OS Position, Navigation and Timing (PNT):

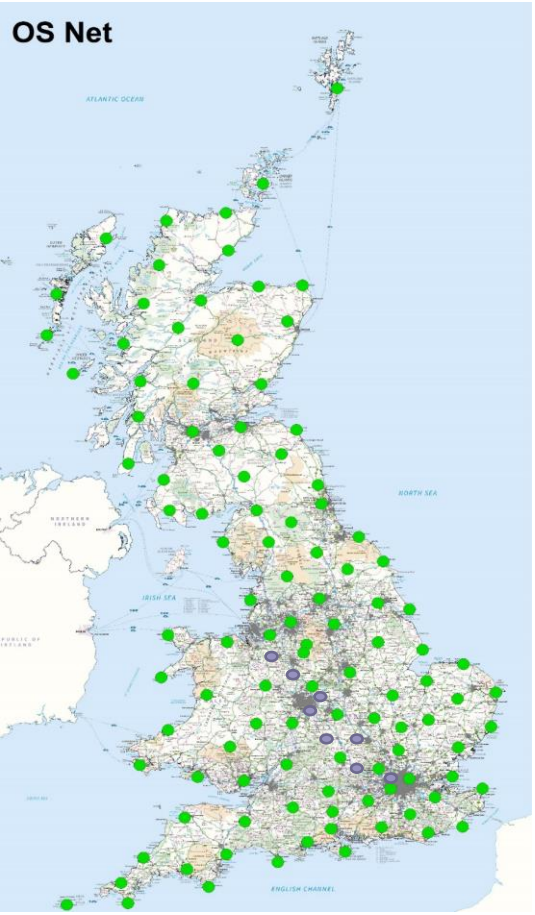
Stephen Hancock

Principal Scientist

Nov 2021

OS and GNSS

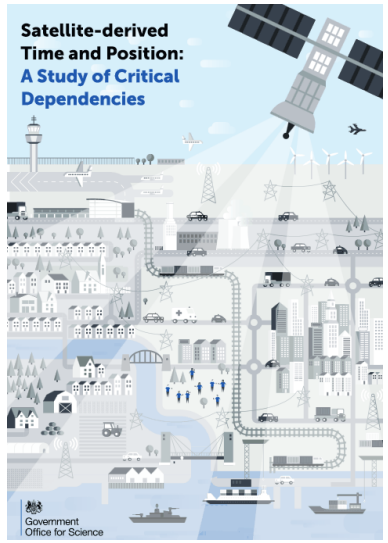
As a society, we rely upon satellite navigation systems and services for delivery wide range time and position applications that are often hidden from view. Alternative PNT systems exist, but for the majority of users, they cannot compete on price or convenience.



Replacing triangulation pillars, for over 15 years OS has operated a network of 115 continuously operating GNSS receivers throughout Great Britain.

OS Net also provides correction and data services enabling real time 2cm GNSS positioning for multiple industries, including:

- Mapping and aerial survey
- Construction
- Ports
- Police
- Meteorological Office
- Agriculture
- Drone users
- Autonomous vehicles
- Geodesy
- Academia



OS is critically reliant upon GNSS and is very good at using and supplying GNSS based data.

OS recognises the need for resilient PNT, and has programmes to understand and develop solutions.

GNSS: Global Navigation Satellite Systems, includes GPS, Galileo, GLONASS and Beidou

GNSS Threats and Vulnerabilities

GNSS is subject to a wide variety of threats and vulnerabilities. For example constellation failures, space weather and radio interference. This aspect is constantly evolving as demands on digital technology grows.

However, disruption can and DOES occur through multiple causes:

Global satellite navigation constellations broadcast very weak signals (60W light bulb from space), this makes disruption easy to achieve.

