題名　ISWI Newsletter - Vol. 3 No. 35
差出人　George Maeda

****
* ISWI Newsletter - Vol. 3 No. 35 31 March 2011 *
*
* I S W I = International Space Weather Initiative *
* (www.iswi-secretariat.org) *
*
* Publisher: Professor K. Yumoto, SERC, Kyushu University, Japan *
* Editor-in-Chief: Mr. George Maeda, SERC (maeda[at]serc.kyushu-u.ac.jp)*
* Archive location: www.iswi-secretariat.org (maintained by Bulgaria) *
* [click on "Publication" tab, then on "Newsletter Archive"] *
* Caveat: Under the Ground Rules of ISWI, if you use any material from *
* the ISWI Newsletter or Website, however minor it may seem *
* to you, you must give proper credit to the original source. *
****

Attachment(s):
(1) "RAoE_Global_Navigation_Systems_Report", 1.05 MB pdf, 48 pages.

: Re:
: Vulnerabilitiy of
: Global Navigation Space Systems
: to hazards in space.

Dear ISWI Participant:

The following note (between + and &) was received by myself
from Dr Hans Haubold of the UNOOSA in Vienna, Austria.
You can access the attached pdf by clicking the indicated
link inside of this email message. This link is alive for only
a few weeks. But all "ISWI Newsletters" are archived at the ISWI
website (www.iswi-secretariat.org) for easy access.

+
%%%
Dear George,
Among the IHY/ISWI instrument arrays, we have GPS-Africa, SCINDA,
and CIDR which are doing very important research work with the GPS
signal for monitoring solar activity impacts on the ionosphere.
Other IHY/ISWI instrument arrays, among them MAGDAS, are utilizing
GPS for pnt (positioning, navigation, timing). Having said this we
know that Global Navigation Satellite Systems (GNSS) are themselves
exposed to adverse impacts of solar activity.

The attached report of the Royal Academy of Engineering (London, UK),
titled Global Navigation Space Systems: reliance and vulnerabilities,
refers in detail to GNSS and space weather and this report might
be of interest to readers of the ISWI Newsletter.

We also note with appreciation that the Committee on Global Navigation
Satellite Systems (ICG) co-organizes and co-sponsors the
ISWI workshops 2010-2012.

Thank you, Hans

(See attached file: RAoE_Global_Navigation_Systems_Report.pdf)

%%%
&

Mit freundlichen Grusen,

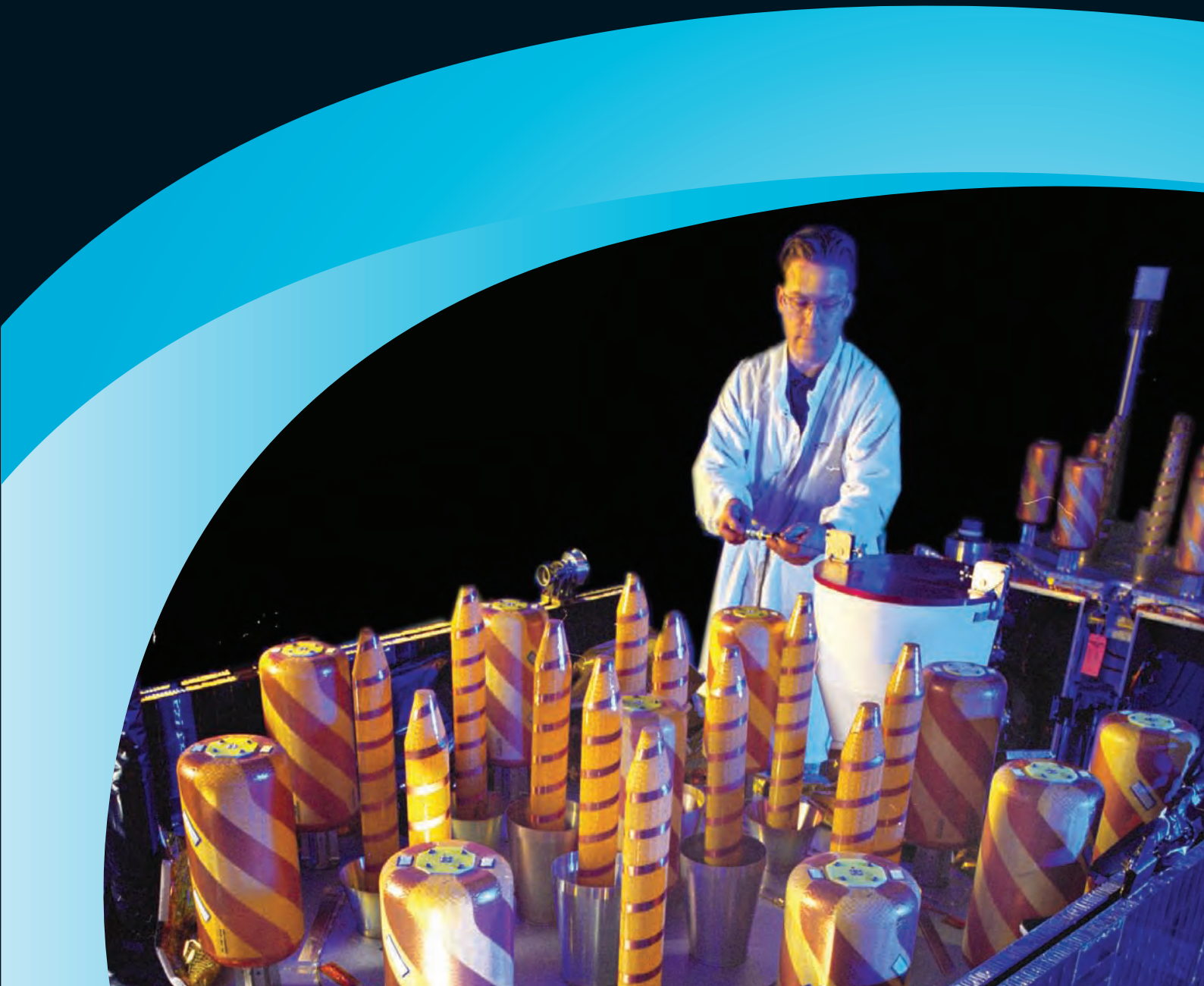
: George Maeda
: The Editor
: ISWI Newsletter

