

# **GNSS** Interference

© ESA-Pierre Carril

 "The Full Operational Capability phase of the Galileo programme is managed and fully funded by the European Union. The Commission and ESA have signed a delegation agreement by which ESA acts as design and procurement agent on behalf of the Commission. "Galileo" is a trademark of the European Union."

#### **Executive summary**

GNSS signals are vulnerable to radiofrequency interference. To address this threat, for more than 15 years Septentrio has been perfecting and fielding unique interference mitigation techniques.

These countermeasures include adaptive notch filtering, pulse blanking, and unique wide band interference mitigation. Working in concert, these and other analogue and digital countermeasures form Septentrio's AIM+ (Advanced Interference Mitigation).

The effectiveness of AIM+ has been demonstrated repeatedly in various real field applications. AIM+, as part of a larger range of Septentrio innovations, helps safeguard positioning accuracy and availability in all possible circumstances.

Over the last 20 years, GNSS has truly established itself as part of the critical infrastructure in today's world – no longer just for positioning and navigation but across a diverse range of applications and markets, especially autonomous vehicles on land, in the air and at sea. These satellite navigation signals are very weak and vulnerable to interference: a phenomenon where other radio signals disrupt the GNSS signals causing reduced positioning accuracy, or even the complete lack of position availability.

This brochure introduces the different types of radio-frequency interference (RFI), their effect on GNSS signals and receivers, and how Septentrio GNSS receivers identify, monitor and overcome the effects of such harmful interference, along with real-life examples from the field.

# It's a noisy, crowded world out there!

# The electro-magnetic radiation and radio frequency spectrum

GNSS radio signals as received on the Earth are extremely weak by design: about 100 times weaker than the background noise of other radio signals. Without special techniques, using a general purpose radio-frequency receiver and antenna, you would not even "hear" the signals above the background static. Think of this as if you would try watching a 100 W lightbulb flying at a height of 20 000 km, it would be impossible to see. The RF spectrum is packed with many existing signal bands such as VHF, microwave, 3G, WiFi and Bluetooth, yet the introduction of new protocols such as 4G LTE and 5G amongst many others is crowding it further.

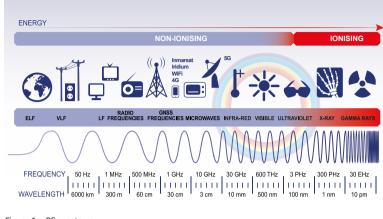


Figure 1 – RF spectrum

Even though the various GNSS (GPS, GLONASS, Galileo and BeiDou) transmit in dedicated frequency bands, there are many RF signals which are emitted 'just next to' GNSS. Some of those signals spill over into the GNSS bands, impacting quality and accuracy of the position, and sometimes even drowning out GNSS signals completely. Moreover, sometimes people disturb the GNSS signals directly, unintentionally or on purpose. There have been reports of flawed maritime television antennas jamming GNSS signals. And with the proliferation of vehicle tracking systems and GNSS-based road tolling, there is a clear increase in the presence of illegal but cheap GNSS car jammers.

### How interference impacts GNSS

Professional GNSS receivers can still extract the GNSS information from the background, even if that background noise is increased slightly by the spillover signals. For the majority of applications using GNSS, positioning is the main objective.



#### Key GNSS positioning performance metrics

GNSS positioning performance depends on the availability and the accuracy of satellite measurements (code pseudo ranges and carrier phases). To deliver high-accuracies and resilience, such high-end receivers track signals at various frequencies and of multiple GNSS constellations as seen below.

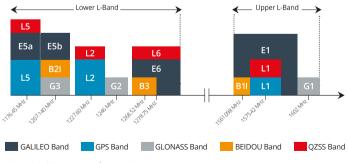


Figure 2 – RF spectrum for GNSS

This redundancy allows the positioning accuracy of high-end receivers to remain unaffected when only few satellite measurements are disturbed by interference. However, a source of interference is likely to affect multiple signals in the same GNSS frequency band and may even completely block reception of a whole GNSS band. In this case, the effect at the positioning level can be more severe.