Space weather causes continuous errors (that we mitigate against by OS Net), but on a bad day can disrupt any radio signal and/or damage satellites, even damaging power networks and telecom links

£60
~5m range

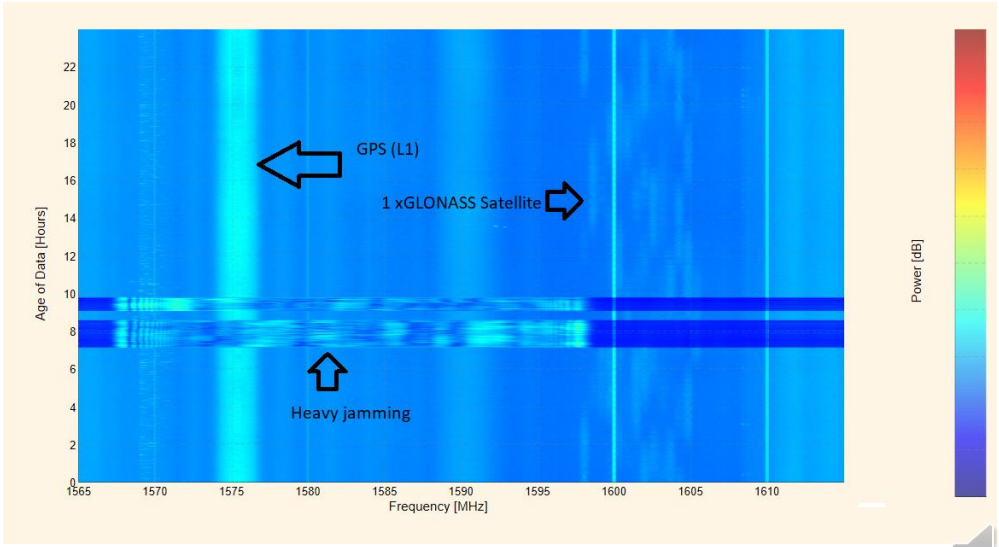
£500
~40km range

Criminal activity is diverse, but aims to disrupt GNSS and other radio based services across the nation. Used by those trying to deny fleet tracking (e.g. for moonlighting) to more serious organised crime (e.g. vehicle theft)

Intentional and non-intentional interference are the biggest and most consistent threats to GNSS. Non-intentional systems often include faulty or incorrectly configured equipment, whilst intentional includes: state actors (MoD conduct regular GPS jamming exercises), criminal actions and hackers.

Cyber threats have only been recently acknowledged by the PNT community. But connected devices have created new attack and vulnerability opportunities.

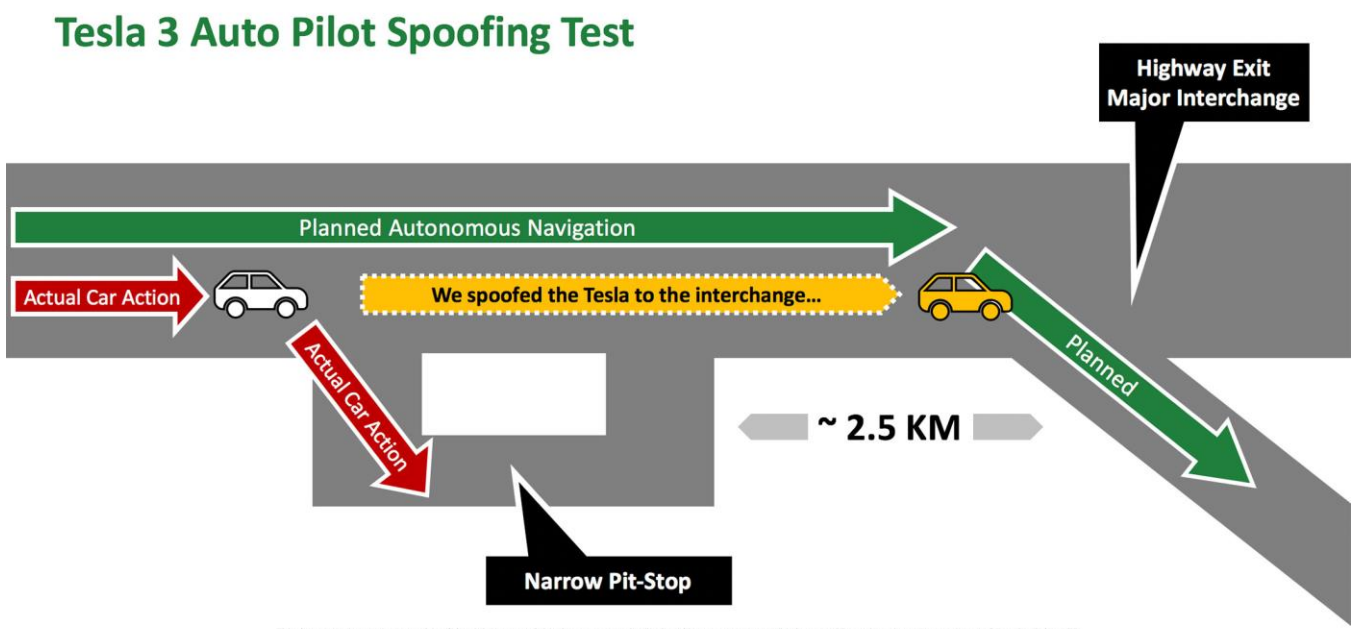
Constellation and other system failures occur from human error and/or system failures due to other causes.