The Royal Academy of Engineering

Published by SERC of Kyushu University
I S W I Newsletter
under the auspices of the United Nations

This pdf circulated in Volume 3, Number 35 on 31 March 2011.

Global Navigation Space Systems: reliance and vulnerabilities



The Royal Academy of Engineering

Global Navigation Space Systems:
reliance and vulnerabilities

ISBN 1-903496-62-4

March 2011
Published by
The Royal Academy of Engineering
3 Carlton House Terrace
London SW1Y 5DG

Tel: 020 7766 0600 Fax: 020 7930 1549
www.raeng.org.uk
Registered Charity Number: 293074

Cover: A Lockheed Martin engineer checks out a GPS IIR spacecraft (courtesy of Lockheed Martin)

A copy of this report is available online at www.raeng.org.uk/gnss

Contents

Foreword 3

Executive summary 5

1 Introduction 8

2 GNNS overview 10

3 The range of applications 13
- 3.1 Some critical applications of GNSS 14
- 3.2 System-level criticalities 14

4 Vulnerabilities of GNSS services 15
- 4.1 System vulnerabilities 15
- 4.2 Propagation channel vulnerabilities 18
- 4.3 Accidental interference 19
- 4.4 Deliberate interference 20

5 Resilience to disruption of GNSS services 22
- 5.1 Position and navigation 22
- 5.2 Timing 22
- 5.3 Vulnerability mitigation 23

6 Conclusions and recommendations 26
- 6.1 Reliance on GNSS for PNT is high and increasing 26
- 6.2 GPS, Galileo, Compass and GLONASS common vulnerabilities 26
- 6.3 Recommendations 27

References 29

Glossary 30

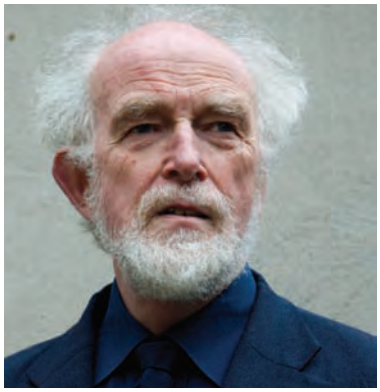
Annex A – Current and planned PNT applications using GNSS 31

Annex B – GNSS failure modes and characteristics 36

Annex C – Some commercial jammers 39

Annex D – Jamming trial example 40

Annex E – Acknowledgements 45



Dr Martyn Thomas CBE FREng

Foreword

As technologies become easier to use and more cost effective their use can become almost ubiquitous. If they present a more convenient solution to an old problem, they can usurp older technologies very quickly, forcing obsolescence on otherwise excellent technologies and taking a dominant position. The use of Global Navigation Satellite Systems (GNSS) for deriving position, navigation and timing (PNT) data is such a case. The Global Positioning System (GPS) is currently the most widely used and best known example of GNSS.

Today, the relative ease of use of GPS in-car navigation systems means that many motorists rely entirely on GPS for navigation and if they have a road map as a back-up, it is not likely to have been used or updated in a long time. This is a trivial example of reliance on GPS with neglect of back-up systems, but the use of GPS signals is now commonplace in data networks, financial systems, shipping and air transport systems, agriculture, railways and emergency services. Safety of life applications are becoming more common. One consequence is that a surprising number of different systems already have GPS as a shared dependency, so a failure of the GPS signal could cause the simultaneous failure of many services that are probably expected to be independent of each other.