Consider if GLONASS L2 (G2 above) reception were completely lost, a receiver in GPS and GLONASS dual-frequency RTK mode would have to switch to GPS-only dual-frequency RTK mode, with potentially reduced accuracy as a result. Should L2 reception be completely lost on both GPS and GLONASS, the same receiver would have to fall back to another position mode such as L1-only RTK, to DGNSS operation or even stand-alone mode.



For applications relying on an RTK solution accuracy of a few centimetres, falling back to a non-RTK mode (such as differential code) could be unacceptable and stop the application from working.

### The good, the bad and the ugly

Interference can come in many different forms, but first it is useful to consider how it is generated. The most common sources are electrical and electronic devices, from everyday items in a home, office, shopping centre or construction site, to those more specific to airports, military installations, ships, industrial machines and communication towers. One simple example is how a radio can sometimes buzz when a mobile phone is operating nearby. Different interferers leave their own footprint on the RF spectrum. Read multiple interference insights on our website septentrio.com/insights

Wide-band jammer

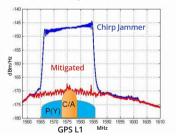


Figure 4 – GPS L1 signal contaminated with a chirp jammer signal: before (blue) and after (red) activation of WIMU (Wide-band Interference Mitigation Unit)

Interference can be described physically through the following two behaviours:

Temporally – depending on how the interference changes over time (in the 'time domain').

An interfering signal may be either:

- non-pulsed (i.e. continuous and always on) or
- pulsed (behaving like a flashing light)
- > Frequency where in the RF spectrum the interference comes from, and its footprint.
- in band directly on the same frequency as a GNSS signal
- partially in band overlapping across the same frequency as a GNSS signal,
- out of band adjacent or nearby in frequency to a GNSS signal
- narrow-band or wide-band this describes the width of the RF band that the interference occupies.

#### Multiple narrowband interference

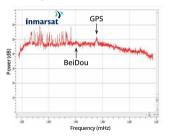


Figure 5 – Satellite communications signals can interfere with GPS signals in L1 band

#### Self-interference

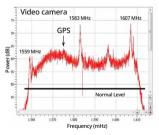


Figure 6 – L1-band Interference from a GoPro™ Hero 2 video camera picked up by GPS antenna

### **Beating interference**

Interference in all its forms must be factored into the architecture, design and development of a highend GNSS receiver from the very start of the design process and impacts all parts of the receiver. From the analogue design in the RF front end – the antenna and those parts of the receiver which capture and treat the high-frequency signals – to the conversion to digital signals and the treatment of those signals with various digital filters and countermeasures, all have to work in concert to effectively combat interferers.

As each interfering signal has its own individual fingerprint, adaptive filtering and innovative signal processing techniques are needed to effectively deal with the many forms of interference encountered in real life. AIM+ combines an array of techniques to mitigate jamming: a set of configurable adaptive notch filters and special pulse blanking technology are complemented by an adaptive wide-band filter capable of rejecting more complex types of interference such as that from GNSS chirp jammers, frequency-hopping signals from aviation devices as well as high-powered Inmarsat transmitters.

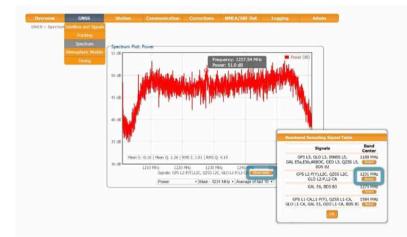


Figure 7 – Visualising RF interference – the spectrum view plot

Visualising the RF spectrum, the type and frequency of the interfering signal, provides an easy way for users, and especially for law enforcement officers, to investigate whether RF interference is present and what may cause them. Using a real-time spectrum analyser built into the receiver, the user can assess the frequency spectrum of all signals entering the receiver. Spectrum figures in this brochure have been created using this internal receiver spectrum plot capability. Figure 7 shows the L2 frequency band with the GPS L2P signal at 1227.60 MHz indicated. Via an intuitive user interface, other bands can easily be selected and visualised as well.

