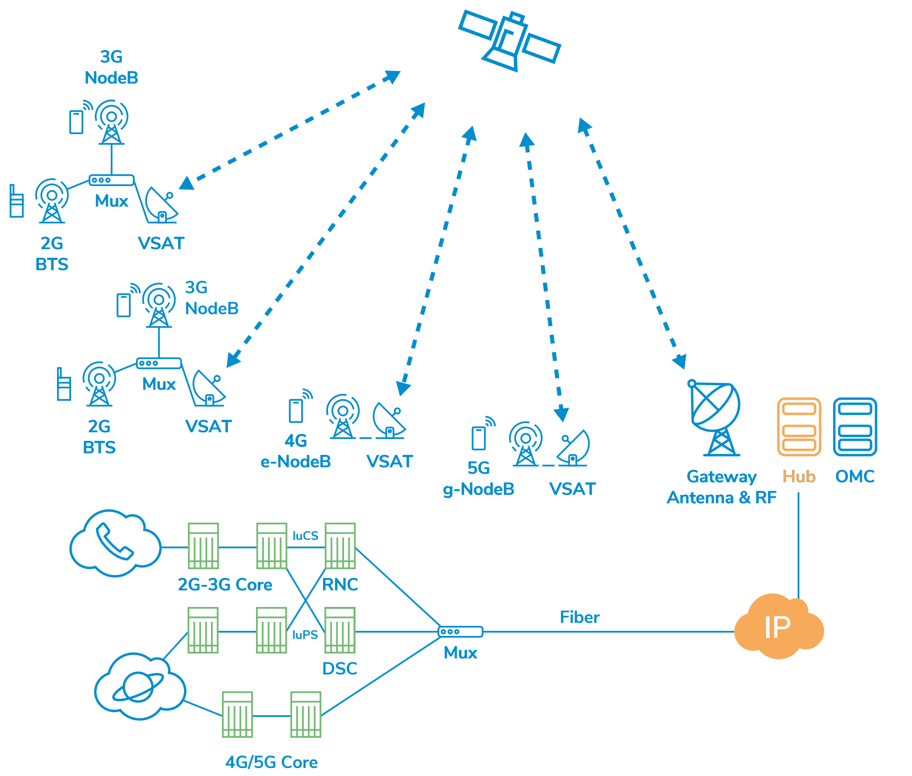
The main standardisation effort at the telecommunication level concerns the physical layer and on the RF (frequencies, MODCOD(s), waveforms, antenna techniques, multiple access schemes), lower layers of network protocols, and cybersecurity protocols.

One of the main efforts has been the standardisation and integration of the 5G Non-Terrestrial Networks (NTN), led by the 3GPP. Since Release 17, the focus has been on the integration of SATCOMs within the terrestrial 5G ecosystem. This integration aims to enhance global connectivity by enabling interconnectivity among systems, with terrestrial, spaceborne and airborne platforms, particularly for secure SATCOMs, increasing reliability and resilience by providing backup solutions in case of failures, crises, threats, or disasters.

In addition, DVB and ETSI standardisations, particularly on DVB-S2x, keep evolving with new annexes. For instance, one of the latest additions includes the enhancements of DVB-S2x and RCS2 to support NGSOs.

Specifically designed for MILSATCOM applications, several secure waveforms and protocols have been implemented or are currently under development. These implement state-of-the-art COMSEC techniques to ensure the authenticity, integrity and confidentiality of the data (in particular, standards will have to agree on the post-quantum algorithms to be implemented by the actors, as well as standard protocol for key distribution). On the other hand, TRANSEC techniques can make the signals more robust to propagation impairments (link availability) and to threats such as jamming, eavesdropping, and emitter spoofing. Ensuring standardisation of these protocols and techniques will enable interoperability between equipment from different manufacturers, and some military standards, such as STANAG (Standard NATO Agreement) 4622, are based on the widely spread DVB-S2X and DVB-RCS standard. Another SATCOM standard that is military-oriented is the MIL-STD-188 set of requirements.

SECURE SATCOM BACKHAULING TYPICAL TOPOLOGY



EDITOR’S SPECIAL: SYNERGIES FROM SPACE

©EC

This Editor’s special is addressing **revolutionary, forthcoming and existing synergies** among the GNSS and secure SATCOM (or more broadly SATCOM) space domains, casting a glance over Earth Observation (EO) or EU space programme components (such as Galileo or Copernicus) where relevant.

The evolution of GNSS, SATCOM and EO systems is becoming increasingly intertwined, with users' requirements further driving equipment manufactures towards a more synergetic use of the space assets. If simplified, synergies can be observed or will be potentially seen at two levels - infrastructure level and user level.

At infrastructure level, a forward-thinking “multi-mission” approach that transcends the silos of traditional space system design, development and deployment is presented. In this vision, connectivity serves as the linchpin for achieving futuristic multi-mission objectives, overcoming isolated solutions. Furthermore, existing and potential SATCOM and GNSS infrastructures` synergies are highlighted as well.

Additionally, the recent surge in space launches, which is leading to congestion in available orbits, has raised major concerns about collision avoidance and space traffic management. Effective coordination can only be achieved through exploiting presented synergies.

Moving on to the **users’ perspective**, even more potential synergies become apparent. The increased availability of space data and services, coupled with the rapid evolution of terminals and receivers designed to keep pace with the deployment of constellations, creates further opportunities for synergies.

Synergies among (secure) SATCOM, EO and GNSS domains are already a reality in the downstream sector. Indeed, this Editor’s special, among other topics, explores the most illustrative examples at the application level in transport and emergency management, or the roles GNSS and SATCOM play in Copernicus.

Moving from space mission silos to a converged data management infrastructure

Current space infrastructure, associated programmes, systems, and sub-systems are typically designed, developed and deployed in silos with very few interactions between them. Institutional bodies, whether international or national, and even space manufacturing organisations themselves, reflect these silos. Navigation, telecommunications, Earth observation, and exploration space activities are divided at the highest levels of these organisations, resulting in very limited interactions and, consequently, few synergies.

Secure SATCOM infrastructure as a space core network for all missions

A new paradigm in conceptual thinking is to view space as an additional, complementary layer of terrestrial connectivity. Fibre optics and wireless connectivity are means of transferring data, whether this data is for sensors (e.g. IoT), calls, or video streaming. Space connectivity is not an end in itself; it is a means to interconnect data producers and data users.

Secure SATCOM is expected to be seen as an additional means of transferring data. Such a shift in conceptual approach may alter the way systems are designed. Instead of managing connectivity, positioning, or sensing activities, space systems can be viewed as tools for data transfer between two points, regardless of whether these points are in space, on the ground, in the air, or over the sea.

In this "multi-mission" concept, any LEO, MEO, or GEO space object (or infrastructure) could become a network node. Secure SATCOM space systems may thus be a key component of a vast network that helps interconnect data producers and users. This multi-mission space infrastructure can also be leveraged to support future initiatives proposed by the EU, such as the **Earth Observation Governmental Service** in which EUSPA is foreseen to play a key role, as mentioned in the European Union Space Strategy for Security and Defence (see JOIN(2012)9).

An EU secure SATCOM system can also reinforce the mission of existing components.

There is no need for every single data producer (and its associated system) to manage end-to-end connectivity to reach every possible end user. The secure SATCOM infrastructure will decrease the overall costs of such programmes.

Secure SATCOM infrastructure hosting edge computing capabilities

Thinking beyond silos with a complete and converged space infrastructure opens up numerous possibilities and new design capabilities.

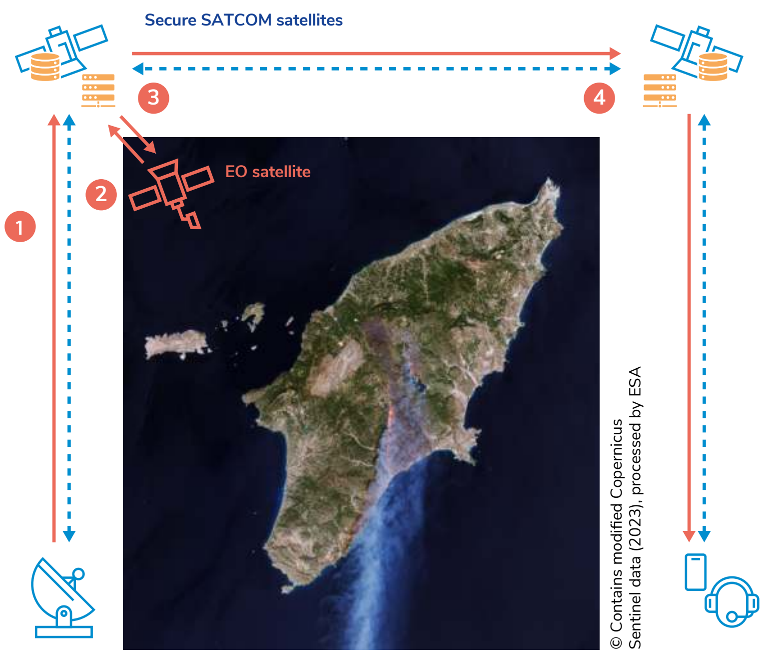
Clear interaction between space systems with standardised capabilities (either RF or optical) is essential. Every space object should be part of the overall system. Connectivity between these components is fundamental to ensure that any infrastructure can be supported by the others.