The European Commission has estimated that, already, 6-7% of GDP in Western countries, that is to say €800 billion in the European Union, is already dependent on satellite radio navigation, so this study into our reliance on GNSS and potential vulnerabilities is both important and timely. Such widespread use of GNSS derived data within our economies means that the secure provision of PNT data is now a matter of national security as well as a major economic asset.

Dr Martyn Thomas CBE FREng
Study Chairman

The Soyuz-Fregat launch vehicle carrying GIOVE-B on launch pad, 2008

Executive summary

In an ever more connected world, society's reliance on high integrity positional, navigational and timing (PNT) data is growing. The easy and cheap availability of Global Positioning System (GPS) and other global navigation satellite systems (GNSS) has meant that their use as primary sources of data can be found in an increasing number of products and services. The range of applications stretch from highly accurate surveying to in-car navigation, and from network synchronisation to climate research.

The Academy's study has identified an increasing number of applications where PNT signals from GNSS are used with little, or no, non-GNSS based back-ups available. The trend is for GNSS to be used in a growing number of safety of life critical systems. Unfortunately, the integrity of GNSS is insufficient for these applications without augmentation (see below). Non-GNSS based back-ups are often absent, inadequately exercised or inadequately maintained.

The original implementation of GNSS, the US operated GPS comprises ground based, space based and receiver segments, all of which are susceptible to failures of various types. There are also some common mode failure mechanisms which can affect whole classes of receiver or even the entire satellite constellation.

A failure, or loss of signal due to some outside influence, can result in a range of consequences depending on the application; in a telecommunications network, a small loss in the efficiency of data handling may occur while the system 'freewheels' until a signal is restored: in a surveying application where timing is not critical, some delays may occur before the survey can be properly completed. In such applications, a temporary loss of GNSS signals might be considered an inconvenience. However, where systems are used in safety of life critical applications, the consequences can be more severe – in some situations, even if operators are well versed in procedures for a loss of GNSS signals, the number of interlinked systems simultaneously activating alarms can lead to eroded situational awareness of operators in what could well be an emergency situation.

Some systems which rely on PNT signals from GNSS are robust in themselves and procedures are in place to deal adequately with any GNSS based system faults that occur. However, disruptive interference can occur unintentionally and, worse still, deliberate interference is a real and growing possibility. As opportunities arise for criminals to make money, avoid costs or avoid detection, it is known that significant effort will be directed towards attacking GNSS based systems. The banking infrastructure has already seen such an increase in high-tech attacks and now devotes considerable time and expense to countermeasures.

Potential and already known mechanisms for deliberate interference include:

- Jamming GNSS based vehicle tracking devices to prevent a supervisor's knowledge of a driver's movements, or avoiding road user charging.
- Rebroadcasting ('meaconing') a GNSS signal maliciously, accidentally or to improve reception but causing misreporting of a position.
- Spoofing GNSS signals to create a controllable misreporting of position, for example to deceive tracking devices.

As the use of GNSS for revenue raising purposes increases through road user charging or vehicle tracking, the prevalence of cheap jamming devices will increase. Because the signal received at ground level from the GNSS satellites is weak – it may be as low as -160dBW (1×10^{-16}W) – jamming over a small area is

easily achieved and it is known that dedicated kit is already readily available for purchase over the internet even though use of that equipment in the UK is illegal. In the United States, monitoring for GPS signal anomalies is routine and the occurrence of jamming incidents, both deliberate and accidental is growing. In the UK, the Technology Strategy Board is supporting a project to establish a service to verify the extent to which GNSS signals can be trusted by users.

We have therefore made a number of recommendations with the aims of (a) raising awareness of the nature and magnitude of the issues; (b) proposing some policy interventions that could reduce the risks; and (c) increasing the resilience of services that rely on GNSS.

Recommendations

a) Raising awareness and analysing impact

1. Critical services should ensure that GNSS vulnerabilities are included in their risk registers and that the risks are reviewed regularly and mitigated effectively.

2. National and regional emergency management and response teams should review the dependencies (direct and indirect) on GNSS and mitigate the risks appropriately.

3. Services that depend on GNSS for PNT, directly or indirectly, should document this as part of their service descriptions, and explain their contingency plans for GNSS outages (say, of duration 10 minutes, 2 hours, 5 days, 1 month)

b) Policy responses

4. It is already illegal to place GNSS jamming equipment on the market in the EU, as it cannot be made compliant with the EMC Directive. The Directive is transposed into UK national legislation. The use of jammers is also a serious offence under the UK Wireless Telegraphy Act 2006[1]. Ofcom also has the ability to close remaining loopholes by putting in place a banning order under the 2006 Act which would prohibit import, advertisement and mere possession of jammers. The case for this is easily justified given the clear danger to safety of life services, which present a clear priority for Ofcom. We recommend that Ofcom should introduce such a banning order, ideally in co-operation with other European legislators.

