The effects of GPS interference and jamming on GNSS timing receivers

Akis Drosinos, Guy Buesnel, Mark Hunter - *Spirent Communications*


SPOOFING
• Covert
• Deception
INTERFERENCE
• Intentional
• Unintentional
GNSS SEGMENT ERRORS
• Erroneous upload data
• SV Faults (e.g. SVN49)
GNSS
Vulnerabilities
MULTIPATH
CYBER ATTACKS
• Non-RF
ATMOSPHERE
• Scintillation
• Solar Activity

Real World Incidents (1)

Photo: RNTF

- **Jan 2021: GPS Jammers Used in 85% of Cargo Truck Thefts**
- Mexican government report that in 85% of 3,400 thefts, GPS jammers were used
- New laws introduced as a result
- Mexico has prohibited not just jamming, but also bans "… manufacture, market, distribute, install, buy, carry, use or operate equipment that hinders or cancels audio, video and data communication signals."
- Stringent penalties: From 12 to 15 years in prison is possible for individuals. Up to 18 years for government officials

Real World Incidents (2)

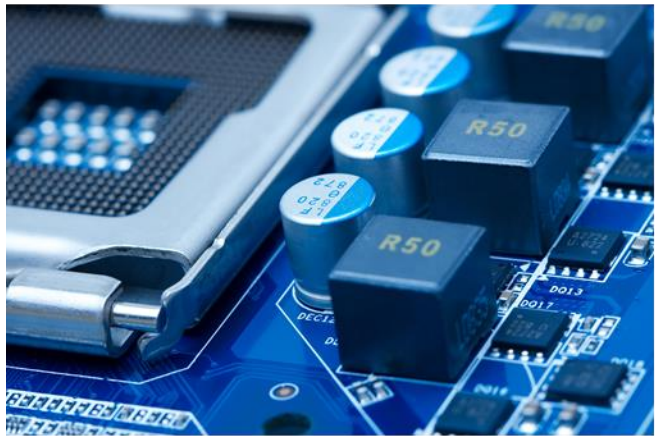


Photo: Stock

- **Feb 2020: “Internet box" jams Galileo GPS signal**
- France's National Frequency Agency (ANFR) responded to a case of interference to Galileo and GPS signals
- An unnamed company had issues receiving Galileo signals and investigated…. Found a pulsed interference, centered on the frequency 1581.15 MHz, which affected GNSS reception
- ANFR used a portable receiver fitted with a directional antenna and traced the interference signals to an “internet box” fitted in an apartment owned by an elderly lady who had no idea that her equipment was causing such problems

Real World Incidents (3)

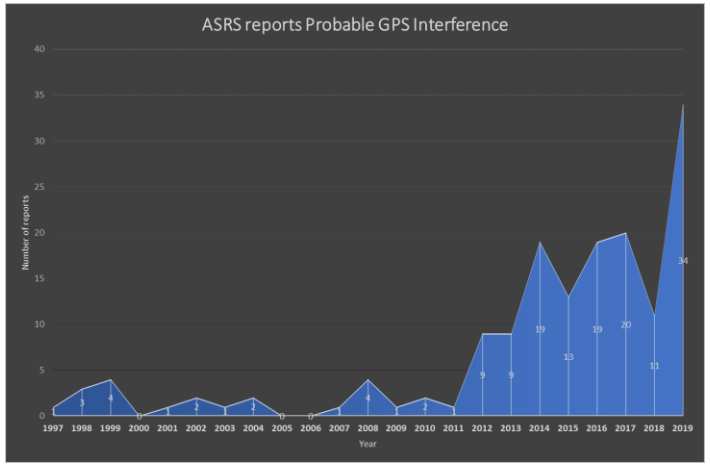


Image: Guy Buesnel

- **Nov 2020: Reports that GPS outages are now “standard occurrences” on commercial flight routes between the US, Europe and the Middle East.**
- Eurocontrol says it received 3,500 reports of GPS disruption during 2019, an all-time high.
- Jamming widespread across the central and Eastern Mediterranean, likely due to electronic warfare between conflicting factions in Syria, Libya and elsewhere in the region
- Update Feb 2021: Previously undisclosed FAA data for a few months in 2017 and 2018 detail hundreds of aircraft losing GPS reception in the vicinity of military tests

Real World Incidents (4)