### Adaptive notch filtering

An adaptive notch filter minimises the impact of continuous wave and narrow-band interference on a receiver's performance, by continuously monitoring the incoming signals for the presence of an interferer. Whenever one is identified, a narrow digital filter (notch filter) is aligned with the interfering signal so that specific interferer is mitigated or suppressed. This operation of the notch filter can be fully automated (including the adaptive fine-tuning of its bandwidth and centre frequency) but, if required, can also be set up or adjusted manually.

### L2 band before applying notch filter

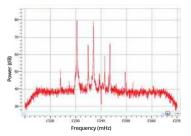


Figure 8 – Local interference shown as the large spikes

### L2 band after applying notch filter

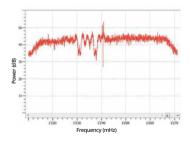


Figure 9 – Note how the peaks have been suppressed by the notch filter

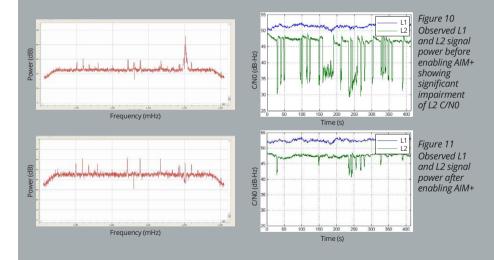
# USER STORY - Overcoming jamming in the fields

A local farming co-operative near Tyumen in Russia was upgrading their farm equipment to add high precision systems for autosteer and precision-farming applications, along with a local base station to provide the required RTK corrections. When they were trying to activate the base station's correction data service, all rovers were unable to obtain an RTK position because of high levels of local interference. Equipping the base station with AIM+ capabilities, and activating adaptive notch filtering, largely suppressed the local interference and cm-accurate positioning became possible.



#### USER STORY - Fixing RFI to get RTK fixes

Many GNSS surveying receivers in the region of Hilversum had trouble maintaining an RTK fix (necessary for centimetre accuracy). When investigating this further, the problem was traced to a radio tower housing an amateur radio transmitter. As this transmitter had a centre frequency of 1240.4 MHz, it was essentially a narrow-band jammer in the GLONASS L2 band (figure 2).





Without AIM+ countermeasures enabled, the C/N0 (a measure of the GNSS signal strength against the background noise) of the L2 signal was severely degraded (figure 10).

After enabling adaptive notch filters, the extraneous signal was suppressed and most importantly, the C/N0 of the L2 signal was much less affected, allowing cm accurate positioning again (figure 11).

### Wide-band interference mitigation unit (WIMU)

The intermittent nature of most jamming events makes them difficult to detect and even more difficult to overcome or predict, which is why Septentrio offers built-in protection against jamming as standard.

GNSS chirp jammers, for example, are small portable low-power devices available via the internet which can easily block out GNSS signals to the extent that it prevents tracking any GNSS satellite. A single 10 mW chirp jammer powered from a 12 V car socket is powerful enough to knock out GNSS signals in a radius of several hundred metres. Chirp jammers are much more difficult to protect against than narrowband 'accidental' jammers, because of the rapid frequency variation (or 'chirping' nature) of their signal which makes notch filters ineffective.

To illustrate the effect, a test was done with a GNSS simulator to see the real impact on positioning in Tampa, Florida. A 10 mW PPD chirp jammer in the centre of Tampa would jam the GNSS signal over a radius of 400 metres meaning 'No RTK' for any GNSS receiver within the red zone indicated in figure 13. The blue trace from the chirp jammer below in figure 12 shows the dramatic results when it interferes with the GPS L1 band.

Once interference mitigation measures have been applied by the AIM+ enabled GNSS receiver, the red trace in figure 12 shows how the (normal) signal (re) appears. With AIM+ activated, the red 'No RTK' zone, is reduced from about 400 m to a few metres effectively confining the range of the jammer to the car it's plugged into. It is worth noting that any other GNSS receivers in the red zone which don't possess AIM+ technologies would not be able to get RTK fixes within that area.