5. The Cabinet Office Civil Contingencies Secretariat should commission a review of the benefits and cost-effectiveness of establishing a monitoring network to alert users to disruption of GNSS services, building on the results of the GAARDIAN and similar projects and the US experience with JLOC.

6. The Cabinet Office should consider whether official jamming trials of GNSS Services for a few hours should be carried out, with suitable warnings, so that users can evaluate the impact of the loss of GNSS and the effectiveness of their contingency plans.

7. Widely deployed systems such as Stolen Vehicle Tracking or Road User Charging should favour designs where the user gains little or no advantage from the jamming of signals that are so important to other services.

8. The availability of high quality PNT sources is becoming a matter of national security with financial transactions, data communication and the effective operation of the emergency services relying on it to a greater or lesser extent.

Greater cross-government coordination of science and technology issues related to national security should explicitly recognise the importance of PNT, treating it as an integral part of the operation of national infrastructure.

c) Increasing resilience

9. The provision of a widely available PNT service as an alternative to GNSS is an essential part of the national infrastructure. It should be cost effective to incorporate in civil GNSS receivers and free to use. Ideally it should provide additional benefits, such as availability inside buildings and in GNSS blind-spots. We are encouraged by progress with eLORAN in this context.

10. The Technology Strategy Board (TSB) and the Engineering and Physical Sciences Research Council (EPSRC) are encouraged to consider the merits of creating an R&D programme focused on antenna and receiver improvements that would enhance the resilience of systems dependent on GNSS.

1 Introduction

The Royal Academy of Engineering became alarmed by a report[2] in May 2009 from the United States General Accounting Office (GAO) which concluded that the United States Air Force would have difficulty in maintaining its investment in the GPS system and in launching new satellites to schedule and cost. The importance of the GPS system to the US and global economies led the Academy to the belief that, although the GAO has sounded alarm bells, it would be politically unacceptable for the United States Government to allow the GPS system fail or become degraded through lack of funding*.

Nevertheless, having concluded that the ongoing funding by the United States Government of the GPS system was, for the time being, safe, the Academy became concerned that the use of GPS for positional, navigational and timing services had become highly ubiquitous, often with little or no consideration of GPS independent back-up systems. In many cases, although GPS independent back-up systems did exist, their use was not adequately exercised and users were not always fully competent in their use.

The Academy, therefore, decided to carry out a study of GNSS, our reliance on them and the consequences of failure or degradation of the GPS service or the associated ground based systems. The study identified a number of threats to GPS as it is currently configured. These range from catastrophic loss of the entire system due to solar activity, bad data uploads to individual satellites or the entire constellation through to local jamming or spoofing of signals or incompatibility of older receivers following system updates.

When a technology such as GPS becomes so useful, so easy to use and universally available, users tend to take the technology for granted and concern themselves less with maintaining and practicing the use of alternatives. At a trivial level, this means that many millions of us now routinely drive around the UK guided by GPS navigation systems, but rarely carry a road map as back-up and, if we do, have probably not invested in an updated road map for many years. Many, more safety critical applications have inadequately exercised back-ups.

> *"It is estimated that, already, 6-7% of GDP in Western countries, i.e. € 800 billion in the European Union, is dependent on satellite radio navigation." - Report from the Commission to the European Parliament and the Council, Mid-term review of the European satellite radio navigation programmes dated 18 January 2011.*

The accuracy, pervasiveness and convenience of GPS mean that its application has moved far beyond navigation and the list of applications continues to grow. The time signals from the GPS system in particular have found application in managing data networks and mobile telephony. The consequences of failure in these applications may only be a loss of efficiency, but the knock-on effects of data congestion to the many users of these networks could cause significant difficulties.

---

* The US GAO published a follow-up report in 2010 called GPS: Challenges in Sustaining and Upgrading Capabilities Persist. The first IIF satellite was finally launched on 27 May 2010, almost 3.5 years late. They conclude: "The IIIA schedule remains ambitious and could be affected by risks such as the program's dependence on ground systems that will not be completed until after the first IIIA launch ... a delay in the launch of the GPS IIIA satellites could still reduce the size of the constellation to below its 24-satellite baseline, where it might not meet the needs of some GPS users."

GIOVE-B arrives in the HPF

With the implementation of the European Galileo system, the resilience of the combined GPS / Galileo system will be considerably improved, but many of the categories of vulnerabilities identified in this report will remain.

The study working group considered that the techniques and equipment needed to interfere with GNSS signals were readily available to anyone who cared to research them. Deliberate interference in GPS signals is already a significant issue with many instances of jamming for criminal purposes and at least one (in Korea) for political motives[3]. With the planned introduction of Galileo, we expect the system to be used for increasingly sophisticated revenue raising purposes, such as road user charging. It is known that organised criminals are willing to invest significant resources in exploiting system vulnerabilities when the potential rewards justify it and we therefore expect a significant increase in attempts to exploit such vulnerabilities over time. We conclude that deliberate interference in GNSS systems will be an emerging threat that needs to be monitored and managed.