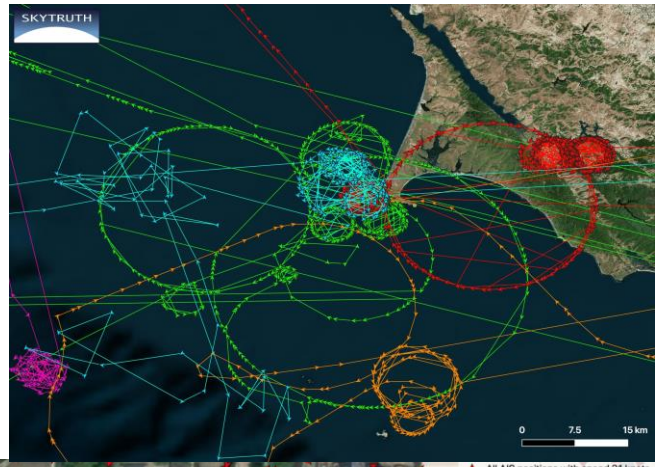
GNSS: Global Navigation Satellite Systems, includes GPS, Galileo, GLONASS and Beidou

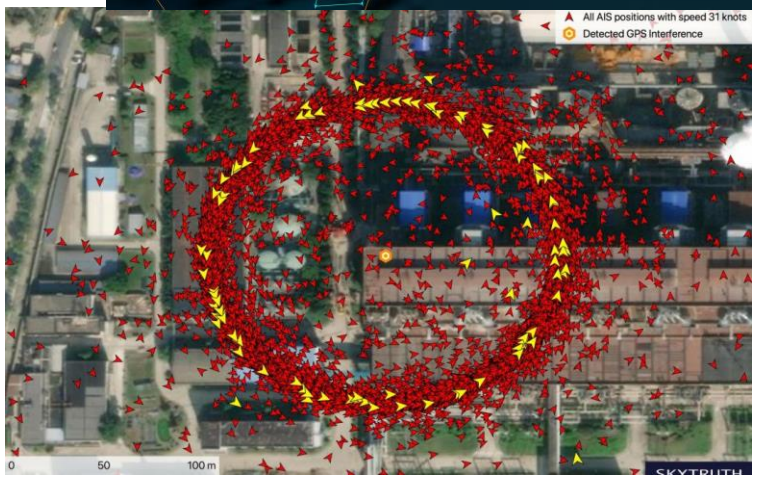
GNSS Spoofing

Real GNSS Spoofing Attack – Tesla Model 3 with "Navigate on Auto Pilot" mode



Courtesy: Regulus.com





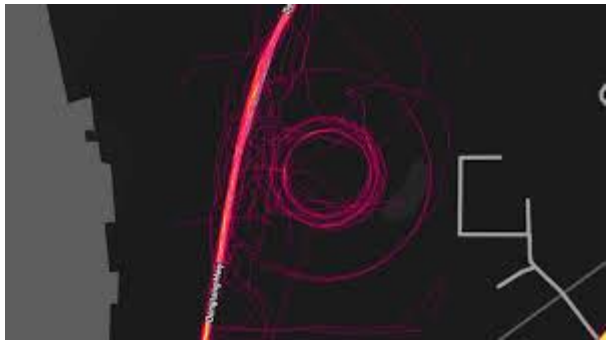
Courtesy: Skytruth.org

Multiple live demonstrations of position spoofing for a Tesla 3…..

Using:

Jammer – ADALAM PLUTO configurable SDR manufactured by Analog Devices ($150).

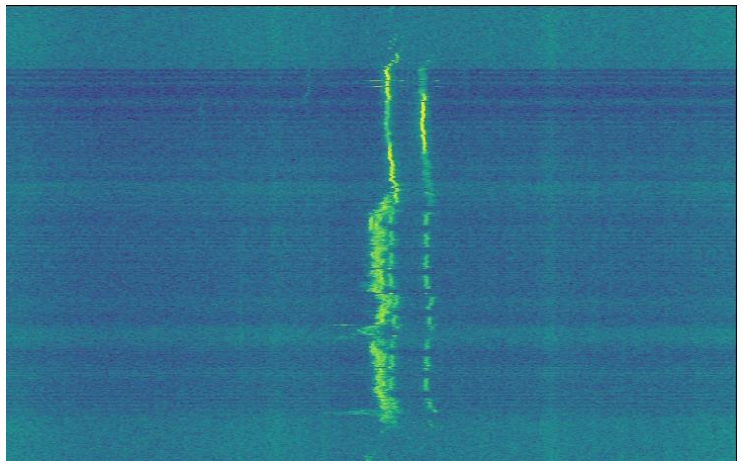
Spoofing device – Blade RF SDR manufactured by Nuand ($400) with external PPS sync connected to a laptop