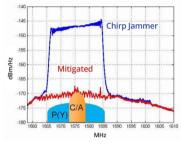


Figure 12 – GPS L1 signal contaminated with a chirp jammer signal: before (blue) and after (red) activation of WIMU (Wide-band Interference Mitigation Unit)



Figure 13 – 10 mW Chirp jammer without mitigation



Figure 14 – 10 mW Chirp jammer with activated AIM+

### Are you ready for driverless cars and GNSS road tolling?

The steady increase in road-going vehicles and the trend towards autonomous vehicles, both of which demand GNSS positioning, is matched by a growing number of illegal jamming devices on the road. Jamming signals can affect GNSS availability over several kms, making it difficult to reliably identify those vehicles equipped with jammers.

# USER STORY - Setting the trap to catch vehicle-mounted jammers

A new technique uses an AIM+ enabled system, mounted on a gantry spanning the toll highway which monitors the presence of GNSS jamming passing through the toll gate. By having two GNSS antennas monitoring for interference, a very reliable means of identifying the exact lane of the offending jammerequipped vehicle was provided. The system also provides a precise time stamp of the exact moment that the jammer passes the detection system and can be connected to cameras for license plate identification. For the full story see GNSS Jamming and Road Tolling on septentrio.com/insights

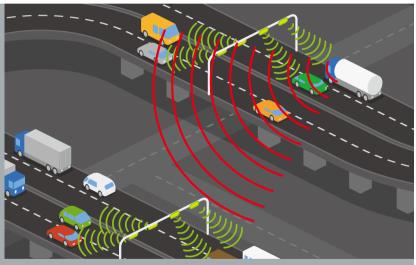


Figure 15 - White truck with illegal jamming device to avoid paying road toll

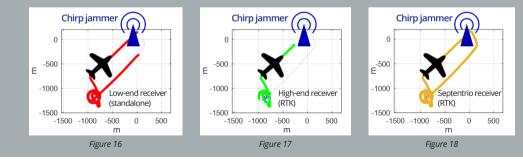
In a recent experiment, over the course of just 7 days, 115 hours of data was collected and 45 jamming events were seen: 16 from chirp jammers, 10 from pulsed jammers and 19 interference events from other sources. Remember that these jammers not only disable the GNSS receiver in the offending car or truck, but possibly GNSS receivers in a wide area surrounding this vehicle.

### Drones and jamming

The use of drones in everyday life has rocketed with applications going from real estate photography and event videography over parcel delivery, surveillance and inspections to aerial mapping and many more. One of the biggest threats to drone safety is GNSS interference. At the very least, disruptions to GNSS signals can impact position quality to drop below high-accuracy RTK to less-accurate positioning modes, hampering some of the high precision applications. In the most extreme cases, interference can cause the drone to lose position awareness and force it to land immediately regardless of where it is and what may be below.

#### USER STORY - The effect of a 10 mW jammer

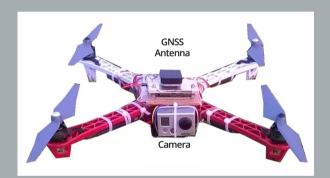
With only 10 mW, jammers are powerful enough to knock out GNSS signals for several hundred metres on land. In the air, the jamming signals have a greater reach – up to 1 km or more – as they are unhindered by trees, buildings and the like. Figure 17 below shows how a 10 mW jammer knocks out RTK positioning over more than 1 km in an unprotected high-accuracy receiver in the air. Even a lower accuracy consumer grade L1 receiver (figure 16) as often used in the navigation system of drones, which is less accurate and less sensitive to interference, loses positioning information up to several hundred metres from the source of interference. With AIM+ countermeasures activated (figure 18), the receiver is able to maintain an RTK fix throughout the simulated flight as well as showing no degradation to its position. More details on this case can be found in our Jam Proofing Drones insight, see septentrio.com/insights



### Internal interference: self-jamming of drones caused by a camera

The small size of drones often means that many different electronic systems are packed closely together and in close proximity to the GNSS antenna. These other electronics, such as motors or cameras often cause harmful interference that degrades or inhibits GNSS positioning.