Next-generation secure SATCOM infrastructure should not be limited to ground-based capabilities. It should incorporate features that mirror those of terrestrial networks. **Core elements in a space-based secure SATCOM network should enable data processing, routing, and potentially storage**. This implies that space infrastructure will need to move towards virtualisation and cloud computing.

If any space object can connect to such a core network supporting connectivity, processing, and storage functions, its associated end-to-end system does not need to include these capabilities or its own dedicated ground segment and network.

With this concept, we may move beyond the current hosted payload model, which requires finding a suitable host with available mass, space, and compatibility with the payload schedule. A space system with minimal connectivity capability (to connect to the core secure SATCOM network in space) may be simpler to launch and may not require a dedicated ground system. Consequently, this approach could be a faster and more cost-effective solution.

EXAMPLE OF SECURE SATCOM FOR ROBUST SPACE-DATA DISSEMINATION



The core secure SATCOM infrastructure could be at the heart of the 4 steps for a user to receive a processed image in the shortest time:

1. An order is issued from the secure SATCOM ground to collect processed images for one end user.
2. Order is transmitted to the payload carrying the sensor via the core secure SATCOM infrastructure.
3. The core secure SATCOM infrastructure collects the raw images and can process them.
4. The core secure SATCOM infrastructure routes the information to the end user that receives only the data associated to his/her need.

SATCOM and GNSS infrastructures' synergies

The LEO PNT approach

The demonstrated feasibility of launching and deploying mega-constellations in Low Earth Orbit (LEO) could significantly influence the future development of GNSS. Commercial services such as Iridium's Satellite Time and Location® (STL), provide LEO-based PNT services that enhance the resilience and survivability of critical infrastructure when GNSS signals are unavailable or disrupted. Additionally, researchers have shown that even if not specifically designed for PNT purposes, telecommunication signals transmitted from the recent LEO mega-constellations could be used as a complementary technology to calculate a positioning solution, leveraging LEO SATCOM transmissions as signals of opportunity[1].

Research into complementary or alternative solutions to GNSS is ongoing, particularly focusing on synergistic solutions that could be seamlessly integrated into future GNSS receivers. Indeed, the solutions under investigation aim to augment existing GNSS constellations with additional navigation signals from LEO, while relying on GNSS for orbit determination and time synchronisation (ODTS). Several projects are currently underway to further explore this approach: Xona (USA); Centispace SATNET (China); Synchrotube (Europe); JAXA LEO PNT (Japan).

LEO PNT pros and cons

The LEO PNT approach could help meet the growing demand for improved performance and enhance GNSS resilience against interference, jamming, spoofing, availability issues, integrity challenges, and other performance concerns such as multipath effects. Compared to MEO PNT, the LEO PNT approach has both advantages and disadvantages. Its main advantages are:

- Smaller, low-cost satellites and multiple launch scenario with 30-60 satellites per rocket (lower launch costs), resulting in shorter innovation cycles of five years design live.
- Reduced free-space loss when using the same frequencies. Higher signal power, leading to greater robustness against interference when allocated in different frequency bands.
- Signal shading due to topography and buildings is more frequent but of shorter duration. Additionally, multipath effects are reduced because of higher Doppler effect (whitening by tracking-loop filter).
- Convergence time in precise point positioning (PPP) is significantly shortened.

However, major drawbacks of the LEO PNT approach include:

- Frequency regulations (both international through ITU and bilateral agreements) are required for new and existing frequency bands, including possible restrictions on the transmitted signal power.
- Compatibility and interoperability between different LEO PNT proposals and with GNSS must be ensured.
- Free-space loss, rain attenuation, and foliage attenuation are particularly strong at higher carrier frequencies, leading to availability concerns.
- The development and production of new GNSS user receivers would be necessary, leading to an unsustainable C-SWaP (Cost, Size, Weight and Power) for many current GNSS applications.
- A more complex ground segment would be required, particularly when aiming for full independence (resilience) from MEO-PNT.
- Orbit predictions for LEO satellites are more challenging due to the impact of surface forces in lower orbits.

For a more detailed analysis of the benefits and drawbacks of LEO PNT solutions, please refer to "A Comparative Study of LEO-PNT Systems and Concepts".

1: e.g. LEO-PNT With Starlink: Development of a Burst Detection Algorithm Based on Signal Measurements.

One site for control centres: existing examples

The ground segment of GNSS and SATCOM must be deployed globally and with a high geographical diversity to keep a continuous connection with the space segment and to monitor the performances at global level. These common needs pave the way for a potential synergy of their ground infrastructures.

Site sharing for different space missions is already occurring in sites such as Fucino, Azores or Oberpfaffenhofen, increasing the cost efficiency of the overall site management.

For example, the Fucino space centre in Italy hosts multiple missions and services:

- Earth Observation: control centre of the dual-use EO mission Cosmo SkyMed.
- Navigation: backup of the Galileo control centre and the Galileo Data Dissemination Network (GDDN) management.
- Space traffic management: provide the LEOP services (Launch and Early Orbit Phase), which runs from the time the satellite separates from the rocket until it reaches its final orbital position.
- SATCOM: at the Fucino space Centre, Telespazio provides connectivity services for the major satellite communications operators. Also, dedicated communication network for major governmental users in the transport, space and energy sectors are managed.

Further efficiency in GNSS and secure SATCOM can potentially be achieved through shared telemetry, tracking and command stations, ground networks, spectrum monitoring and security management.

©ESA

Main antenna site of the Fucino space centre in the Appennines (Italy)

Space traffic management (and collision avoidance) needs precise orbitography

Around 46,300 space objects, of which 10,300 had active payloads, were orbiting the Earth on 28 August, 2024, according to Space-track.org. The higher the number of object the greater the risk of them colliding, and it is thus important to anticipate such collisions.

Secure SATCOM constellations operations imply precise management of collision avoidance

Satellite operations (and Space Traffic Management, STM) are facing growing challenges, especially when managing secure SATCOM LEO constellations: collision avoidance (CA), management overload, straining ground assets, limited coordination tools, limited choice of SSA providers, rules between satellites with autonomous CA and hectic traffic coordination.

To ease, or at least decrease, the complexity of space traffic management the space community requires three fundamental elements:

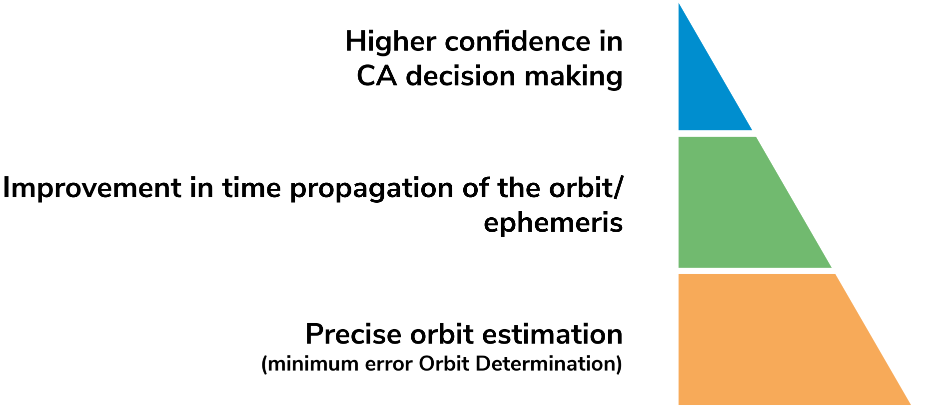
- Manoeuvre planning strategies to mitigate risk;
- Sophisticated algorithm to calculate collision risk and conjunction assessment methodology; and
- Reliability of the uncertainty range of the object's state at Time of Closest Approach (TCA).

As highlighted in the right-hand side pyramid, Precise Orbit Estimation (which is the minimum error of the Orbit Determination) is the foundation to achieve a higher confidence in CA decision making. **Error in orbit modelling has a cascading effect on the main factors influencing the orbit determination processing and manoeuvring (linked to CA strategy)**, which includes:

- Impact of high-quality satellite ephemeris – The Precise Orbit Estimation (minimum error Orbit Determination) is the entry point to determine the propagation of the orbit/ephemeris of a space object and therefore the probability of a collision with another space object (from your own fleet or from a third party).
- Well-calibrated thruster performance and precision manoeuvre planning – Knowing with more confidence where the space object will move gives more confidence on the thrust (power and direction) that must be planned.
- Fuel efficiency – Accurate positioning facilitates performing only essential manoeuvres, leading to reduced fuel consumption.
- Expand satellite lifetime – Direct consequences of fuel saving since space object lifetime used to be mostly driven by the fuel tank fill rate.
- Facilitate better (reduce complexity and risk) CA strategies development – With more accurate planned CA manoeuvres, fewer operations and less complex strategies are anticipated (limiting the domino or ripple effects).