- **September 2020 – US MARAD Notice extended**

Date of Disruption	Location	Date of Disruption	Location
09/08/2019	Shanghai, PRC	3/7/2019	Dongguan, China
09/02/2019	Shanghai, PRC	11/17/2018	Egypt, Straits of Tiran
09/02/2019	Shanghai, PRC	11/04/2018	Egypt
08/14/2019	Alexandria, Egypt	11/01/2018	Haifa Port, Israel
08/12/2019	El Shaikh Mobarak, Egypt	10/29/2018	Strait of Hormuz
08/06/2019	Mediterranean Sea, South of Sicily	10/13/2018	Jeddah Port, Saudi Arabia
08/01/2019	Mediterranean Sea, East of Malta	10/15/2018	Jeddah Port, Saudi Arabia
06/20/2019	Tripoli, Libya, Malta	10/01/2018	Port Said, Egypt
07/24/2019	Sabratha Oilfield - Offshore Libya	08/11/2018	50 miles from Qingdao, China
07/23/2019	Mediterranean	07/23/2018	Port Said, Egypt
07/16/2019	Shanghai, PRC	07/04/2018	Port Said, Egypt
07/10/2019	Port Said, Egypt	07/04/2018	Port Said, Egypt
07/03/2019	Libya	05/18/2018	100NM off Port Said, Egypt
06/26/2019	Port Said, Egypt	05/18/2018	35 NM North of Egyptian coast
06/20/2019	Sabratha Field - Offshore Libya	05/10/2018	Port Said, Egypt
06/12/2019	Ukraine, South of Odessa	04/18/2018	Eastern Mediterranean Sea
05/20/2019	Port Said, Egypt	04/16/2018	Port Said, Egypt
05/15/2019	Larnaca, Cyprus	03/22/2018	Mediterranean
5/12/2019	Port Said, Egypt	03/21/2018	Port Said, Egypt
05/06/2019	Port Said, Egypt	03/21/2018	Suez
04/27/2019	Damietta, Egypt	03/19/2018	Cyprus
04/25/2019	Port Said, Egypt	03/18/2018	Port Said, Egypt
03/19/2019	Pireaus, Greece	10/24/2017	Sea of Japan
02/09/2019	Hodeidah, Yemen	06/22/2017	Black Sea, Novorossiysk, Russia

Multiple instances of significant GPS interference reported worldwide in the maritime domain.

Images :USTRANSCOM Message to Industry

The threat actors

- Unstructured Hacker
- Structured Hacker
- Organised crime/industrial espionage
- Insider
- Unfunded terrorist group
- Funded terrorist group
- Nation State

(Source: SANS Institute)