#### **USER STORY - Drones and self-jamming**



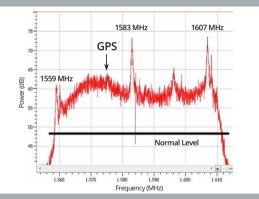


Figure 19 - GoPro™ Hero 2 camera pick-up monitored by an AsteRx4 receiver

The above figure 19 shows what happened to the GPS L1-band spectrum when a consumer action camera was installed on a quadcopter. The three peaks in the spectrum are exactly 24 MHz apart pointing to their origin: the MMC/SD logging interface used in a range of consumer action cameras. For the design engineers this view of the RF spectrum analyser was an invaluable tool for both identifying the source of interference and determining the effectiveness of measures such as modifying the setup or adding shielding, measures which are important complements to receiver solutions such as AIM+. For the quadcopter installation in this example, the loss of RTK was solved by a combination of placing the camera in a shielded case and activation of AIM+ interference mitigation.

### Fighting military interference peacefully

## USER STORY - Protecting against unwanted leaking of military jammers into civilian waters and projects

Commercial marine dredging operations are essential to keep busy waterways and harbours open for international trade. However, as happened recently, these operations can significantly have an impact when the transmissions of a military system normally used for military exercises 'leaks' into commercial waterways. The impact of this military system was significant with major periodic in-band interference, knocking out the complete L2 band (both for GPS and GLONASS) on all commercial receivers every 7 seconds for a few hundred milliseconds (ms). With the activation of AIM+ countermeasures in the land-based reference receivers and the ship-based receivers, all of the in-band interference was reliably filtered out from the GPS and GLONASS L2 bands leaving real high-quality GNSS signals available for the high accuracy real-time positioning needed for these dredging operations.

Thanks to AIM+ technology being activated on these receivers, dredging work could continue with minimal delay from external interferers, avoiding losses in the range of 10 000s of dollars per hour of interrupted operation of these expensive dredging ships.



### Interference - a fact of life

#### Regional communications systems adjacent to GNSS

There are several well-known examples where existing and planned communications infrastructure around the world significantly impacts the performance of GNSS positioning.

- Globally, LTE (Long-term Evolution) cellular communications, Inmarsat and Iridium
- Regionally, Ligado (formerly Light Squared) in USA and DoCoMo in Japan

The examples of Light Squared and Ligado operation close to the GPS L1 frequency show that the RF spectrum is an increasingly rare commodity, and efforts to expand ever more access to internet and data for ever more people inevitably impact other existing systems such as GNSS.

#### Robustness against LTE interference in central Tokyo

A LTE base transceiver station located in central Tokyo, capable of providing higher rate cellular data and voice communications, knocked out the GNSS signals over a radius of more than 100 metres.



The AIM+ enabled receiver operating at this location consistently tracks signals from more satellites than one impacted by the LTE signal, essential when striving to provide accurate and reliable position solutions.

### Summary

The ever-increasing number of connected devices operating across the increasingly crowded RF spectrum can cause unintentional interference of GNSS signals. Maintaining position accuracy, reliability and availability is a serious challenge both today and tomorrow for GNSS receivers operating in this crowded RF interference environment. As more and more new applications for GNSS are developed, challenges grow as more complex forms of interference appear worldwide. Identifying and overcoming interference with the application of advanced mitigation technologies is critical to ensure the quality of GNSS measurements and positioning.

#### 1. RF Interference is everywhere!

RF signals can cause interference with GNSS operation, unintentionally or intentionally. The presence of interference is increasing at an alarming rate, as more and more electronic devices are being used everywhere. GNSS and its unique features make it a critical provider of positioning in many existing and new technologies, such as autonomous systems (vehicles, drones, machines and vessels).