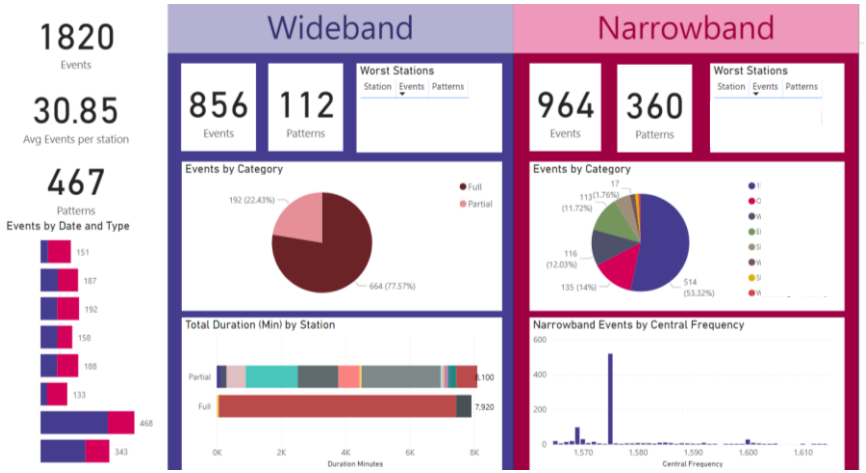


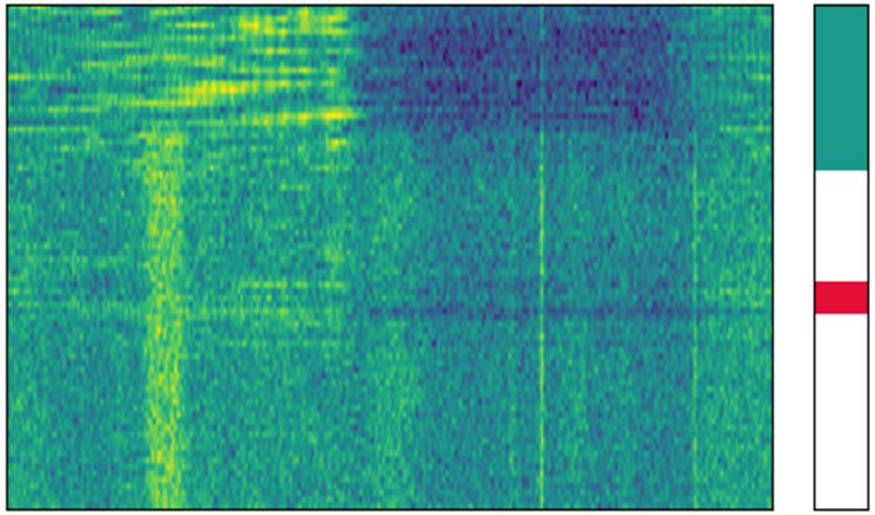
Courtesy: Strava.com

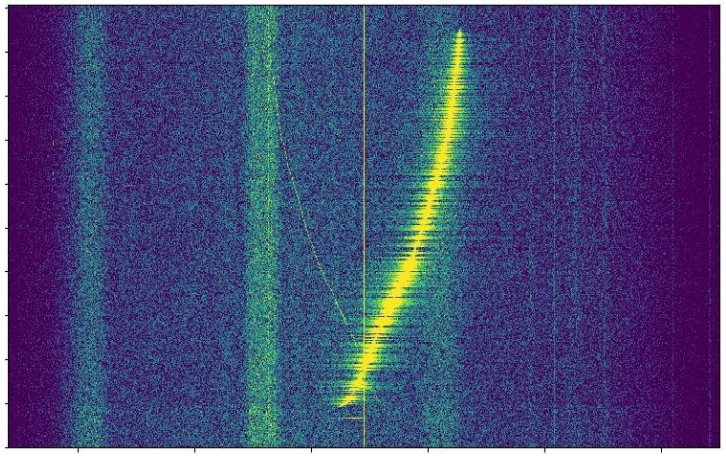
Ordnance Survey

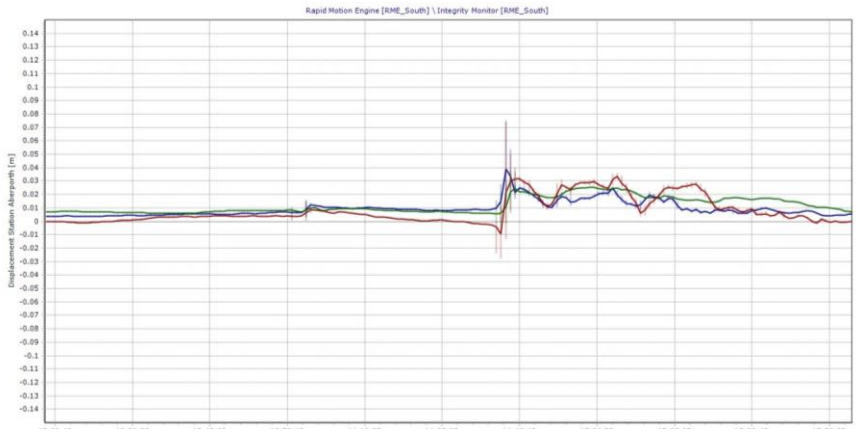
What we see









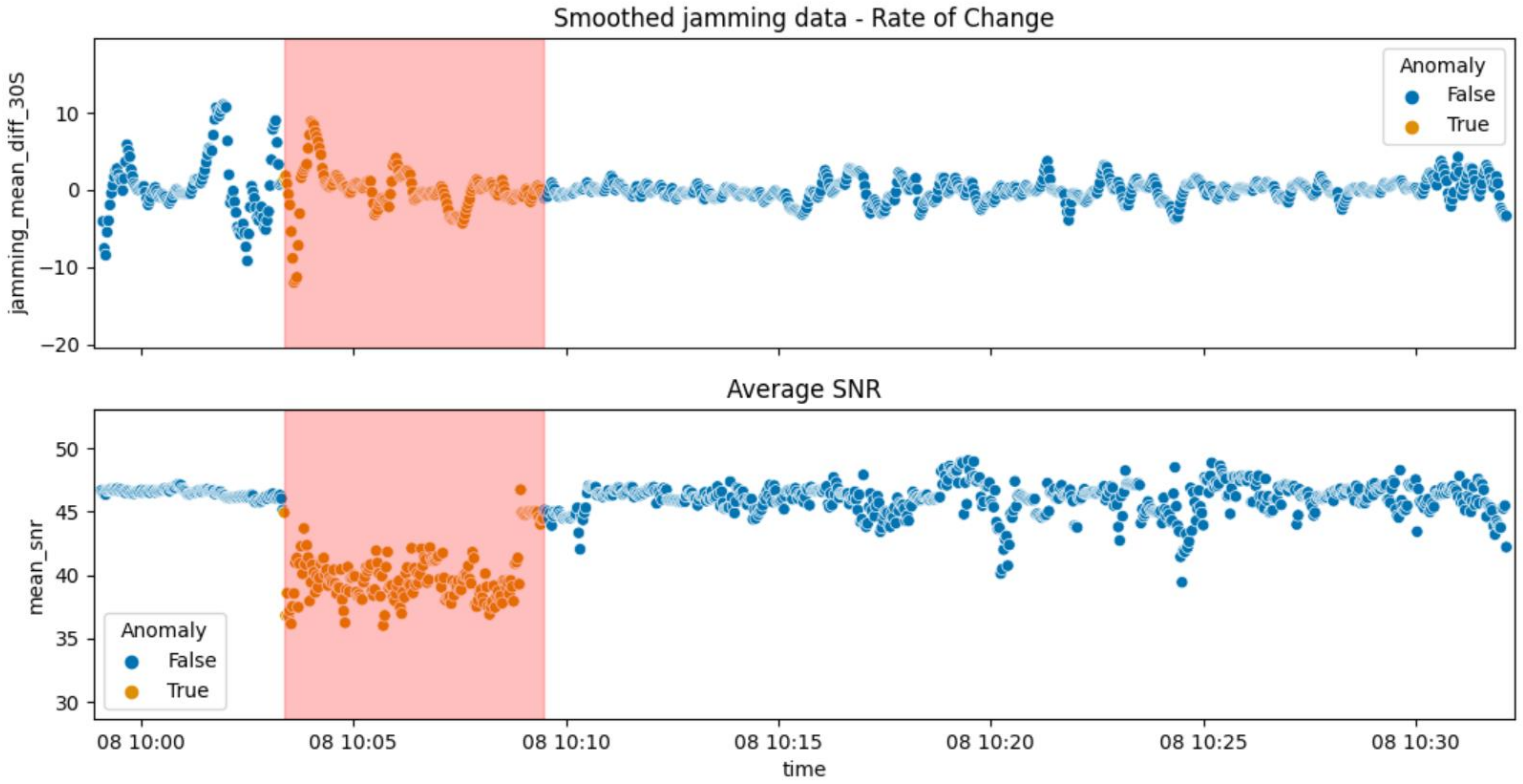