1: The STM and associated CA procedures are closely linked with GNSS receiver family #5 (special apps including space) where POD is a significant driving use case.

PRECISE ORBIT ESTIMATION AS THE FOUNDATION OF COLLISION AVOIDANCE DECISION MAKING



GNSS as complement to the positioning of Secure SATCOM

The accuracy of orbit determination required for STM/station keeping is improved with the use of GNSS receivers (compared to orbit determination with just range measurements, when available)[1]. These can also contribute to the spacecraft's attitude determination, which is primarily based on other technologies such as Sun/Earth sensors, star trackers, gyroscopes and accelerometers.

Below are some non-exhaustive examples of in space activities using GNSS in-orbit positioning solutions:

- **Position-velocity-time (PVT) for LEO satellites** – These satellites, as a subset of a large constellation, need to know their orbit position with high accuracy. In addition, the GNSS receiver module delivers accurate and reliable GNSS time. Communications between satellites need accurate time for synchronisation, either for routing or modulation capabilities.
- **In-space infrastructures coordination** – Coordinating the alignment of two in-space infrastructures requires highly accurate orientation and positioning. The associated applications can range from a combination of sensors (or instruments) to In-Orbit Servicing. GNSS receiver or using GNSS-like techniques can provide the expected accuracy. By extension, GNSS can enhance other sensors such as a camera.
- **Earth observation sensor reference** – The close proximity to the Earth enables continuous and permanent Earth observation by LEO satellites. High accuracy positioning is then needed for referencing the collected data or images taken from such distances. The exact orientation of the sensor is also needed for proper image or data processing algorithms application.

For a complete description of the link with SST from GNSS perspective , please see "Report on Space: User Needs and Requirements".

Secure SATCOM terminals and GNSS receivers' complementarity

Accurate GNSS key to SATCOM OTM/OTP set-up and antenna pointing

As presented in the secure SATCOM technological review, more and more electronical flat panel terminals are developed. One of the consequences on the market is the growth of secure SATCOM terminals that are either mobile or transportable (due to their ease of integration). Mobile or transportable terminals need accurate location, or even relative orientation accuracy, to manage their link towards the satellites either for OTP or OTM applications.

The time it takes to power up the terminal and its effective availability for transmission is a key selection criteria for any Secure SATCOM solution. Proper localisation of the user terminal guarantees a rapid registration procedure to access LEO constellations.

In addition to enabling accurate location, GNSS receivers (with two antennas) can be used for antenna pointing (fixed or transportable), while three to four antennas can allow full 3D orientation (On-The-Move). The objective is to achieve ~0.1° precision for the first step of the antenna pointing accuracy.

Some companies have embedded GNSS receivers into secure SATCOM terminals that are used as part of the network registration process, while location data are used for trouble shooting and data analytics, for example.

GNSS can enhance the performance of SATCOM terminals, but the reverse is also true: GNSS receivers, particularly those used by professionals like surveyors, can benefit from space-based communication to achieve the positioning accuracy necessary for their tasks. As mentioned on page 102, SATCOM links are already being exploited to transmit augmentation data, improving the accuracy of remote GNSS receivers. GNSS receivers and secure SATCOM terminals working together is a native objective complementarity.

Synergies in the HW/SW architecture

Secure SATCOM terminals and GNSS receivers may also share some building blocks. Currently, identified technological moves are similar for both GNSS receivers and secure SATCOM terminals, and it would end up with techno sharing or even common design and development approaches. The initial assumption for such a statement is that Software Defined Radio concepts are increasingly present in current receiving systems. Secure SATCOM terminals' and GNSS receivers' suppliers may collaborate on:

- **Shared development strategies** – Secure SATCOM and GNSS are facing the same move from HW-oriented to SW-oriented solutions. Sharing on the tested approach can help select a more industry-fitted development methodology – e.g. Agile, DevOps or Lean.
- **COTS hardware** – The satellite industry move towards SW-oriented solutions favours the use of commercial off-the-shelf (COTS) processing solutions rather than specific ASICS or FPGA. The associated complexity concerns the hardening and the compatibility of this HW with space environment. Having secure SATCOM and GNSS pushing in the same direction toward the processor manufacturers with a similar base of providers would favour more compatible and viable solutions. Moreover, COTS hardware can also consist of chipsets that integrate both SATCOM and GNSS processors, as seen in smartphones used for terrestrial communications, for instance.
- **Software ecosystem** – Relying more on SW implies that some functions, such as reliability or integrity, are not only managed at the HW level meaning that SW must hold part or full responsibility. One consequence is that SW ecosystem, and associated implementations must meet standards that were previously set with HW-oriented concepts. Sharing a similar approach between secure SATCOM and GNSS is essential.
- **Software building blocks implementation** – The ultimate goal of SW synergies is for SW building blocks developed by either GNSS or SATCOM to be easily used or modified and integrated by the other – i.e. an accessible common open library to decrease the overall development costs.

Benefits to have receivers with the two technologies embedded in one single HW

Despite the architectural synergies outlined above, current synergies between GNSS and secure SATCOM still mostly concern the combination of two segregated 'basic' services and technologies. The associated terminals are taken separately, and the integration is performed at the services level.

However, below is a non-exhaustive list of the benefits of favouring terminals embedding both GNSS and secure SATCOM capabilities:

- **Decrease in SWaP** (Size, Weight and Power). A reduced SwaP is always preferred but it becomes of pivotal importance for specific use cases that require an easy handling of the user terminal (e.g. On-The-Move or Deployable terminals; see also the secure SATCOM user technology types in page 71). It may not be seen as a problem for boats or aircraft, but it is, and it will be for drones. The GNSS and secure SATCOM integration in the terminal can virtually reduce the overall cost of the device thus enabling mass market verticals, such as cars, that express a binding constraint on the cost of components.
- **Ease of integration** – It may sound obvious but having one single HW to cover two capabilities definitively eases the overall physical integration. For example, wiring is embedded in the terminal and not managed externally (with associated constraints like isolation, connectors management).
- **Simplifying interfaces** – Having synergies at the end terminal level would imply a greater relationship between GNSS and secure SATCOM actors, easing the interfaces and increasing the synergies.

SATCOM as a broadcast tool for GNSS augmentation services

GNSS systems can be used as SATCOM channels supporting emergency scenarios, as we will see on **page 105****. However, SATCOM links can also augment GNSS applications requiring a high degree of positioning accuracy.**

GNSS augmentation and the augmentation services market

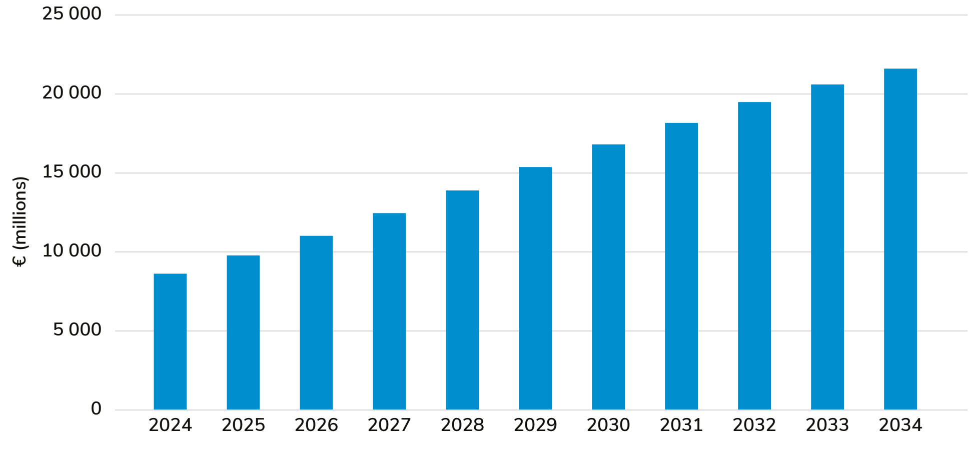
When the basic GNSS performances are not sufficient, SBAS augmentation is the most readily available solution to improve the performance of a GNSS receiver being it **free of charge and compatible** with the vast majority of devices.

Professional applications needing better accuracy, such as surveying, precision agriculture and geodesy, **rely on the sophisticated augmentation of PPP, RTK and PPP-RTK** (see page 15 for the details on these techniques).

The provision of GNSS corrections is an expanding as shown in the graph displayed, reporting the revenue forecast over the next decade. **The agriculture sector is the main contributor in this market with a share above 50%** and it will see a doubling of revenues over the next five years. Augmentation services are still predominantly supplied on a commercial basis, as highlighted by the large number of operators that are listed on the "UseGalileo" website.

© chriswalley07/shutterstock.com

FORECASTED REVENUE OF COMMERCIAL GNSS AUGMENTATION SERVICE MARKET



SATCOM stepping in for synergies

Augmentation services require a communication link to share precious information with the GNSS receiver (e.g. orbit corrections) which are needed to improve the accuracy of the positioning solution. For this purpose, cellular communications are the preferred channel.