During the course of the study our concerns over redundancy and resilience were exacerbated when we became aware that the United States Government had closed its LORAN-C stations. Considerable research and development has been undertaken by the General Lighthouse Authorities and others on an enhanced LORAN (eLORAN) which has been demonstrated to provide a robust alternative to satellite based systems, but the funding of the eLORAN system is not yet secure.

As part of the study, the working group examined the likely future developments of GNSS both in terms of the satellite systems themselves, the receivers and the uses they are put to. At each stage, threats to the continued use of GNSS both locally and globally were examined. Threats were generally categorised as isolated system failures, global system failures and external threats which, except in the case of solar activity, were localised.

2 GNSS overview

Global Navigation Satellite Systems (GNSS) is the generic term for space-based systems that transmit signals that can be used to provide three services: Position, Navigation, and Timing - known collectively as PNT. The best known and most popular of the GNSS is the US Global Positioning System (GPS), although the Russian GLONASS system is regaining its strength and other systems are being developed, most notably Galileo in Europe and Compass in China. The systems all work in approximately the same way so only a description of GPS follows for brevity.

GPS can be split up into three areas, the ground, space and user segments.

- The ground, or control, segment is used to upload data to the satellites, to synchronize time across the constellation and to track the satellites to enable orbit and clock determination.
- The space segment consists of the GPS satellites in six orbital planes. 24 satellites make a full constellation, although there are currently (January 2011) 32 in service, 2 of which have been declared unusable until further notice. The satellite's code is used to identify it in orbit (it should be noted that this is the fundamental difference between GPS and GLONASS which differentiates satellites by frequency channel).
- The user segment consists of the receivers and associated antennas, used to receive and decode the signal to provide PNT information.

GPS is a ranging system with three available carrier frequencies, all multiples of a fundamental frequency (Table 1). The distance is derived primarily through measuring the time difference between the transmission from the satellite and reception at the receiver of a coded signal. This range is more properly known as the pseudorange since it is affected by a number of system unknowns including clock biases and propagation delays which must be solved for or estimated. The carrier phase of the signals can also be used to derive the range, providing for a more accurate position fix, but with inherent ambiguity. Ranges to at least four satellites are required to determine position and time. (Timing applications can function with a single satellite in view, although for verification reasons, two are preferred.)

GPS	GLONASS	Galileo
L1 1575.42 MHz	L1 1602.00 MHz	E1 1575.42 MHz
L2 1227.6 MHz	L2 1246.00 MHz	E5A 1176.45 MHz
L5 1176.45 MHz		E5 1191.795 MHz
		E5B 1207.14 MHz
		E6 1278.75 MHz

Table 1: GNSS RF Carrier Frequencies

The navigation message is transmitted from the satellite to the user and gives the satellite identifier together with information on satellite health, predicted range accuracy, ionospheric and clock correction coefficients as well as orbital ephemeris to allow the receiver to calculate the satellite position. The message also contains an almanac which gives status, location and identifier information for all satellites in the constellation.

Errors or biases occur within GPS as a matter of course and are independent of the interference or denials of service outlined within this report (Table 2).

Error Source	Description
Satellite orbit	Orbital biases occur within the ephemeris transmitted, mostly as a result of un-modeled gravitational forces.
Satellite clock	The satellite clocks experience drift and noise which are modeled and included as part of the broadcast message, although residual error remains.
Ionosphere and plasmasphere	The signals are delayed in the region above an altitude of 80km by an amount proportional to the number of free electrons. The effect is lower when the satellite is at the zenith than when it is near the horizon and it is frequency dependent. Uncorrected this is the largest error source.
Troposphere	Delay in the signal caused by varying temperature and humidity levels at up to 12km in height. Basic models can correct up to 90%.
Receiver noise the signal.	Inherent noise within the receiver which causes jitter in
Multipath	In addition to the direct satellite-to-receiver path, the signals are also reflected from the ground and other objects. These cause multiple copies of the signal or a broadening of the signal arrival time both of which reduce precision.

Table 2: Primary GPS system error sources.

In normal standalone operation, GPS will give a three-dimensional position accuracy of around 5-10m, and also provides velocity to approximately 20 cm/s and time to within 1 microsecond. These accuracies are dependant on the user equipment, error sources present and the configuration of the satellites that are being tracked. If the satellites tracked are all in one portion of the sky for example, the geometry is poor and attainable accuracy will be affected.