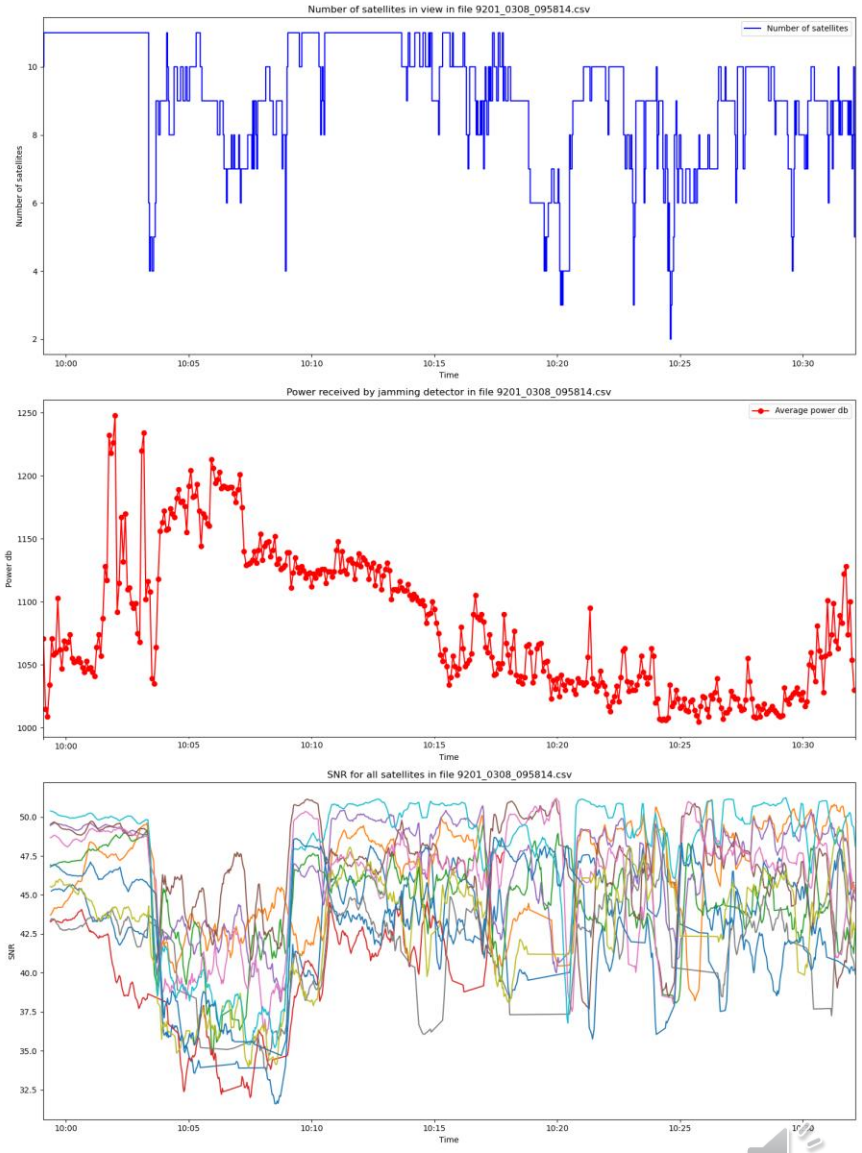
Copy to clipboard | Save as CSV | Search:

Start	Duration	Band	Signatures	
2020-12-03 21:52:45.476	9.874	L1		View Event
2020-12-03 21:52:20.304	11.524	L1		View Event
2020-12-03 21:51:55.869	13.579	L1		View Event
2020-12-03 21:45:53.895	29.897	L1		View Event
2020-12-03 21:27:30.596	7.219	L1		View Event
2020-12-03 20:51:33.612	3.528	L1		View Event
2020-12-03 20:48:29.817	2.249	L1		View Event

Results from surveyors data and ML processing to identify anomalies

- An event that the anomaly detector found (data from one OS surveyor), shows an SNR drop (bottom) combined with a rapid increase in the jamming detector signal (top)





Ordnance Survey

Other PNT

OS recognises society's growing dependence upon GNSS in addition to its own use of GNSS systems and services, consequently we are involved across multiple programmes, including:

Current hot topics and activities:

ESA NAVISP Element 3:

https://navisp.esa.int/project/details/116/show

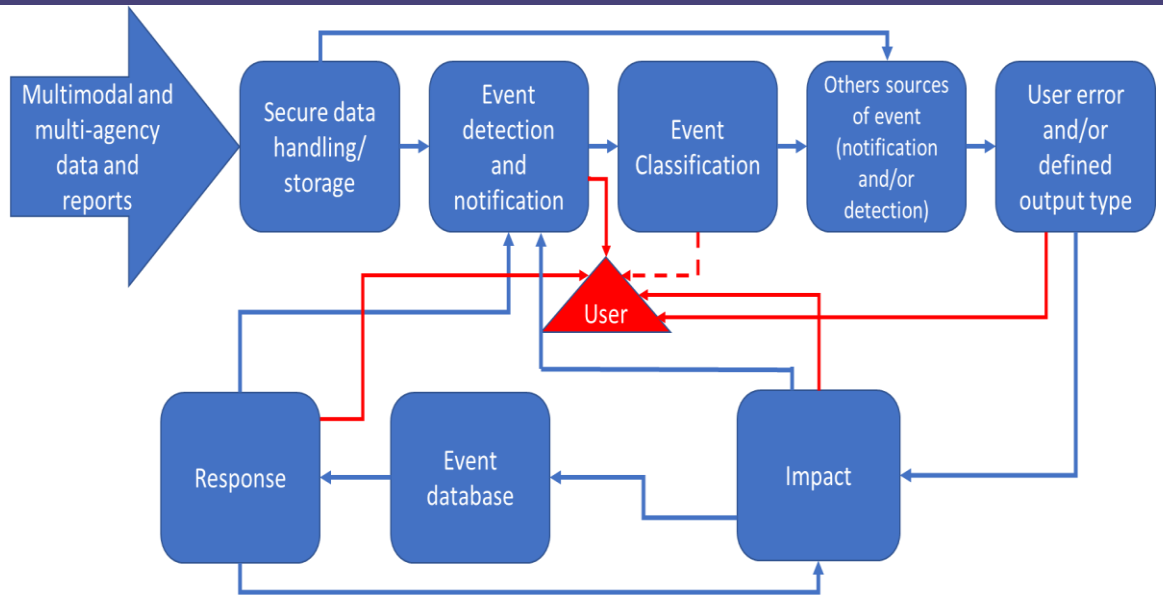
Led by CGI UK; The GNSS Event Notification Service (GENS) project's aim is to create an initial national demonstration capability for GNSS event notification that is robust, secure and aligned to the UK national interest. In addition, GENS is planned to act as a catalyst to create a national centre for GNSS service threat identification and response.

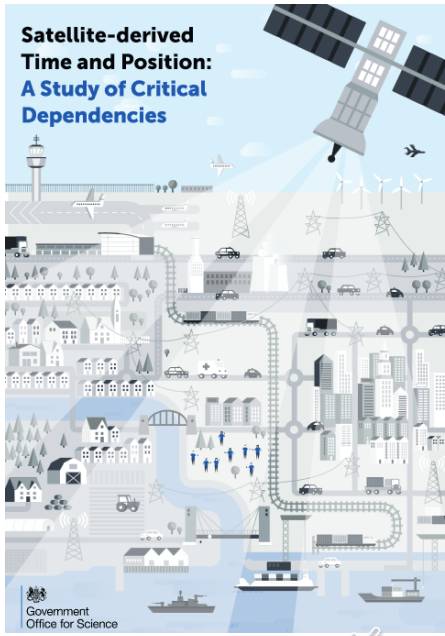
HM Government

CGI

gmv NSL

NPL National Physical Laboratory





Ordnance Survey

Thank you

Stephen Hancock
Principal Scientist (GNSS)

www.os.uk

stephen.hancock@os.uk

M: +44 (0) 7880 091710

Ordnance Survey