However, augmentation services can be disrupted when the positioning solution is required in a remote area with a small probability of a terrestrial link at hand (e.g. in oceans, remote agriculture fields or when surveying in desertic areas for a pipeline construction). In those scenarios, PPP is the most common correction technique applied to cope with the probable absence of a nearby local reference station supporting the faster RTK methods. Both GNSS operators and commercial actors have integrated space-borne capabilities to enable PPP corrections, filling the gap of the terrestrial communications.

While Galileo relies on its data channels to deliver its High Accuracy Service, other providers use private satellite communication operators to distribute corrections to their subscribers.

The Novatel or Trimble ecosystems are apparent commercial cases for the integration of SATCOM for GNSS augmentation purposes. Relying on terrestrial communications, their subscribers can indeed switch to a satellite communications link to access, respectively, the Novatel Terrastar and Trimble CenterPoint RTX augmentation services. Both solutions have selected L-Band channels for the satellite communications thanks to its strong propagation ability, its use of a single antenna in the receiver design and its ease of operation on-the-move.

SATCOM and GNSS enabling remote sensors' reading

Synergies among space segments is essential for accessing remote sensors deployed in isolated areas which are serving a range of purposes including meteorology, ocean physical property characterisation, climate monitoring, and the calibration of space-based sensors.

The Copernicus In Situ data

Copernicus relies on a collection of satellites, most notably the Sentinel series, which are specifically designed to meet the requirements of Copernicus services and their users. Perhaps less known is the In Situ component of the programme. **Copernicus indeed gathers data from diverse networks of sensors located on the ground, in the sea, and in the air**. These sensors enhance the satellite datasets, providing continuous and punctual measurements in a specific location, overcoming the limitations of resolution and revisit times of EO satellites.

At the same time, the In Situ component is pivotal in the final steps of the Copernicus data provision. **The Copernicus Sentinels cannot provide valuable data without appropriate calibration and validation data** from In Situ networks: raw data need to be compared and aligned with ground truth provided by local sensors. As the resolution of satellite observations improves, higher accuracy is also required from the supporting In Situ component.

EXAMPLES OF IN SITU DATA FOR COPERNICUS

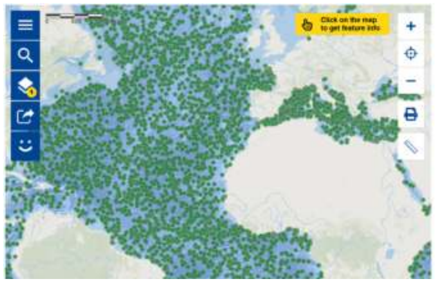
Meteorology	**Real-time and historic data** • **Ground:** Weather station data (temperature, precipitation, relative humidity, wind, solar UV etc.) • **Atmospheric profiles:** temperature, wind, humidity.	Atmospheric composition	• Concentrations of major air pollutants (NOx, PM10, PM2.5, CO, SO2, HCHO, Pb, TSP, C6H6) • Size-resolved chemical composition of aerosol. • Greenhouse gas concentrations.
Oceanography	• **Physical:** Temperature, salinity, ocean currents, sea surface height, sea ice and mixed-layer depth. • Biological: chlorophyll, dissolved oxygen, nutrients.	Terrestrial	River discharge, Water use, Groundwater, Lakes, Snow cover, Glaciers and ice caps, Ice sheets, Permafrost, Albedo, Land cover including vegetation type, Soil carbon, Fire disturbance, Soil moisture.

Networking the remote sensors

Sensor units are easily networked through terrestrial communications when they are within reach. However, when **sensors must be deployed in remote areas, satellite communication is the main solution to collect the measured datasets**. Moreover, when the sensors are roaming and not in a fixed position, the use of GNSS is also crucial. Sensors placed in floats around the world's oceans are a typical example of synergies across the major space-derived services, thereby contributing to the EO services, supported by GNSS for the positioning of free drifting floats and by SATCOM for accessing the sensed data remotely.

The European Marine Observation and Data Network (EMODnet) and the Copernicus Marine Service jointly distribute open access marine data free of charge. Among the multiple sources, Copernicus Marine services and EMODnet collect data from the **ARGO float programme, an international network of 3,800 autonomous profiling floats** that drift freely, measuring temperature, salinity, and various other characteristics of the ocean's upper 2000 metres. Most of the newer floats in the ARGO array now rely on **GNSS to determine their positions and use SATCOM (Iridium) for data transmission**. The use of GNSS and SATCOM enables the floats to minimise the time spent at the surface sending data, thereby reducing the chance of them drifting ashore.

ARGO FLOATS AS TRACKED BY EMODNET

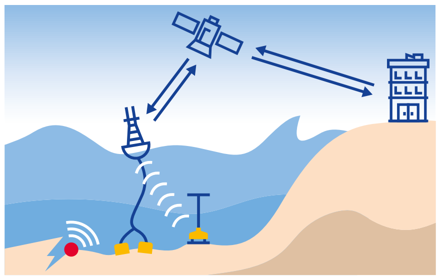


© EMODnet Physics

In the frame of the ARGO initiative, 12 European countries gathered in 2008 within the **Euro-Argo project** with a common aim to provide an optimised and sustained European contribution to Argo by deploying 250 floats per year. The Euro-Argo is now able to take up this challenge by responding also to specific European interests for marginal seas, high latitudes, biogeochemical measurements and depths greater than 2000m.

Meteorologists were the first to utilize remote sensing and played a pioneering role in the space-based data collection from in situ sensors.

THE TSUNAMI WARNING SYSTEM



The first space-borne **Data Collection System (DCS)** was established in 1978 through an agreement between the French Space Agency (CNES), the National Aeronautics and Space Administration (NASA), and the National Oceanic and Atmospheric Administration (NOAA). Today, the DCS remains active, supporting the transmission from **over 5,000 environmental platforms worldwide**. Such platforms based on buoys and ships send oceanographic and meteorological data, while those on land deliver meteorological and hydrological information, and platforms on balloons collect atmospheric data.

DCS payloads are typically hosted on meteorological satellites. For instance, **the Meteosat Third Generation**, a joint mission between ESA and EUMETSAT, includes a DCS payload that serves as a relay for tide-level data transmitted in the UHF band by moored buoys, which are part of tsunami warning networks.

Opening room for synergies in transport and emergency management

Mobility needs GNSS and secure SATCOM complementarity

GNSS and secure SATCOM are of a fundamental combination in the maritime, rail and aviation sectors. Existing global distress and safety systems, such as GMDSS (M for maritime) and GADSS (A for aviation) integrate both technologies. For example, GMDSS combines an Emergency Position Indicating Radio Beacon (EPIRB) for exact localisation and several communication means using specific frequency bands allocated by the ITU. In addition, the rail sector is also in the process of upgrading their communications infrastructure to enhance the European Rail Traffic Management System.

Other available technologies include Automatic Dependent Surveillance – Broadcast (ADS-B) for aviation or for maritime; Automatic Identification System (AIS) combined with VHF Data Exchange System (VDES); and Vessel Monitoring System (VMS) combined potentially with terrestrial connectivity. It should be noted that some satellites/constellations/services can receive messages broadcasted by aircraft and ships (and the data is then sent to ground and potentially sold to customers).

Vehicles are becoming more autonomous, and even unmanned such as drones (terrestrial, maritime or flying), thereby creating more synergies between GNSS and Secure SATCOM. Autonomy is basically a trade-off between reliable secure connectivity and more autonomous on-board sub-systems. GNSS along with secure SATCOM in remote areas where terrestrial networks are out of reach cover two of the main needs for the self-management of connected and automated platform – i.e. where am I? Where do I collect data on my environment (e.g. own sensors or external data)?

The growth of connectivity needs associated to the increase of mobility verticals needs will push the community to use frequency bands outside of the traditional ITU "safety services" to manage the connectivity part. Secure SATCOM will have a key role to play in maintaining the complementarity with GNSS data.

Secure SATCOM making EO data actionable by informing deployed personnel

Personnel deployed in isolated areas (e.g. maintenance operators of remote critical infrastructures) or in an emergency scenario where terrestrial communications are disrupted can benefit from secure SATCOM to access vital information such as real-time maps derived from EO data, position of other teams and assets, keep-out zones.

Also operational centres can inform decisions based on EO data; information and instructions that can be effectively communicated to the deployed personnel, even when other communication means are unavailable. Similarly other data gathering means (as drones or handheld devices) can relay data streams (e.g. live video) to the coordination centres, augmenting the information gathered by satellites.

The weak point of deployed end-users on-the-move is the fragility of their connection, regardless of the handheld or deployable antenna. Nevertheless, this connectivity is required to comply with the real-time and security aspects of their mission. Therefore, the data to be transferred to deployed personnel through a secure SATCOM link, should be adapted to its need, while being effective and, as far as possible, 'light' (in terms of size).