Image from Unsplash

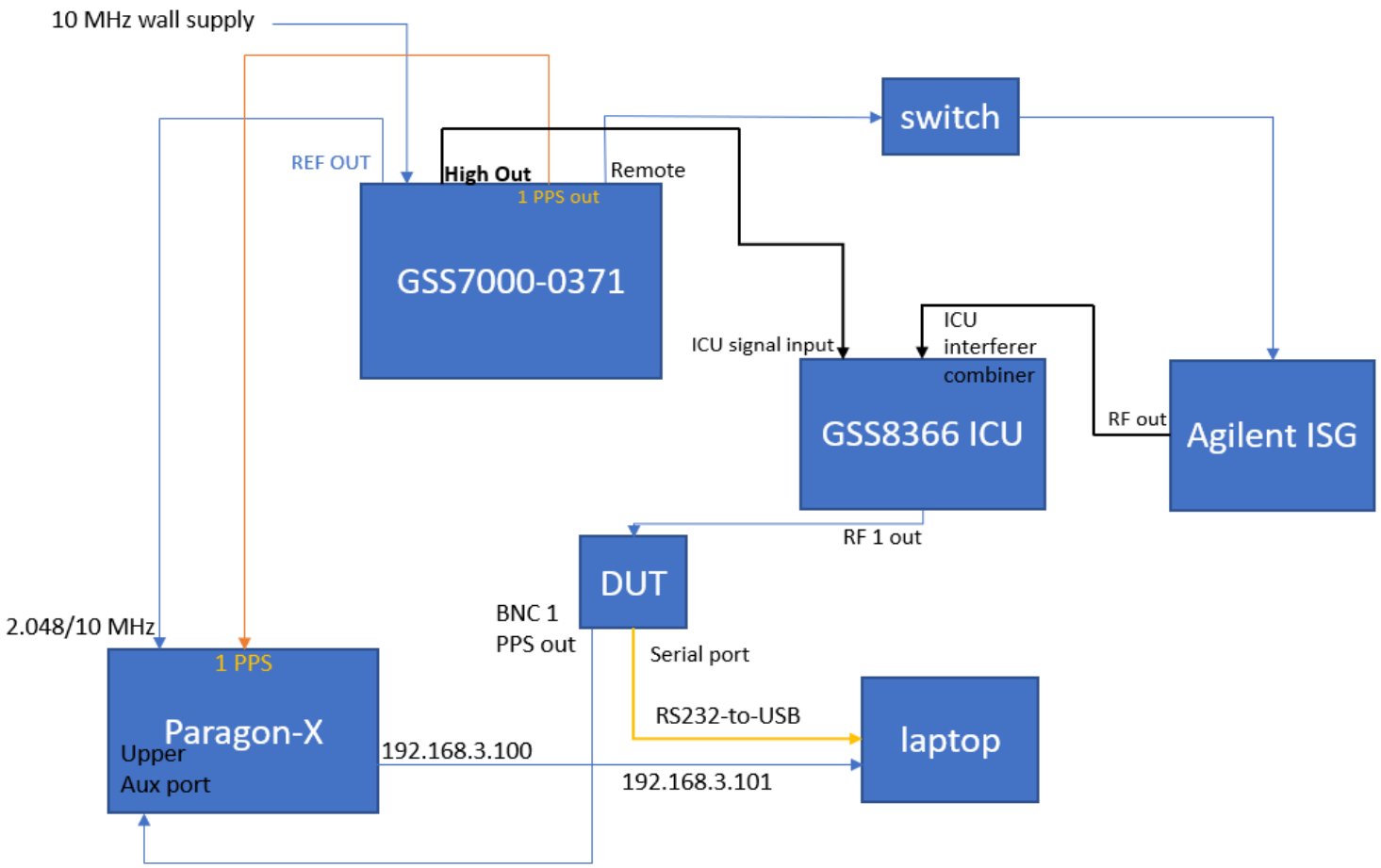
Image from mil.ru

Low

Resources

Very High

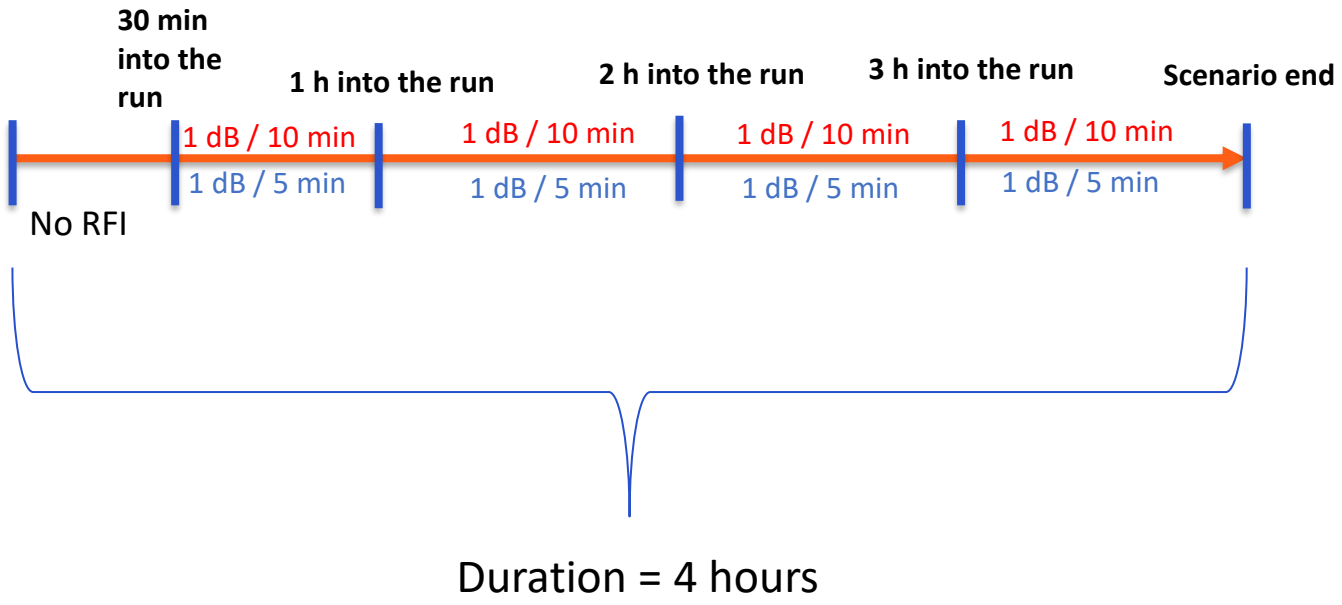
Assessing the impact of GNSS jamming on receivers (1)