Different GPS applications require varying degrees of positional accuracy. In-car and personal navigation, for example, require only the standard GPS positioning accuracy, whereas more demanding applications require augmentation of the standard GPS data, be it in terms of integrity or correction information. Differential GPS (DGPS) is widely used to improve upon GPS accuracies. Here corrections to the pseudoranges (and / or carrier phases) are computed to improve the positional accuracy of a user's GPS receiver. DGPS corrections can be applied in either post processing or real-time. DGPS can generally improve positional accuracy to between a metre and a centimetre depending on the signals used, user equipment and methodologies adopted. Some examples of DGPS services are:

- The Wide Area Augmentation System (WAAS) was developed as an air navigation aid by the Federal Aviation Administration to improve GPS accuracy, integrity, and availability. WAAS uses a network of ground-based reference stations to monitor the GPS satellites signals, and geostationary satellites to transmit information to users.
- The European Geostationary Navigation Overlay Service (EGNOS) is a satellite based augmentation system developed by the European Space Agency, the

European Commission and EUROCONTROL. It is intended to supplement GPS, and potentially GLONASS and Galileo by providing integrity messages, corrections and additional ranging signals.

- The General Lighthouse Authorities' DGPS service is a network of 14 ground-based reference stations providing corrections to GPS via MF radio transmissions out to at least 50 nautical miles from the coast around the United Kingdom and the Republic of Ireland.
- Ordnance Survey runs the national OS Net GNSS infrastructure of 110 base stations. OS Net provides free GPS and GLONASS data products as well as a commercial high accuracy DGPS service.

Augmentation can also take the form of a data service enabling fast acquisition, where the receiver is sent orbital and timing information to enable almost immediate tracking when the receiver is switched on. This technique is one form of Assisted GPS. High-sensitivity GPS receivers exist and are used in difficult environments, for example to aid tracking of the very weak signals indoors.

The next five years will see a massive boost to GNSS with the introduction of satellites from up to four systems, plus the extra, more powerful, signals being added to GPS and GLONASS. 100 plus satellites could be available to the user. Apart from very low-cost applications, GPS only receivers will probably become a thing of the past. This will be partly driven by the plan to move GLONASS from frequency to code division multiple access, and partly driven by the development of the Galileo and Compass systems. Multi-GNSS tracking will deliver improved availability, accuracy and integrity. There are some concerns, however, that the increased number of signals will raise the level of noise leading to lower resilience against other sources of interference.

Photo: ESA

ESA expert inspecting GIOVE-A in clean room

3 The range of applications

The free availability and accuracy of the GNSS signals for location and timing, combined with the low cost of receiver chipsets, has made GNSS the chosen solution for a very wide and growing range of applications. These include transport (rail, road, aviation, marine, cycling, walking), agriculture, fisheries, law enforcement, highways management, services for vulnerable people, energy production and management, surveying, dredging, health services, financial services, information services, cartography, safety monitoring, scientific and environmental studies, search and rescue, telecommunications, tracking vehicles and valuable or hazardous cargoes, and quantum cryptography. Some applications are described below; a fuller list of applications is contained in Annex A.

At present, road transport applications are the majority users of GNSS signals, for in-car navigation, commercial fleet management, taxi services, public transport monitoring and passenger information, and emergency vehicle location, dispatch and navigation. GNSS-based road user charging schemes have been introduced in other countries and are under consideration in the UK.

In aviation, most commercial aircraft now use GNSS for en-route navigation and several States have licensed GNSS for initial approach and non-precision approach to specified airfields. Automatic Dependent Surveillance – Broadcast (ADS-B) is increasingly used in areas of the world where there is no radar coverage; this involves aircraft calculating their position using GNSS and other sources and broadcasting it to other aircraft.

Maritime applications include ocean and inshore navigation, dredging, port approaches, harbour entrance and docking, vessel traffic services (VTS), Automatic Identification System (AIS) hydrography, and cargo handling.

Railway applications include the management of rolling stock, passenger information, preventing doors opening unless they are alongside the platform, cargo tracking signalling, train integrity and level crossing approach.

The use of GNSS for navigation of civil unmanned vehicles includes Unmanned Aerial Vehicles (UAVs), and autonomous land vehicles (from lawnmowers to agricultural machinery).

Scientific applications of GNSS are widespread and include surveying, environmental and atmospheric monitoring, animal behaviour studies, botanical specimen location, meteorology and climate research.

GNSS are used in agriculture and fisheries for land area mapping, yield monitoring, precision planting and spraying, autonomous vehicle control and to monitor fishing limits.

Security applications include tracking of vehicles and valuable cargoes, and covert tracking of suspects.

GNSS timing is important for telecommunications applications. Synchronous technologies are much more efficient than asynchronous technologies but require a time source with appropriate accuracy, stability and reliability to operate effectively or at all, and GNSS can provide this. While ground-based clocks are accurate enough for this purpose (especially with the availability of chip scale atomic clocks (CSAC)), the synchronisation of many such clocks is problematic. GPS allows the derivation of synchronised UTC through resolving the signals from a number of satellites at a known position. Only a 'good guess' of the current time is required and quartz clocks have therefore been adequate for this process making synchronous time keeping significantly more cost effective.

The use of time can be split into three clear and separate aspects: frequency control, time of day and common epoch (usually UTC) time slot alignment (also known as 'Phase').