The synergies between Earth Observation and secure SATCOM are opening the door to the next generation space infrastructure that should be multi-mission oriented and designed.

Communication features of GNSS enabling warning and rescue services

Search and Rescue (SAR) services are one of the first satellite communications applications. For more than 30 years, users in distress can issue an SOS request through a dedicated beacon that can reach orbiting satellites. The advent of GNSS constellation has paved the way for a deployment of a wide network of space-based SOS receivers. Also, exploiting the capability of GNSS signals to carry reduced but valuable datasets, a link with the user in distress can be established.

COSPAS-SARSAT Search and Rescue

In the 1980s, France, the United States, Canada, and the Soviet Union collaborated on the creation of COSPAS-SARSAT, a satellite-based system designed to locate individuals in need of rescue. Over the past decade, GNSS systems have become the predominant platform supporting SAR satellite services: the extensive satellite constellations of GNSS deployed in MEO can host SAR payloads (MEOSAR) providing wide coverage areas and sufficient relative motion between the satellites and the transmitting beacon on the ground. This motion enables the use of Doppler measurements to help determine the location of the distress beacon. For an accurate localisation of the beacon, the Doppler measurement is validated and refined by the position computed by the GNSS module included in the beacon terminal and shared in the data fields of the SAR communication channel.

The Galileo constellation hosts more satellites for distress-alert detection and location than any other constellation. Also, the Galileo "Return Link Service" (RLS) that provides users with an acknowledgement of the rescue request, has been endorsed by the COSPAS-SARSAT Council in March 2021 as having achieved the transition to Full Operational Capacity, available globally.

Galileo Search and Rescue evolution

Additional services are currently being implemented within the Galileo programme to better support international search and rescue activities through bidirectional communications.

The SAR/Galileo Two-Way Communications Function represents an enhancement of the Return Link Service, allowing for the exchange of information between Rescue Control Centres and individuals in distress.

The operator of the Rescue Control Centres (authorised users) will have the capability to send questions to the activated beacon to gather information about the ongoing distress situation or to provide instructions to facilitate the rescue process.

The SAR/Galileo Remote Beacon Activation Function is an enrichment of the current Return Link Service allowing on-demand authorised users to send predefined commands to compatible SAR beacons such as "start transmitting".

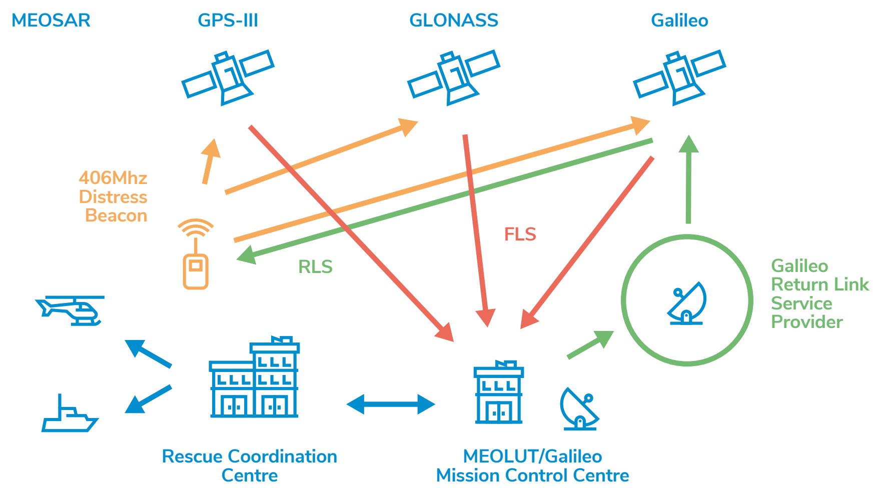
The service will be provided free of charge through the Galileo Open Service (E1). Once activated, the beacon starts transmitting distress alert messages which are detected by Galileo SAR payloads and its estimated position will be provided to the authorised user allowing the tracking of the beacon.

Galileo Emergency Warning Satellite Service (EWS)

GNSS transmissions can play a pivotal role in the broadcasting of alert messages over vast geographical areas: the majority of portable devices are indeed able to decode GNSS signals that are available even in critical scenarios where terrestrial communication lines are disrupted.

In this context, the Galileo EWS will be able to disseminate alert messages directly to the population in areas threatened by natural or manmade disaster. The service will be free of charge and provided in cooperation with Member States National Civil Protection Authorities. It will complement existing warning systems by providing exceptional resilience against major disruption of mobile networks and power lines on the ground.

GALILEO SAR WITHIN MEOSAR



SATCOM emergency SOS from smartphones

The integration of GNSS and COM (SATCOM) chipsets into smartphones opens capabilities such as texting emergency services with no cellular nor Wi-Fi coverage. Localisation is ensured by GNSS chipset and connectivity is using L-band chipset. Apple initiated with iPhone 14 (2022) an emergency SOS function using Globalstar satellite network. In the same year, Huawei launched a first service covering China only, while Google introduced this capability in 2024 in the US only using satellite network of Skylo, an NTN service provider that works with multiple satellite operators. Samsung announced in 2024 that its next generation of top-of-the-line smartphones will integrate this capability with the support of Iridium. By contrast, Starlink is partnering with T-Mobile to offer such services re-using the terrestrial frequency bands in areas where there is no coverage.

Annexes

Annex 1A: Definition of GNSS performance parameters

Key GNSS performance parameters

Accuracy is the difference between true and computed solution (position or time). This is expressed as the value within which a specified proportion – usually 95% – of samples would fall if measured. This report refers to positioning accuracy using the following convention: centimetre-level: 0-10 cm; decimetre level: 10-100 cm; metre-level: 1-10 m.

Availability is the percentage of time the position, navigation or timing solution that can be computed by the user in the coverage area. Values vary greatly according to the specific application and services used.

- System availability: is what GNSS Interface Control Documents (ICDs) refer to.
- Overall availability: takes into account the receiver performance and the user's environment.

Continuity is the ability of a system to perform its function (deliver PNT services with the required performance levels) without being interrupted for the intended operation. It is usually expressed as the risk of discontinuity and depends entirely on the timeframe of the application. A typical value is around 1*10-4 over the course of the procedure where the system is in use.

Indoor penetration is the ability of a signal to penetrate inside buildings (e.g. through windows). Indoor penetration does not have an agreed or typical means for expression. In GNSS this parameter is dictated by the sensitivity of the receiver, whereas for other positioning technologies there are vastly different factors that determine performance (for example, availability of WiFi base stations for WiFi-based positioning).

Integrity is a term used to express the ability of the system to provide warnings to users when it should not be used. It is the probability of a user being exposed to an error larger than the alert limits without timely warning. The way integrity is ensured and assessed, and the means of delivering integrity related information to users are highly application dependent. Throughout this report, 'integrity' is to be understood at large, i.e. not restricted to safety-critical or civil aviation definitions but also encompassing concepts of quality assurance/quality control as used in other applications and sectors.

Latency is the difference between the reference time of the solution and the time this solution is made available to the end user or application (i.e. including all delays). Latency is typically accounted for in a receiver but presents a potential problem for integration (fusion) of multiple positioning solutions, or for high dynamics mobile devices.

Power consumption is the amount of power a device uses to provide a position. It will vary depending on the available signals and data. For example, GNSS chips will use more power when scanning to identify signals (cold start) than when computing a position. Typical values are in the order of tens of milliwatts (for smartphone chipsets).

Robustness relates to spoofing and jamming and how the system can cope with these issues. It is a more qualitative than quantitative parameter and depends on the type of attack or interference the receiver is capable of mitigating. Robustness can be improved by authentication information and services.

Time To First Fix (TTFF) is a measure of time between activation of a receiver and the availability of a solution, including any power on self-test, acquisition of satellite signals and navigation data and computation of the solution. It mainly depends on data that the receiver has access to before activation: cold start (the receiver has no knowledge of the current situation and must thus systematically search for and identify signals before processing them – a process that can take up to several minutes); warm start (the receiver has estimates of the current situation - typically taking tens of seconds) or hot start (the receiver understands the current situation - typically taking a few seconds).

Other performance parameters

Authentication gives a level of assurance that the data provided by a positioning system has been derived from real signals. Radio frequency spoofing may affect the positioning system resulting in false data as output of the system itself.

Connectivity refers to the need for a communication and/or connectivity link of a device to be able to receive and communicate data to third parties. Connectivity relies on the integration with both satellite and terrestrial networks, such as 5G, LEO satellites, or LPWANs.

Interoperability refers to the characteristic of a product or system, whose interfaces are completely understood, to work with other products or systems, in either implementation or access, without any restrictions (e.g. ability of GNSS devices to be combined with other technologies and the possibility to merge the GNSS output with the output coming from different sources).

Resiliency is the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions; including the ability to recover from deliberate attacks, accidents, or naturally occurring threats or incidents. A resilient system will change its way of operations while continuing to function under stress, while a robust (but non-resilient) system will reach a failure state at the end, without being able to recover.