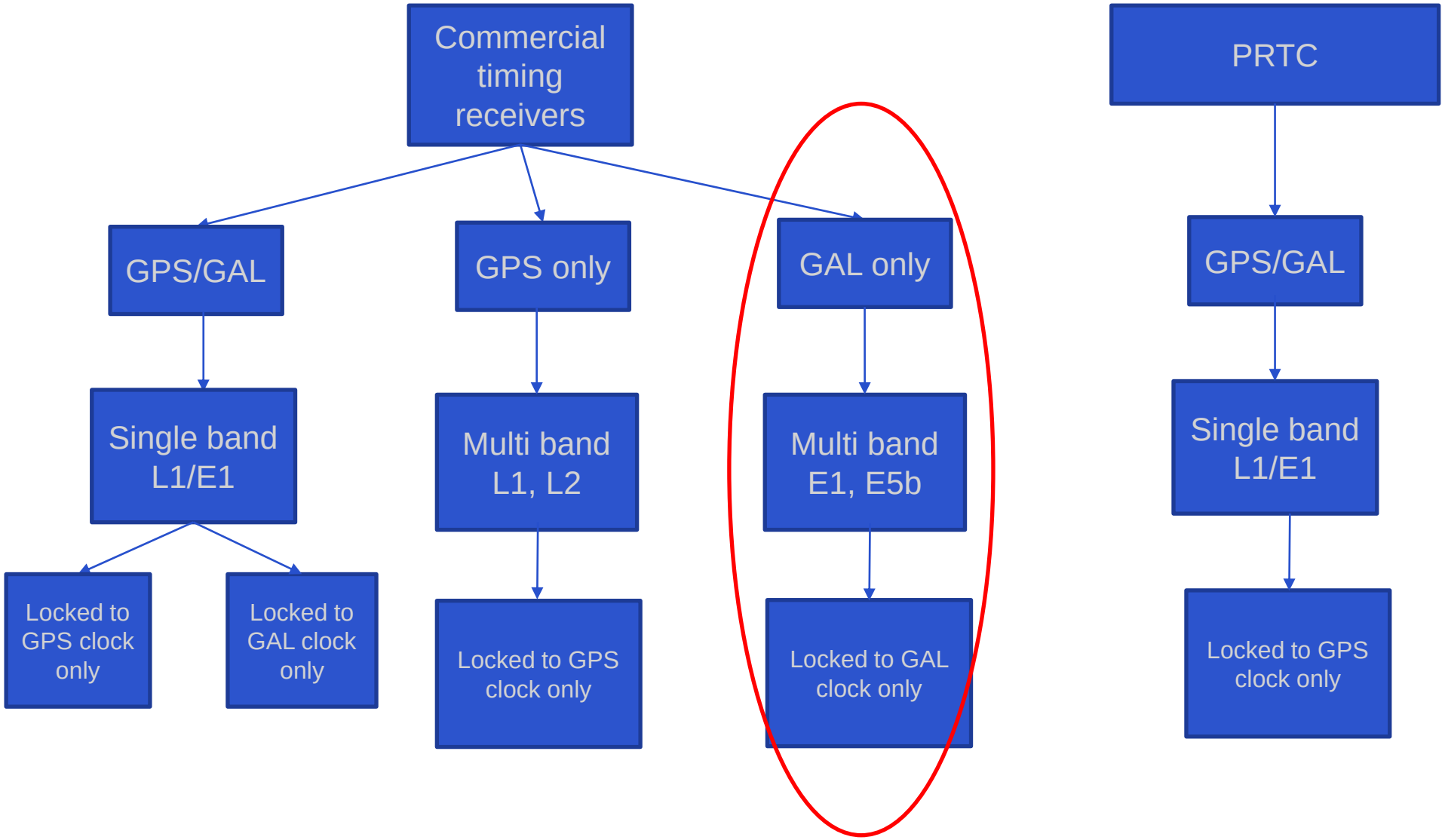
Assessing the impact of GNSS jamming on receivers (2)

Test Parameters (CW Swept jammer)	
Interferer initial RF power level (dBm)	-95
Reference Level (dBm)	-128.5
Start Freq (MHz)	1570.42
Stop Freq (MHz)	1580.42
Number of points	100
Dwell Time (ms)	100

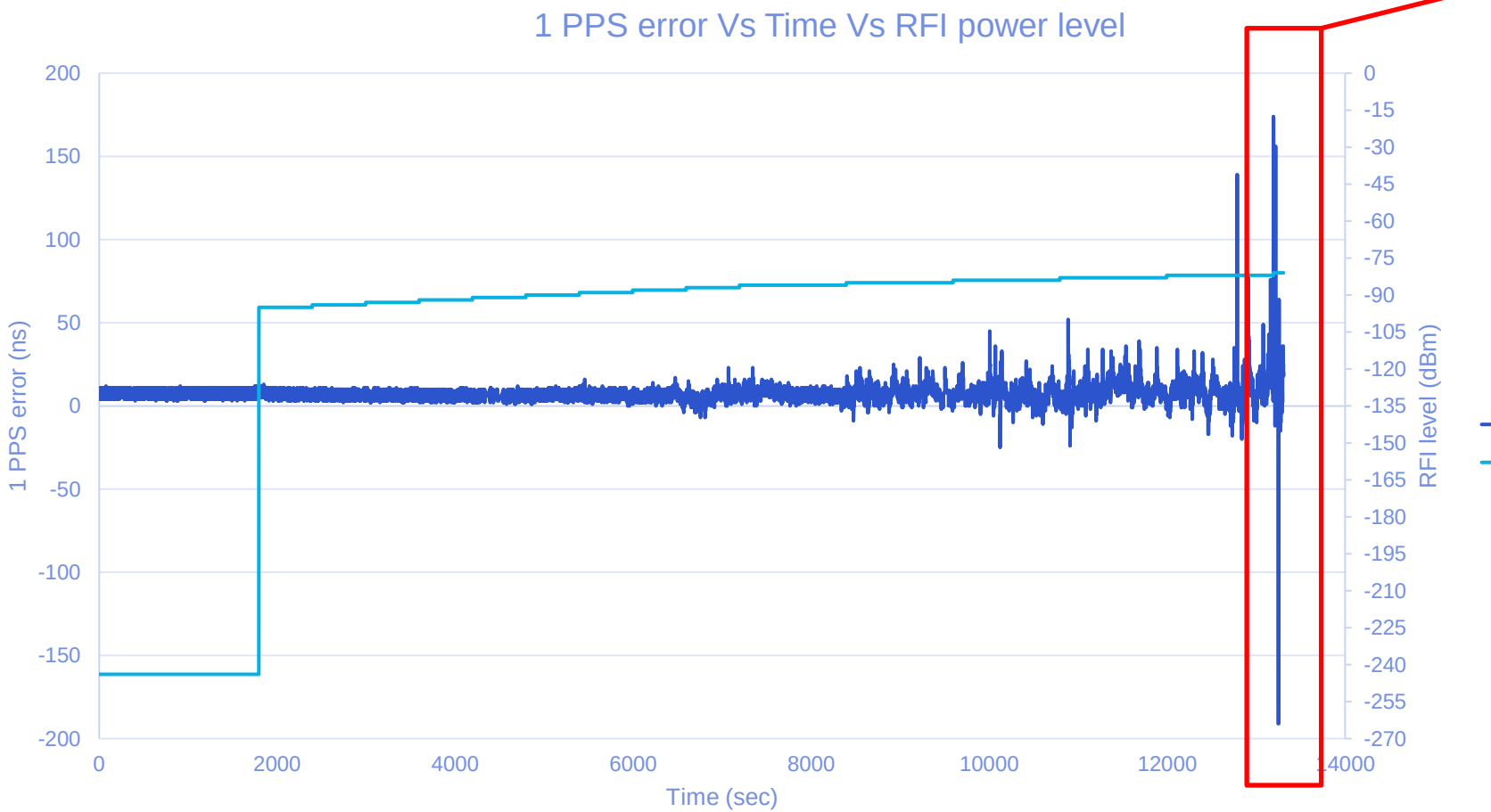
Assessing the impact of GNSS jamming on receivers (3)