#### 2. Solving GNSS interference

The omnipresence of interference in all its forms limits the accuracy, reliability and availability of GNSS positioning systems, and their final applications. Overcoming these interferers reliably and effectively requires an intimate experience of GNSS and its characteristics, along with mastery of complex technologies and algorithms. These solutions need to be designed into the GNSS receiver from the start and complemented with other measures.

#### 3. Adapt, evolve, overcome

Septentrio's Advanced Interference Mitigation (AIM+) technology has been designed as a core built-in component of all of Septentrio's products in the analogue and digital domains. The resources built into its receivers allow the technology to continue to evolve and be tuned based on new experiences, new signals and new interferers.

#### Septentrio's solutions

Septentrio's AIM+ technology meets this challenge head-on with a market-leading range of interference countermeasures in the analogue and digital domains, combined with Septentrio's ongoing commitment to track all navigation signals in the sky.

With more than 15 years of experiences around interference, our latest AIM+ technology brings the best of all the latest innovations on hardware/software and comprises of continuous design of dedicated hardware, software and countermeasures to mitigate continuous wave, narrow-band and pulsed interference (amongst others). In most cases, position accuracy and availability can be maintained even when a whole GNSS band is jammed thanks to the abundance of GNSS signals on multiple frequencies from multiple constellations. The more signals, frequencies and constellations a receiver can track, the more likely its AIM+ countermeasures will be able to overcome interference on tracked signals.

In summary, the effectiveness of Septentrio's AIM+ technology has been repeatedly demonstrated in real field applications and ensures customers of highest possible GNSS performance (positioning accuracy, reliability and availability) in all possible circumstances – no matter how challenging the RF environment.

### Septentrio's AIM+ Technology

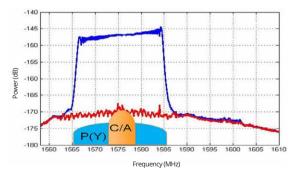
Septentrio has developed a sophisticated RF interference monitoring and mitigation system (AIM+). This AIM+ technology is built into every Septentrio receiver. Working in harmony together, a suite of analog and digital countermeasures forming Septentrio's AIM+ tools typically include:

- Adaptive Multiple Notch Filters
- Pulse Blanking Units
- Wide-band Interference Mitigation Unit (WIMU)
- Integrated Spectrum Analyser visualisation tools to view the RF input from the antenna in both time and frequency domains.

To mitigate the effects of narrow-band interference, multiple notch filters can be configured either in auto or manual mode. These notch filters effectively remove a narrow part of the RF spectrum around the interfering signal. The L2 band, being open for use by radio amateurs, is particularly vulnerable to narrowband interference. The effects of wide-band interference, both intentional and unintentional, can be mitigated by enabling the Wide-band Interference Mitigation Unit. This system also reduces, more effectively than traditionally used pulseblanking methods, the effects of pulsed interference.

#### A never ending battle

As a premier maker of high-end GNSS receivers, Septentrio is continuously developing and optimising its AIM+ technologies to provide customers with the best chances of overcoming the increasing number of interfering signals. These developments will keep evolving to rise and respond to new interferers and threats.



GPS L1 signal contaminated with a chirp jammer signal: before (blue) and after (red) activation of WIMU also shown on page 6

### Glossary

Accuracy: a common navigation system performance indicator that checks the solution error.

Adaptive notch filter: is an algorithm to achieve narrow-band interference rejection.

AIM+: Advanced Interference Mitigation (AIM+), is a market-leading range of interference countermeasures, developed by Septentrio. It is a core component of all Septentrio's products in the analogue and digital domains.

Availability: a common navigation system performance indicator that checks the amount of time the expected solution is available to the user.

Carrier phase measurement: a measure of the range between a satellite and receiver expressed in units of cycles of the carrier frequency.

Chirp jammer: this is a GNSS jammer or PPD (Personal Privacy Device) that is used to disrupt GNSS signals by sweeping through a certain frequency range (like a siren). It can be installed in a vehicle to disrupt road tolling tracking equipment to avoid paying road toll. Using this device is illegal.