Traceability is the ability to relate a measurement to national or international standards using an unbroken chain of measurements, each of which has a stated uncertainty. E.g. in finance applications, knowledge of the traceability of the time signal to UTC is essential to ensure regulatory compliance of the timestamp.

Important Notices:

1. Applications often trade off parameters against each other depending on their requirements. For example, in safety-critical applications integrity is prioritised over accuracy, whilst in mass market applications low power consumption and TTFF are prioritised over integrity.
2. The above definitions are applicable to this report only and are not meant to be used for any other purpose.

Annex 1B: Definition of main secure SATCOM terms

This annex presents the most important Secure SATCOM terms used throughout the report.

Deployable, handheld and secure IoT user technology type

The deployable, handheld and secure IoT user technology type is mainly characterised by the capability of communicating and deploying its terminals in a more compact and easy way. The deployable user terminals (fly-away or manpack) share characteristics with the OTP terminals. However, the key difference is that they are more compact and easier for users to deploy and install. Fly-away user terminals are equipped with directional parabolic or flat panel antennas. Manpacks are deployable terminals that bridge the gap between fly-away and handheld units. They allow secure SATCOM users to carry the antenna and terminal components (such as a more robust power source) in a backpack, offering better performance and functionality than a simple handheld terminal. Handheld terminals, typically lightweight, use omnidirectional antennas that can be integrated into the terminal or carried in backpacks or held by the operator. IoT terminals uniquely identifiable connected devices can process data and communicate with each other with or without human involvement. They are usually characterised by low throughputs and periodic transmissions at regular or event-driven intervals, while they are installed either at fixed locations or at moving platforms, such as trains, and ships.

Fixed and backhauling user technology type

The fixed and backhauling user technology type is not constrained by the mobility requirement like the other two technology types. As such, the user installs the terminals in a stable place, where the secure SATCOM service will be needed for long periods of time or even permanently. Fixed user terminals are traditionally designed to allow for higher throughput than e.g. OTM/OTP and they have a simplified architecture since the antenna does not need tracking systems as it usually does in other cases. Meanwhile, backhauling terminals allow for the communication between the core network, for instance cellular base stations, and local terrestrial networks usually located in remote locations and/or unavailable via terrestrial links, by aggregating and backhauling via satellite all the data required.

On-The-Move/On-The-Pause (OTM/OTP) user technology type

The OTM/OTP user technology type is based on one major constraint, which is mobility (i.e. non-fixed connectivity). Therefore, OTM/OTP should meet the following requirement: the capability to connect to a network at a location that is rarely the same to the last connection. To fulfil this requirement, the terminals are usually integrated into a moving/transport platform (airplane, ship, or land vehicle). OTM is required when the user communicates with a GEO/NGSO constellation while installed on a moving platform, whereas OTP is required when the user must stop to allow for the pointing of the terminal's antenna and must remain immobile during communication.

(Secure) SATCOM (user) terminal

A SATCOM terminal is any device used by a user capable of establishing a satellite link for telecommunication purposes. The device normally includes the modem, the antenna and its control. More specifically, a secure SATCOM terminal guarantees enhanced levels of availability, confidentiality and integrity of the communication link. Three categories of terminals (called user technology types) have been defined, covering the vast majority of the available secure SATCOM terminals: On-The-Move/On-The-Pause (OTM/OTP); deployable, handheld and secure IoT; and fixed and backhauling.

Transparent payload

A payload that does not perform any modulation or demodulation of the data on board. The transponder and processor only perform RF processing (such as frequency conversion, amplification, filtering, multiplexing, and beam management).

Regenerative payload

A payload that can perform modulation, demodulation, and processing (encoding/decoding, routing, etc) of the data on board. This is done either with a digital on-board processor or a fully regenerative transponder.

Annex 2: List of acronyms (1/3)

3D	Three Dimensional
3GPP	Third Generation Partnership Project
5G NR	5th Generation New Radio
ACM	Adaptive Coding and Modulation
ACU	Antenna Control Unit
ADS-B	Automatic Dependent Surveillance – Broadcast
AGC	Automatic Gain Control
AI	Artificial Intelligence
ALTBOC	ALTernative Binary Offset Carrier
AMS(R)S	Aeronautical Mobile Satellite (Route) Service
APT	Advanced Persistence Threat
AR	Augmented Reality
ARAIM	Advanced RAIM
ARNS	Aeronautical Radio Navigation Service
ASAS	Airborne Separation Assistance System
ASIC	Application Specific Integrated Circuits
ARINC	Aeronautical Radio, INCorporated
ATM	Air Traffic Management
BDS	BeiDou Navigation Satellite System
BDS-3	Third Generation BeiDou System
BDSSBAS	BeiDou Satellite-based Augmentation System
BFN	Beam-Forming Network
BGAN	Broadband Global Area Network
BSS	Broadcasting Satellite Services (as defined per ITU)
BUC	Block UpConverter
CAA	Civil Aviation Authority
CDMA	Code Division Multiple Access
CED	Clock And Ephemeris Data
CERT	Computer Emergency Response Team
CGSC 2000	China Geodetic Coordinate System 2000
CIR	Committed Information Rate
CLAS	Centimetre Level Augmentation Service (QZSS)
CNE	Computer Network Exploitation
CNR	Combat Network Radio
COMSEC	COMmunication SECurity
CORS	Continuously Operating Reference Stations
COSPAS-SARSAT	(Russian) Cosmicheskaya Sistyema Poiska Avariynich Sudow - Search And Rescue Satellite-Aided Tracking
COTS	Commercial Off-the-shelf (Product)

CPU	Central Processing Unit
CRPA	Controlled Reception Pattern Antenna
CSDP	Common Security And Defence Policy
CSWAP	Cost, Size, Weight And Power
DDOS	Distributed Denial-of-Service
DFMC	Dual-Frequency Multi-constellation
DGNSS	Differential GNSS
DOCSIS	Data Over Cable Service Interface Specifications
DRFS	Direct Radio Frequency Sampling
DSSS	Direct-sequence Spread Spectrum
DV	Discrete Variable
DVB	Digital Video Broadcasting
EASA	European Union Aviation Safety Agency
ECSS	European Cooperation For Space Standardisation
EDAS	EGNOS Data Access Service
EDRS	European Data Relay System
EGNOS	European Global Navigation Overlay System
E-GNSS	European GNSS
EHF	Extremely High Frequency
EIRP	Equivalent Isotropically Radiated Power
ENISA	European Union Agency For Cybersecurity
EO	Earth Observation
EPIRB	Emergency Position Indicating Radio Beacon
ERA	European Union Agency For Railways
ERTMS	European Rail Traffic Management System
ESA	Electronically Steered Antenna
ESMAS	Egnos Safety of Life (SoL) assisted service for MAritime userS
ETA	Estimated Time Of Arrival
ETSI	European Telecommunications Standards Institute
EU	European Union
EU NAVFOR	EU Naval Forces
EUCPM	European Union Civil Protection Mechanism
EUEOMS	Eu Election Observation Mission
EUROJUST	European Union Agency For Criminal Justice Cooperation
EUSL	European Space Law
EUSPA	The European Union Agency for the Space Programme
EUTRAN	Evolved-UMTS Terrestrial Radio Access Network
EWS	Emergency Warning Satellite Service (Galileo)
EWSS	Emergency Warning Satellite Service (QZSS)

Annex 2: List of acronyms (2/3)

FE	Fundamental Elements
FDMA	Frequency Division Multiple Access
F/NAV	Navigation message provided by the Galileo E5a signal
FPGA	Field Programmable Gate Array
FSS	Fixed Satellite Services (as defined per ITU)
G1G	Galileo 1st Generation
G2G	Galileo 2nd Generation
GADSS	Global Aeronautical Distress And Safety System
GAGAN	GPS Aided Geo Augmented Navigation
GDPE	Generalised Double Phase Estimator
GMDSS	Global Maritime Distress And Safety System
GNSS	Global Navigation Satellite System
GOVSATCOM	Government Satellite Communications
GPS	Global Positioning System
GSC	Galileo Service Centre
GSM	Global System For Mobile Communication
GSO	Geo-Synchronous Orbit
HAPS	High-altitude Platform Systems
HAS	High Accuracy Service (Galileo)
HE	Horizon Europe
HPA	High-Power Amplifier
HTS	High Throughput Satellites
ICAO	International Civil Aviation Organisation
IDU	InDoor Unit
IF	Intermediate Frequency
IGS	International GNSS Service
IGSO	Inclined Geo-Synchronous Orbit
ILS	Instrument Landing System
IMO	International Maritime Organisation
IMU	Inertial Measurement Unit
I/NAV	Navigation message provided by Galileo E5b and E1-B signals
IOE	In-orbit Eavesdropping
IoT	Internet of Things
IOS	In-orbit Spoofing
ISAC	Information Sharing Analysis
ISL	Inter-Satellite Links
IT	Information Technologies
ITU-T	International Telecommunication Union-Telecommunication