Assessing the impact of GNSS jamming on receivers (4)



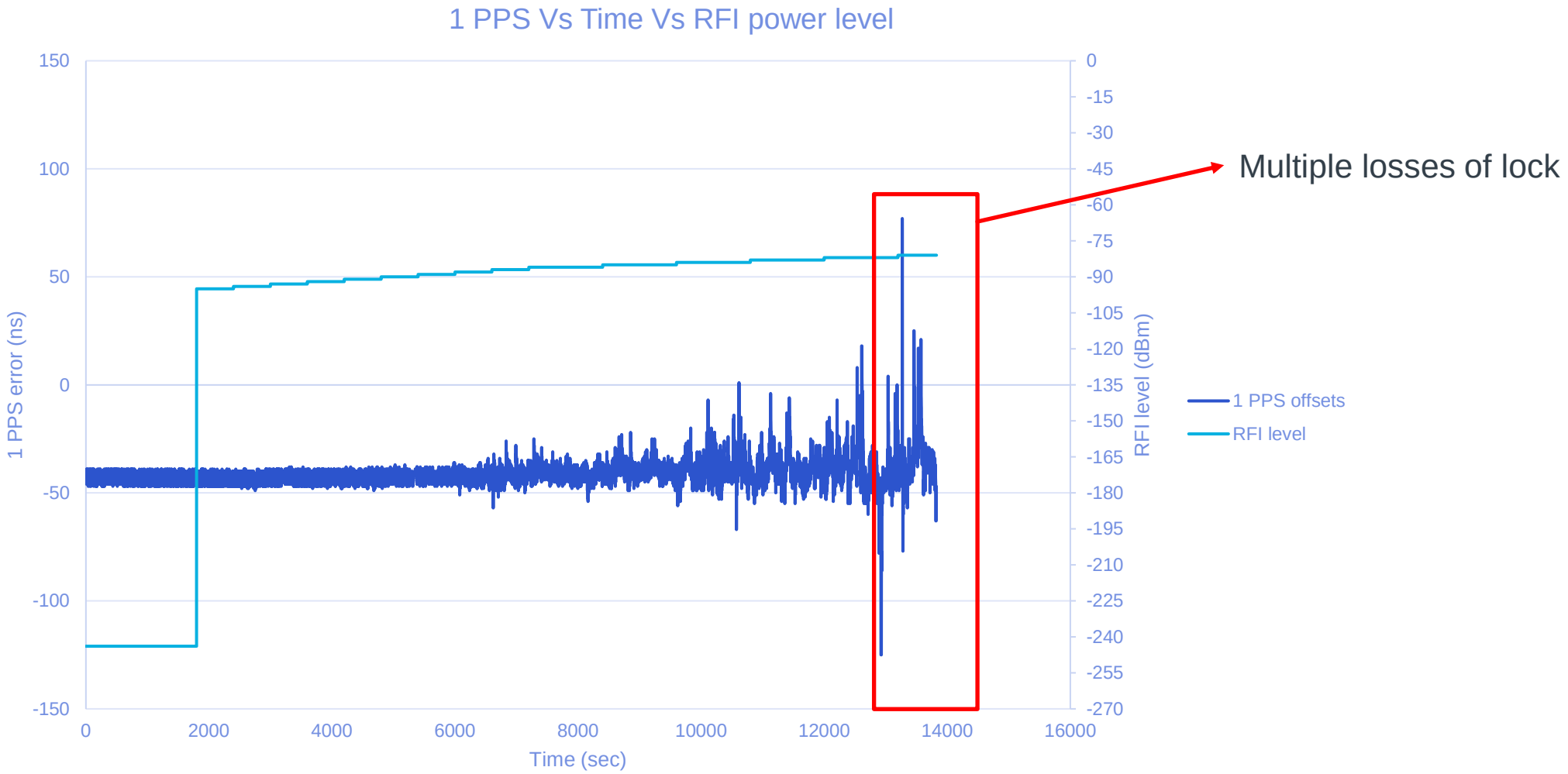
DUT 1 – GPS L1 / GAL E1 – locked to GPS time



