

GSS200D

INTERFERENCE DETECTION AND ANALYSIS SOLUTION

A new way to understand your RF environment

Because Radio Frequency Interference (RFI) impacts GNSS performance, knowing your RF environment is critical. The Spirent GSS200D is a truly end-to-end solution that builds up a complete picture of interference activity at a site of interest.



GNSS interference is a growing threat

Interference is the most important threat to GPS and other global navigation satellite systems (GNSS), and it is becoming more common. This is partially due to the popularization of illegal jammers of the kind that are commercially available online and powered by a vehicle's power socket. However, RFI can also be unintentional - especially in busy industrial areas. At the same time, satellite positioning data from GPS and other GNSS systems is being increasingly relied upon in many industries. For safety-related and commercially sensitive applications, such as critical infrastructure or civil aviation, intentional and accidental jamming has the potential to fundamentally disrupt key outcomes. And the implications are potentially disastrous.

Monitoring the GNSS signal environment gives the benefit of allowing interference events to be correlated with any unexpected outages or system behaviour. This allows GPS jamming to either be highlighted or, just as significantly, eliminated as a cause of the problems.

Introducing GSS200D

The GSS200D continuously monitors and analyses the GNSS bands for interference events, enabling 24/7 constant monitoring on multi-constellation and multi-frequency bands.

When RFI is detected in one or both frequencies, the system will capture the interference data and send an encrypted event to PT Cloud, Spirent's secure cloud. Events are characterised

and given a type, because it is important to understand the difference between unintentional interference and jamming. They are also automatically ranked according to a score based on the likely impact to GNSS services, allowing a quick prioritisation of the threats.

What's more, whenever an event occurs, you can choose to be notified by email almost instantaneously.

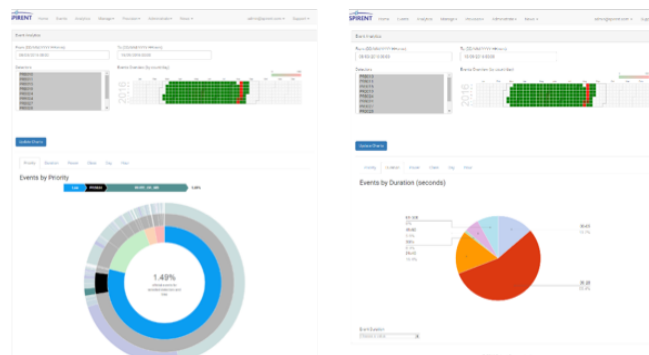
By using the GSS200D it is possible to distinguish different types of interference and jamming, to highlight multiple detections of the same jammer, to identify trends in RFI threats, and to support decision making about the development of countermeasures.

In a nutshell, the GSS200D gives you a comprehensive picture of your RF environment.

PT Cloud

Spirent's cloud server, PT Cloud, is the secure, fast and easy way to access the data detected by the GSS200D. Interference events are logged with the spectrum and spectrogram of the signal, and include information such as duration, power, type and priority of interference.

PT Cloud integrates data analytics and visualization tools, enabling monitoring over time and in-depth trend analysis - quantified information about GNSS interference threats at your site of interest.



Discover PT Cloud's data analytics and visualization tools

GSS200D

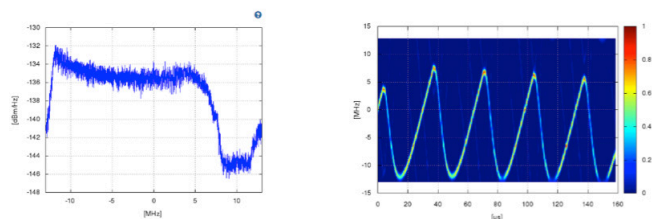
INTERFERENCE DETECTION AND ANALYSIS SOLUTION

	GSS200D GPS GLO L1	GSS200D GPS L1 L5
		
Segments	<p>Critical Infrastructure</p>  <p>Telecoms networks and service providers, Connected and Autonomous Vehicles, Road Tolling, Ports, Rail, Power Grids</p>	<p>Civil Aviation SBAS/GBAS</p>  <p>Airports, Air Navigation Service Providers, Regulation authorities, GBAS/SBAS Equipment and Service Providers</p>
Supported Bands	GPS / GALILEO / GLONASS L1	GPS / GALILEO L1 L5 (E5a)
Bandwidth	GPS L1, 16 MHz (± 8 MHz) GLO L1, 9 MHz (± 4.5 MHz)	L1 (1575.42MHz), 20 MHz (± 10 MHz) L5 (1176.45MHz), 20 MHz (± 10 MHz)
RFI Detection based on	Calibration level, with absolute power.	GPS L1: ICAO Mask Annex 10 GPS L5: EUROCAE Galileo MOPS for E5a DME / TACAN pulsed RFI identification
Spoofing Alerts	Not supported	Jam and spoof Take-over spoofing



Capture on L1 for event 711. Event start time: 10/03/2017 08:44:27

Priority	Frequency	Power	Class	Detector	Capture Time	Duration (s)	DME / TACAN
High	L1	-61.950686	Chirp-triangular	10001	10/03/2017 08:44:54	46	No



Detected jammer signature observed on PT Cloud

SALES AND INFORMATION

Spirent Communications plc, Aspen Way, Paignton, Devon TQ4 7QR, UK
T: +44 1803 546325 globalsales@spirent.com | spirent.com/positioning

US Government & Defense: Spirent Federal Systems Inc. 1402 W. State Rd, Pleasant Grove, UT 84062

T: +1 801 785 1448 info@spirentfederal.com | spirentfederal.com



© 2017 Spirent Communications plc. All of the company names and/or brand names and/or product names referred to in this document, in particular the name "Spirent" and its logo device, are either registered trademarks or trademarks pending registration in accordance with relevant national laws. All rights reserved. Specifications subject to change without notice.