KEK	Key-Encryption Key
KPS	Korean Positioning System
LAN	Local Area Networks
LBS	Location Based Service
LEO	Low Earth Orbit
LIDAR	Light Detection And Ranging
LNA	Low-Noise Amplifier
LNB	Low-Noise Block-converter
LOS	Line Of Sight
LPD	Low Probability of Detect
LPI	Low Probability of Intercept
LPWAN	Low-Power Wide-Area Network
LTE	Long-Term Evolution, commonly known as 4G LTE
M2M	Machine To Machine communications
MADOCA	Multi-GNSS Advanced Demonstration tool for Orbit and Clock Analysis
MEC	Mobile Edge Computing
MEO	Medium Earth Orbit
MEOSAR	Medium Earth Orbit Search And Rescue Satellites
MEMS	Micro Electro-Mechanical Systems
METI	Ministry of Economy, Trade and Industry
MF	Medium Frequency
MIMO	Multiple-Input Multiple-Output
MODCOD	MODulation and CODing
MOEMS	Micro Opto Electro-Mechanical Systems
ML	Machine Learning
MSS	Mobile Satellite Services (as defined per ITU)
NATO	North Atlantic Treaty Organisation
NFV	Network Functions Virtualization
NGSO	Non-Geostationary Orbit
NIS	Network Information Security
NLOS	Non Line Of Sight
NMA	Navigation Message Authentication
NMS	Network Management System
NOC	Network Operations Centre
NTN	Non Terrestrial Network
NTS3	Navigation Technology Satellite – 3
NWP	Numerical Weather Prediction
ODU	OutDoor Unit
OFDMA	Orthogonal Frequency-Division Multiple Access

Annex 2: List of acronyms (3/3)

OS	(Galileo) Open Service
OSNMA	Open Service Navigation Message Authentication
OSR	Observation Space Representation
OTM	On The Move
OTP	On The Pause
PACE	Primary, Alternate, Contingency and Emergency
PDOP	Position Dilution Of Precision
PNT	Positioning, Navigation and Timing
POD	Precise Orbit Determination
PPP	Precise Point Positioning
PPS	Pulse Per Second
PQA	Post Quantum Algorithms
PQC	Post Quantum Cryptography
PRS	Public Regulated Service
PTP	Precision Time Protocol
PVT	Position, Velocity, Time
QKD	Quantum Key Distribution
QP	Quasi-pilot
QRA	Quantum Resistant Algorithms
QZNMA	QZSS Navigation Message Authentication
QZSS	Quasi Zenith Satellite System
RAIM	Receiver Autonomous Integrity Monitoring
RBA	Remote Beacon Activation
RCS2	Return Channel Satellite Second Generation
RECS	Re-Encrypted Code Sequence
R&D	Research And Development
RF	Radio-Frequency
RFI	Radio-Frequency Interference
RNSS	Regional Navigation Satellite System
RSMC	Regional Short Message Communication
RTK	Real Time Kinematic
S2A	Space To Air
S2G	Space To Ground
S2M	Space To Maritime
S2S	Space To Space
S2X	Second Generation Satellite Extensions
SAR	Search And Rescue
SAS	Signal Authentication Service
SATCOM	Satellite Communications
SAW	Surface Acoustic Wave
SBAS	Satellite Based Augmentation System
SDN	Software Defined Networks
SDR	Software Defined Radio
SDS	Software Defined Satellite
SHF	Super High Frequency
SIS	Signal In Space
SLAS	Sub-metre Level Augmentation Service (QZSS)
SOO	Signal Of Opportunity
SPP	Single Point Positioning
SPS	Standard Positioning Service
SQM	Signal Quality Monitoring
SRC	Sample Rate Conversion
SSA	Space Situation Awareness
SSPA	Solid-State Power Amplifier
SSR	State Space Representation
SYNCHE	Synchronous Ethernet
SOO	Signals Of Opportunity
TAR	Time Ambiguity Resolution
TCA	Time of Closest Approach
TDMA	Time Division Multiple Access
TDS	Time Dissemination Scheme
TLE	Two Line Element
TN	Terrestrial Networks
TOA	Time Of Arrival
TRANSEC	TRANsmission SECurity
TRL	Technology Readiness Level
TT&C	Telemetry, Tracking and Command
TTFF	Time To First Fix
TWC	Two-Way Communications
TWTA	Traveling-Wave-Tube Amplifier
UAV	Unmanned Aerial Vehicle
UCP	User Consultation Platform
UHF	Ultra-High Frequency
UTC	Coordinated Universal Time
VDES	VHF Data Exchange System
VHF	Very High Frequency
VMS	Vessel Monitoring System
VSAT	Very Small Aperture Terminal
WAAS	Wide Area Augmentation System
WB	Wide Band
WARTK	Wide-Area Real-Time Kinematics
WLAN	Wireless Local Area Network
WMO	World Meteorological Organization

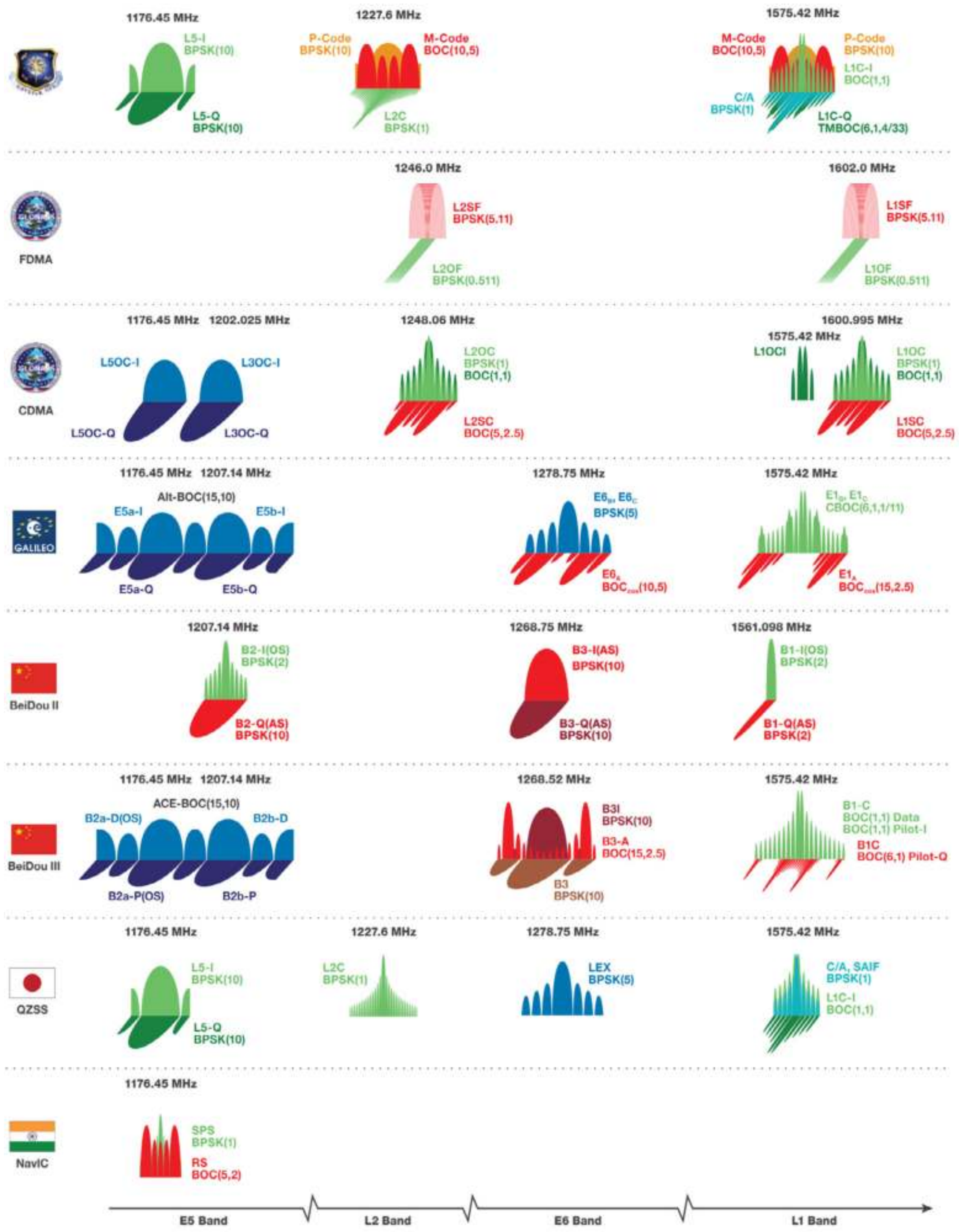
Annex 3: GNSS constellations and frequencies