Stability of radio communications transmission, constant digital traffic flow, time slot alignment and traditional services over next generation Ethernet based infrastructure are some of the features that good time and timing bring to communications networks.

Financial systems increasingly need precise time stamping to prioritise trades and to provide an audit trail.

3.1 Some critical applications of GNSS

In road transport, emergency vehicle location, dispatch and navigation require medium availability and accuracy. Future applications such as automated highways and lane control will need very high availability, integrity and accuracy.

In aviation, search and rescue already uses GNSS, and control of the movement of aircraft and other vehicles on airports and precision landing approaches are being considered.

Safety of Life maritime applications include search and rescue, synchronisation of flashing navigational aids, and navigation in crowded waterways under low visibility conditions.

The Rail Safety and Standards Board forecasts that GNSS will be in use this decade for railway signalling and train movement control and monitoring.

The police use GNSS for tracking suspects and generating evidence to use in prosecutions and for situational awareness for armed response units.

Annex A contains a more complete list of existing and planned GNSS applications together with their required PNT accuracy.

3.2 System-level criticalities

The wide range of applications dependent on GNSS signals provides many ways in which seemingly unrelated services could fail simultaneously as a result of disruption to the GNSS signals resulting from the vulnerabilities described in the next section of this report. Dependence on GNSS connects many otherwise independent services to form an accidental system with a single point of failure. Erroneous GPS signals in an urban area could cause road accidents whilst disrupting the dispatch and navigation of emergency vehicles and causing their communications systems to fail. At sea in fog or at night, jamming could cause collisions between ships or with obstructions whilst causing emergency beacons to broadcast false positions, delaying search and rescue.

No-one has oversight of the increasing range of services that are dependent on GNSS or the complex ways in which they interact, and therefore no-one can reliably fully predict the consequences of a significant disruption of GNSS signals. This is an unsatisfactory situation for important services that are dependent on GNSS. This can be addressed through analysis of the effect of different types of disruption to the service, then making the decision between investing in detection, adding extra robustness or supplementing with an independent source of PNT data that has been shown to be unaffected by the types of GNSS failure that cause concern. In carrying out such an analysis, it will be important to consider whether the service that is being analysed forms part of a larger service and whether GNSS failures might simultaneously disrupt other services that are relied on to provide resilience.

4 Vulnerabilities of GNSS services

All GNSS are vulnerable to failure, disruption and interference, and much work has been done to assess the possible failure modes and their effects on services, and to develop strategies to detect failures and correct them. One important analysis of possible failures in GPS dependent systems is given in Annex B.

The vulnerabilities of GNSS can broadly be classified into three different categories:

1) System related (including signals and receivers).

2) Propagation channel related (atmospheric and multipath).

3) Interference related (accidental or intentional).

GNSS have system-level vulnerabilities: GPS satellites have on rare occasion broadcast dangerously incorrect signals, a reduced number of satellites visible could prevent availability of a position fix, and GNSS receivers can incorrectly process valid signals to give unpredictable results.

GNSS signals are very weak: typically less than100 watts transmitted from a distance of 20,000 km to 25,000 km. When received at the surface of the earth, the signal strength may be as low as –160 dBW (1×10^{-16}) watts, with a spectrum spread out effectively below the noise floor in the receivers. Deliberate or unintentional interference with this signal can easily defeat the signal recovery or overload the receiver circuitry.

Furthermore, signals are vulnerable to disruptions in the atmospheric medium they pass through, and receivers can also unintentionally lock onto reflections of the signals, known as multipath, giving unexpectedly large errors.

These causes can have quite different effects on users, such as partial or complete loss of the positioning and timing service, poorer accuracy, very large jumps in position, velocity or time, and 'hazardously misleading information' (HMI) that is to say, believable data that is dangerously wrong in safety critical applications.

4.1 System vulnerabilities

Each GNSS has three segments: ground, space and user, and each of these segments have vulnerabilities to problems or failures.

Ground and satellite segment vulnerabilities

The ground segment is responsible for maintaining the system time, controlling the satellites, uploading navigation data (Clock prediction data and Almanac and Ephemeris orbit prediction data) that will be broadcast to users from the satellites, and monitoring the signals broadcast across the globe. The satellites carry clocks, signal generation units and amplifiers and antennas to broadcast the signals, modulated with the navigation data.

These systems are designed with high reliability in mind, and in the case of GPS, the ground segment and satellites are designed to be resistant to military attack, but nevertheless there are vulnerabilities, including the following:

Too few satellites – The US Government Accountability Office has identified a long term risk of a shortage of GPS satellites due to potential simultaneous failure of old spacecraft and late delivery of next generation satellites[4]. As the number of satellites drops down to or below the specified minimum of 24

satellites, users would experience a reduction in service, more position outages and periods of worse accuracy due to less favourable satellite geometry. Although the original GAO report was perhaps overly pessimistic and the warnings have been toned down in the more recent version, it highlights how the availability of satellite navigation requires long-term political and financial commitment from the responsible governments, and careful programmatic management. An example of where such governmental commitment became unsustainable was the temporary decline of GLONASS in around 1999[5]. Although the GLONASS constellation has since largely recovered, all GNSS have a long-term dependence on stable financing and good management.