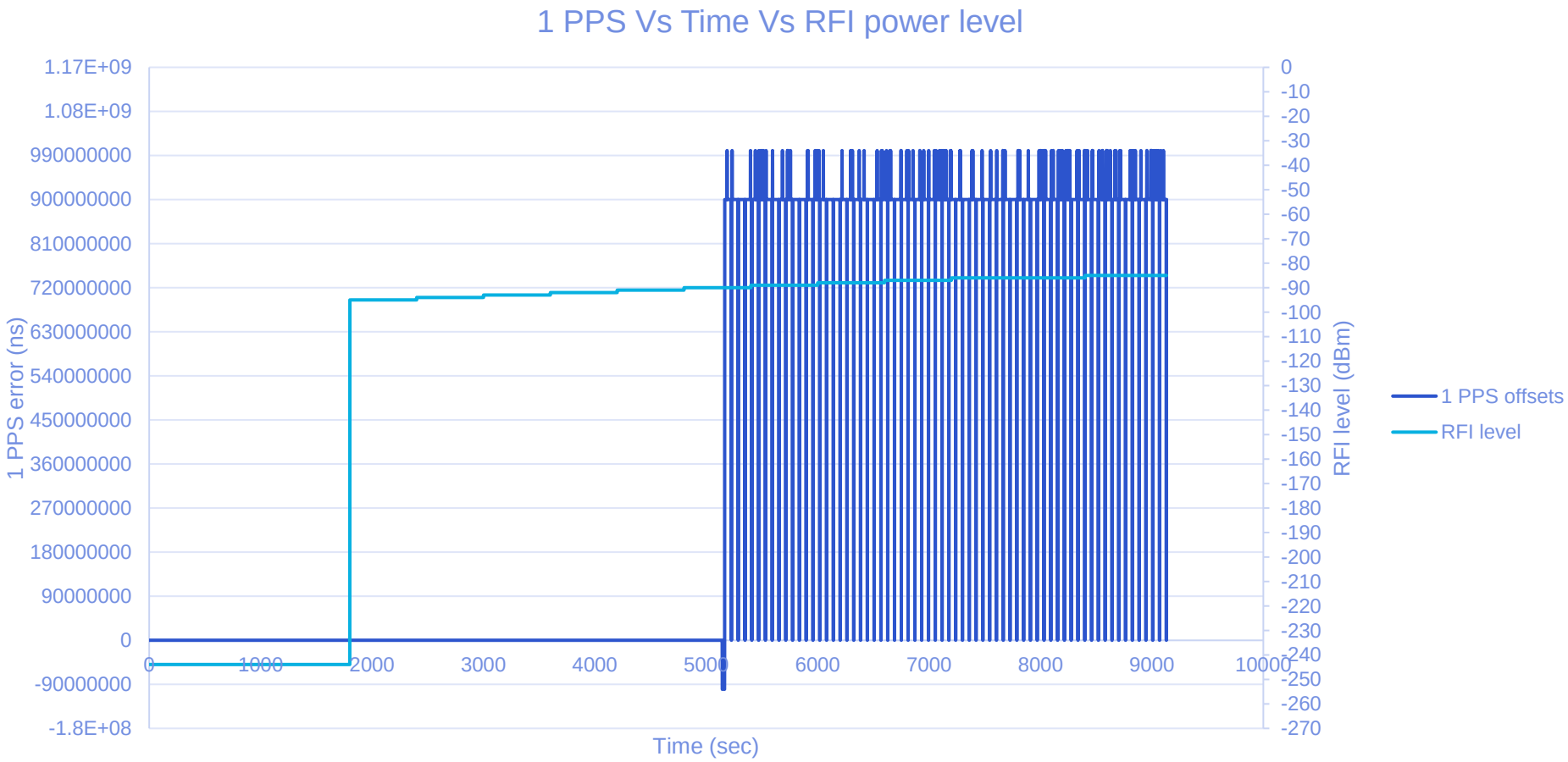
Multiple losses of lock

1 dB / 10 minutes was applied, starting 30 minutes into the run.