DGNSS: a network of reference stations. There are several DGNSS techniques, such as classical DGNSS (or DGPS), Real Time Kinematic (RTK) and Wide Area RTK (WARTK). DoCoMo: a mobile phone operator in Japan

GNSS: Global Navigation Satellite Systems or the generic term for satellite navigation systems that provide autonomous geo-spatial positioning with global coverage. Common GNSS Systems are GPS, Galileo, GLONASS and BeiDou.

Inmarsat: a British satellite telecommunications operator, offering global mobile services. In GNSS often used to distribute corrections to improve accuracy.

Interference: (in a GNSS context) the unwanted negative impact of other RF signals on a GNSS signal.

Iridium: an American satellite telecommunications operator, offering global mobile services.

Jamming: unintentional or intentional interference impacting the accuracy, reliability and availability of a GNSS receiver.

Ligado: an American wireless communication service provider developing a satellite-terrestrial network to support 5G and Internet of Things applications in North America. LTE: a 4G mobile communications standard.

MMC/SD logging: Data logging through the use of a multimedia or SD card.

Pseudo range: a measure of the distance between a satellite and a navigation satellite receiver.

Pulse blanking: technique of 'ignoring' all signals (including the GNSS signals) for a very short time during a strong pulsing signal that comes from a pulsing RF interference source, whilst tracking and using signals observed between the pulses. As an analogy, think of a lighthouse at night. Every 15 seconds or so, the light is shining directly at you and 'blinding' you. To ignore this light, you could try and blink every 15 seconds when the lighthouse shines at you.

Radio spectrum: The electromagnetic spectrum with frequencies from 3 Hz to 3000 GHz (3 THz). Electromagnetic waves in this frequency range, called radio waves, are widely used in modern technology, particularly in telecommunication.

Reliability: describes the ability of a system or component to function under stated conditions for a specified period of time. In GNSS terms, the confidence that the position is correct and accurate within the indicated error limits.

RF: Radio frequency, a frequency or band of frequencies, suitable for use in telecommunications.

RTK: Real-Time Kinematic positioning, a satellite navigation technique used to enhance the accuracy of a GNSS position.

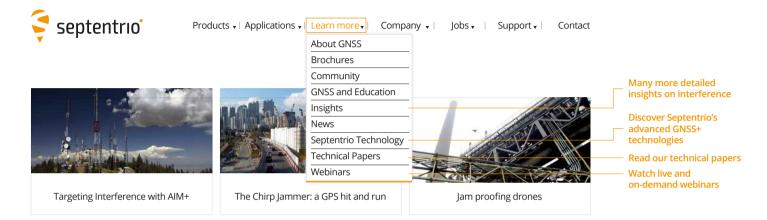
Spectrum Analyser: visualising tool to measure the magnitude (amplitude or strength) of a given input signal set against the full frequency range of the instrument.

**Spoofing:** the intentional broadcast of altered and misleading GNSS signals and information, ultimately fooling a GNSS receiver into giving an incorrect position. Users typically do not notice the presence of spoofing as there is no loss in 'signal availability' and can wrongly assume that signal availability means reliable positioning.

UAV: an unmanned aerial vehicle or an aircraft piloted by remote control or onboard computers.

WIMU: wide-band interference mitigation unit that can reduce or eliminate interference from a wider frequency range.

### Explore septentrio.com for more background info on interference





GPS spoofing: is your receiver ready for an attack?

Set adrift by GPS jamming

6 essentials for a machine control GPS receiver

#### EMEA

Greenhill Campus (HQ) Interleuvenlaan 15i 3001 Leuven, **Belgium** 

#### Espoo, Finland

Americas

Suite 200 23848 Hawthorne Blvd Torrance, CA 90505, **USA** 

septentrio.com/contact



Asia-Pacific Shanghai, China Yokohama, Japan Seoul, Korea

septentrio.com