GNSS CONSTELLATIONS

Parameter	GPS	GLONASS	Galileo	BeiDou III
Orbital Period (MEO)	11hrs 58min	11hrs 15mins	14hrs 04mins	12hrs 37min
Orbital Height (MEO)	22,200 Km	19,100 Km	23,222 Km	21,528 Km
Inclination (MEO)	55°	64,8°	56°	55°
Number of Orbital Planes (MEO)	6	3	3	3
Number of satellites	24 MEOs + 6 spares	24 MEOs + 2 spares	24 MEOs + 6 spares	24 MEOs + 3 GEOs + 3 IGSOs + spares
Reference frame	WGS-84	PZ-90	GTFR	CGCS 2000
Reference time	GPS Time (GPST)	GLONASS Time (GLONASST)	Galileo System Time (GST)	BeiDou Time (BDT)

RNSS CONSTELLATIONS (REGIONAL COVERAGE)

Parameter	NavIC	QZSS	KPS
Coverage	India and a region extending 1,500 km (930 mi) around it	Asia-Oceania region	Korean peninsula and surrounding areas
Number of satellites	5 IGSOs + 3 GEOs	3 IGSOs + 1 GEO	5 IGSOs + 3 GEOs
Reference frame	WGS-84	JGS	Korea Geodetic System 2020 (KGeS2020)
Reference time	IRNSS Network Time (IRNWT)	QZSS Time (QZSST)	Korea Standard Time (KST)



Source: adapted from Navipedia, http://www.navipedia.net/index.php/GNSS_signal

Back to main table of contents | Back to annexes overview page

Annex 4: Methodology used for creating the user technology report

The GNSS User Technology Overview section of the GNSS and Secure SATCOM User Technology Report uses outputs of the EUSPA's internal Technology Monitoring Process (TMP).

It complements the market monitoring and forecasting process, and its objective is to monitor trends and developments in the GNSS supply industry. It supports the EUSPA in defining the best strategy towards Galileo market adoption; in providing updated statistics on Galileo penetration in user terminals and chipsets; and in analysing Galileo positioning among other GNSS and location technologies.

Part of the process is to keep up-to-date independent analysis, which assesses the capabilities of user terminals, receivers, chipsets and modules currently available on the market. For the analysis, each device is weighted equally, regardless of whether it is a chipset or a receiver, and no matter what its sales volume is. The results should therefore be interpreted not as the split of constellations utilised by end-users, but rather the split of constellations available in manufacturers' offerings.

The analysis includes all major receiver manufacturers in Europe and worldwide, such as: Accord, ACR Electronics Inc, Airbus Group SE, Allystar, Alpine Electronics Inc, Arag S.R.L., Arbiter Systems, Beijing Bdstar Navigation Co Ltd, Beijing UniStrong Science and Technology Corporation Limited, Broadcom, Cobham Plc, ComNav Technology Ltd, Deere & CO, DJI Baiwang Technology Co Ltd, Elproma, Esterline, Faro Technologies INC, FEI-Zyfer, Furuno, Garmin, GMT Co Ltd, Heico, Hexagon AB (Leica, Novatel), Huawei (HiSilicon), Hitachi Ltd, Hi-Target Surveying Instrument Co Ltd, Honeywell, Hopf Elektronik GMBH, Hyperion, Intel, Japan Radio Co Ltd, Johnson Outdoors Inc, Jotron, Kongsberg, Mediatek, Meinberg Funkuhren GmbH & Co. KG, Microchip Technology, Microsemi Corp, Moog Broad Reach, National Instruments Corp, Navico (Navico Holding As), Newspace Systems, NVS Technologies AG, Ocean Signal, Oscilloquartz SA, Qualcomm, Riegl Laser Measurement Systems, Rockwell Collins Inc (UTC), RUAG, Safran (Orolia), Samsung Electronics Co Ltd, Samyung ENC Co Ltd, SatLab, Seiko Solutions Inc, Septentrio, Shanghai Huace Navigation Technology Co Ltd, SONY, SpaceManic, STMicroelectronics, Surrey Satellite Technology Ltd, Synergy Systems LLC, Telit, Tersus, Thales SA, Topcon Corporation, Total, Trak Microwave, Trimble Navigation Ltd, u-blox, Unisoc.

The GNSS and Secure SATCOM User Technology Report also addresses in detail the Secure SATCOM topic. The dedicated section has been made with publicly available sources.

Secure SATCOM terminals have been segmented according to their mobility through three different user technology types: (1) On-The-Move/On-The-Pause (OTM/OTP) (2) Deployable, Handheld and secure IoT and (3) Fixed and backhauling.

The last user technology type focuses on users with no mobility requirements while the others are dedicated to users that require to establish a secure SATCOM link in changing positions. The technological landscape and evolution have been analysed, based on the most relevant technologies considered by the authors, but it is not a full exhaustive technological review of all secure SATCOM technologies.

The information contained within this report is a compilation of in-house knowledge, scientific papers, receiver and other user technology manufacturers' websites and, if needed, has been verified by consultation with experts in the relevant domain.

Annex 5: About the authors

The European Commission

European Commission (EC) and more specifically the Directorate General for Defence Industry and Space (DG DEFIS) has overall responsibility for the implementation of the Union Space Programme and its components (Galileo, EGNOS, Copernicus, GOVSATCOM and SSA).

This includes:

- Overseeing the implementation of all activities related to the programme;
- Defining its priorities and long-term evolution;
- Managing the funds allocated to the programme;
- Ensuring a clear division of responsibilities and tasks, in particular between the EU Agency for the Space Programme and the European Space Agency;
- Ensuring proper reporting on the programme to the Member States of the EU, the European Parliament and the Council of the European Union.

DG DEFIS further contributes to shaping the EU space policy and fostering a strong, innovative and resilient EU space ecosystem. It supports the emergence of New Space in the EU, including SMEs and new entrants, fosters entrepreneurship and access to finance, and contributes to the growth of the EU space industry.

DG DEFIS promotes EU space research fostering a cost-effective, competitive and innovative space industry and research community. It ensures that space technology, services and applications meet EU policy needs, and the R&I needs of the EU Space Programme. It also ensures that the EU can access and use space with a high level of autonomy.

The EU space policy addresses some of the most pressing challenges facing the EU today, such as fighting climate change, supporting EU's priorities, whilst strongly contributing to the green and digital transitions and to the resilience of the Union.

The European Union Agency for the Space Programme

EUSPA is the operational European Union Agency for the Space Programme. It adopts a user-oriented approach to promote sustainable growth and improve the security and safety of the European Union. EUSPA's mission revolves around three core principles: service provision, market growth, and security.

The EU Agency for the Space Programme:

- Provides state-of-the-art, safe and secure positioning, navigation and timing services based on Galileo and EGNOS, cost-effective satellite communications services for GOVSATCOM and soon IRIS[2], and Front Desk services of the EU Space Surveillance Tracking whilst ensuring the systems' service continuity and robustness.

- Promotes and maximises the use of data and services offered by Galileo, EGNOS, Copernicus, GOVSATCOM and soon IRIS[2] across a broad range of domains.

- Fosters the development of a vibrant European space ecosystem by providing market intelligence, and technical know-how to innovators, academia, start-ups, and SMEs. The agency leverages Horizon Europe, other EU funding, and innovative procurement mechanisms.

- Implements and monitors the security of the EU Space Programme components in space and on the ground with the aim to enhance the security of the Union and its Member States; EUSPA operates the Galileo Service Monitoring Centre.

The Security Accreditation Board established within the Agency is the security accreditation authority for all of the Programme's components, where Member States take accreditation decisions in a strictly independent manner from the Programme.

EUSPA Mission Statement

The mission of the European Union Agency for the Space Programme (EUSPA) is defined by the EU Space Programme Regulation. EUSPA's mission is to be the user-oriented operational Agency of the EU Space Programme, contributing to sustainable growth, security and safety of the European Union.

The EU Agency for the Space Programme:

- Provides state-of-the-art, safe and secure positioning, navigation and timing services based on Galileo and EGNOS, cost-effective satellite communications services for GOVSATCOM and soon IRIS², and Front Desk services of the EU Space Surveillance Tracking whilst ensuring the systems' service continuity and robustness.
- Promotes and maximises the use of data and services offered by Galileo, EGNOS, Copernicus, GOVSATCOM and soon IRIS² across a broad range of domains.
- Fosters the development of a vibrant European space ecosystem by providing market intelligence, and technical know-how to innovators, academia, start-ups, and SMEs. The agency leverages Horizon Europe, other EU funding, and innovative procurement mechanisms.
- Implements and monitors the security of the EU Space Programme components in space and on the ground with the aim to enhance the security of the Union and its Member States; EUSPA operates the Galileo Service Monitoring Centre.

The Security Accreditation Board established within the Agency is the security accreditation authority for all of the Programme's components, where Member States take accreditation decisions in a strictly independent manner from the Programme.

The European Union Agency for the Space Programme: linking space to user needs.

market@euspa.europa.eu

www.euspa.europa.eu

@EU4Space

EUSPA

@space4eu

#EUSpace

Catalogue Number: TS-01-25-000-EN-N

ISBN 978-92-9206-088-6

doi: 10.2878/9596833