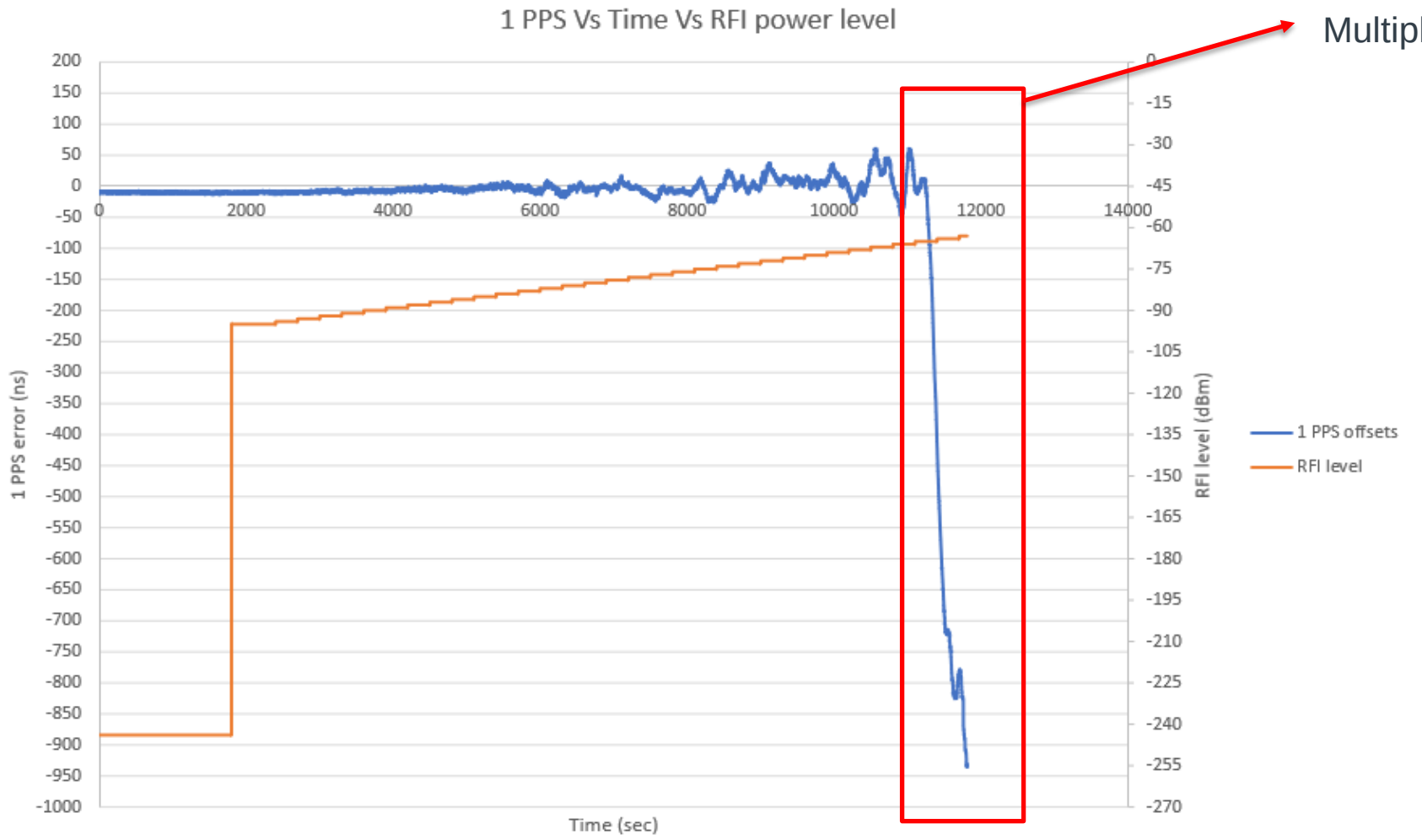
DUT 1 – GPS L1 / GAL E1 – locked to GAL time



DUT 1 – GPS L1 / L2 – locked to GPS time



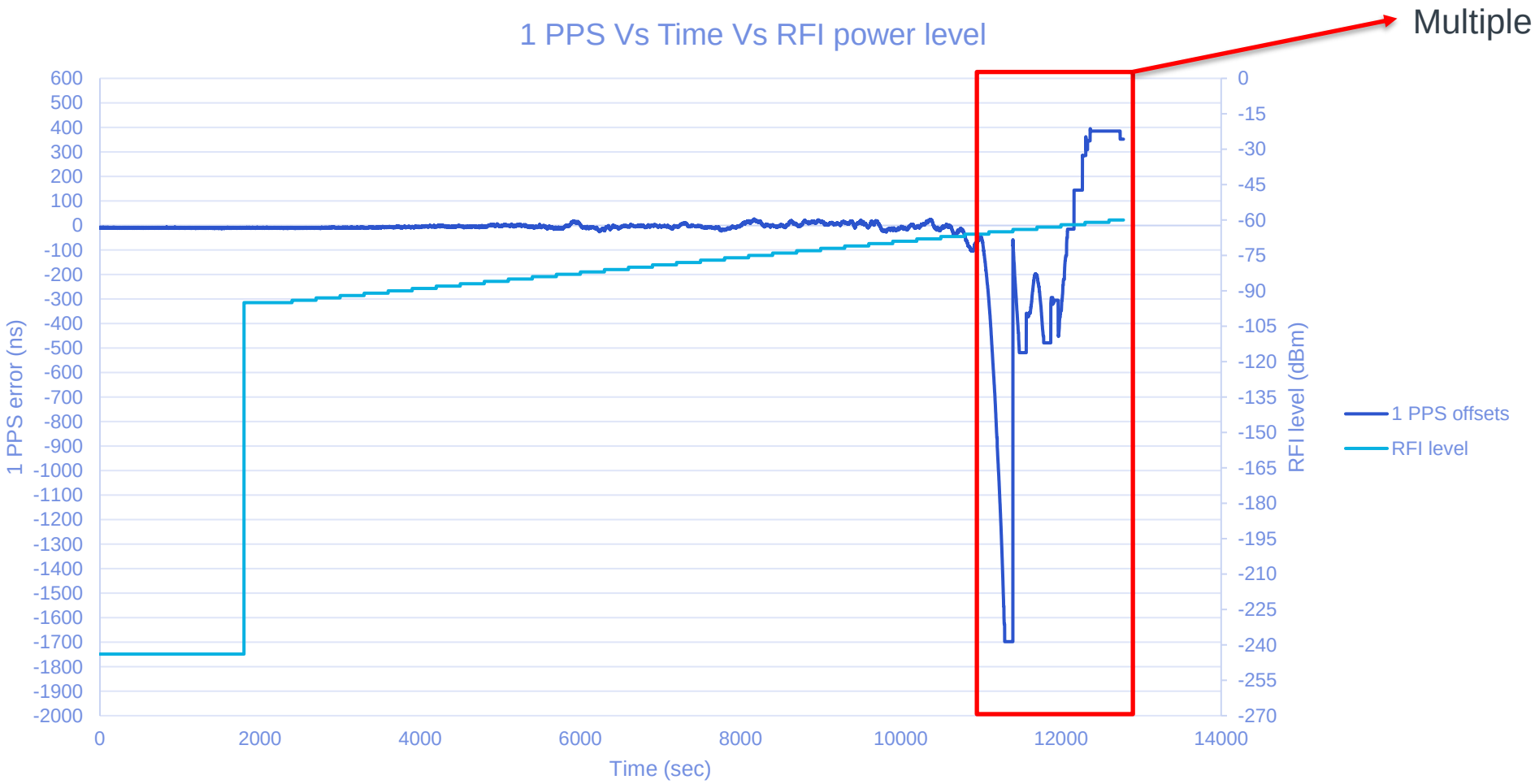
DUT 2 – GPS L1 / GAL E1 – locked to GPS time



Multiple losses of lock

1 dB / 5 minutes was applied, starting 30 minutes into the run.

DUT 2 – GPS L1 / GAL E1 – locked to GAL time



PRTC – GPS L1 / GAL E1 – locked to GPS time

Summary of results

		1 PPS TE (ns)			
		Single Band GPS L1 / GAL E1			Multi Band GPS L1 / L2
		DUT 1	DUT 2	PRTC	DUT 1
Locked to GPS	*Mean*	7.53	-30.81	-19.6	X
	Min	-191	-936	-49	X
	Max	174	61	-2	X
	Max-Min	365	997	47	X
	RFI level (dBm)	-81	-63	-90	-90
Locked to GAL	*Mean*	-40.88	-36.34	X	X
	Min	-125	-1698	X	X
	Max	77	395	X	X
	Max-Min	202	2093	X	X
	RFI level (dBm)	-81	-60	X	X

From real world threats to resilience (1)

Table 1. Minimum requirements for each resilience level.

Level*	Minimum Requirements
Level 1	**Ensures recoverability after removal of the threat.** 1. Must verify that stored data from external inputs adheres to values and formats of established standards. 2. Must support full system recovery by manual means, making all memory clearable or resettable, enabling return to a proper working state, and returning the system to the defined performance after removal of the threat. 3. Must include the ability to securely reload or update firmware.
Level 2	**Provides a solution (possibly with unbounded** degradation) during threat.** Includes capabilities enumerated in Level 1 plus: 4. Must identify compromised PNT sources and prevent them from contributing to erroneous PNT solutions. 5. Must support automatic recovery of individual PNT sources and system, without disrupting system PNT output.
Level 3	**Provides a solution (with bounded degradation) during threat.** Includes capabilities enumerated in Levels 1 and 2 plus: 6. Must ensure that corrupted data from one PNT source cannot corrupt data from another PNT source. 7. Must cross-verify between PNT solutions from all PNT sources.
Level 4	**Provides a solution without degradation during threat.** Includes capabilities enumerated in Levels 1, 2 and 3 plus: 8. Must have diversity of PNT source technology to mitigate common mode threats.
Note	* **Level 0** indicates a source or system that does not meet the criteria in Level 1, and thus is considered a non-resilient system or source.

- **DHS Science and Technology report defines 5 resilience levels for US**

- May not be defined same way for UK but illustrates the challenge
  - How to prove equipment complies with the minimum requirements in each level?
  - Does the equipment/system need to meet the same level for each type of threat or can it be e.g. level 4 for jamming and level 2 for spoofing?
  - What test methodologies are likely to help map real world threats to lab based verification/test activities?

Spirent Insights

- Real world jamming incidents that result in disruption to GNSS are on the rise
  - Incidental/accidental more likely than being deliberately targeted
  - Live sky jamming trials/exercises can cause problems

- Total dependence on GNSS for precision timing isn’t adequate for safety or liability critical applications – Responsible use of PNT requires a resilient system

Trust but Verify

akis.drosinos@spirent.com@spirent.com

www.spirent.com/products/pnt-vulnerability-test-solutions

Join the GNSS Vulnerabilities group on LinkedIn to find out more about GNSS jamming and spoofing

Questions?