Upload of bad navigation data – Pages of navigation data are uploaded to GPS satellites in advance of applicability, including the clock predictions and precise orbit predictions (ephemeris) required to achieve full position accuracy. If a page of bad data is uploaded to a satellite, the clock and position knowledge of that satellite may suddenly be in error when the page becomes applicable (typically the Ephemeris set is changed every 2 hours), or the error could grow slowly as the time from epoch of applicability increases. Examples of bad GPS data uploads, fortunately without too serious consequences, occurred in June 2002, March 2000 and March 1993[5]. A feasible but extremely unlikely scenario is that bad data is uploaded in advance such that the whole constellation simultaneously transmits erroneous navigation data causing all GPS receivers to fail across the world.

Jump or drift of clock on satellite – GNSS depends on the predictable performance over 48 hours of precise atomic clocks carried onboard the satellites. On occasion, these clocks behave unpredictably, and produce errors that grow slowly in a potentially dangerous way before the operators can spot it and mark it as unhealthy. On 1st January 2004, the clock on GPS satellite SVN-23 drifted for 3 hours before the command centre marked it unhealthy, by which time the range error had grown from 0 to 300 km[6]. Another similar case happened in July 2001[7].

Bad signal shapes – If there is a fault in the signal modulation or generation process on a satellite, an unusual signal envelope can be transmitted that causes unpredictable behaviour in receivers, potentially causing dangerous errors in some cases, while possibly undetectable in others, subject to signal tracking loop implementation. Two examples are the so-called 'evil waveform' produced by GPS satellite SVN 19 in 1993 that caused an error of up to 8 metres[8], and GPS SVN 49 launched March 2009 which carried a piggy-back L5 signal generator unfortunately causing an onboard multipath effect on the main signals, and resulting in variable, sometimes substantial errors in receivers at different elevation angles[9].

Service interruption or loss of satellite due to orbital environment – GNSS satellites pass through the radiation belts around the Earth, and are consequently subject to intense radiation. When solar storms occur (flares, Coronal Mass Ejections (CMEs), etc.), the satellite is subjected to bursts of highly energetic and disruptive particles. These effects are mitigated by the spacecraft design and are not normally a cause for concern, although they reduce the satellite lifetime. Unusually intense events could, however, cause a temporary shut down of the satellites. In the worst case, if a super-storm, or a so-called Carrington event occurs, multiple satellites could be disabled causing major widespread disruption on the ground. Such an event has not occurred since the advent of satellites and although unlikely, it cannot be ignored as a potential threat to society.

Attack on ground segment – The GPS ground segment is designed to withstand military attacks, but could feasibly still have some vulnerabilities to terrorist or cyber attacks. As more GNSS systems become available, there are more targets available to attack (remote monitoring stations could be especially vulnerable) although relative independence of the systems provides some protection.

GNSS user segment vulnerabilities

Unlike the ground and space segment, the GNSS user segment is extremely diverse and uncoordinated, comprising all GPS receivers. These include decryption-capable military receivers, certified safety-of-life aviation receivers, scientific survey receivers and receivers embedded in mass-market mobile phones, and numerous others. Different manufacturers design GNSS receivers to different levels of quality, but even the simplest GNSS receiver is a highly complex mixture of radio and digital hardware and software. The common thread is that all receivers are designed to interface with the broadcast GNSS signals, as documented in the 'Signal-in-Space Interface Control Document' (ICD) definition, for example GPS Open Service[10]. This diversity means that systematic vulnerabilities in GNSS receivers will not affect all users, but still could affect one particular user sector badly, possibly globally, where receivers from one manufacturer with a latent software bug are used widely. Vulnerabilities could include the following:

Leap seconds and roll-overs – Generally the correct ongoing function of a GPS receiver can be tested and verified by manufacturers and users within the course of hours or days. GPS, however, is subject to events which occur rarely and may not be accounted for properly and only discovered after the event has occurred. GPS had a numerical roll-over in August 1999[11] that upset some receivers, and also the derivation of UTC from GPS time is subject to leap seconds once every few years that must be correctly handled. Although the ICD200 describes the correct way to handle leap seconds, some receivers still handle them wrongly and can cause a timing error.

System upgrades – Even though GPS has been operating stably for at least the last decade, system upgrades do occur and can cause unexpected behaviour in receivers due to ambiguities in the ICD or mistakes by manufacturers. In April 2007 a 32nd GPS satellite was added to the constellation which caused problems in some receivers only designed to handle 31 satellites. In January 2010, an upgrade to the GPS ground segment software caused problems with military and timing receivers[12] believed to be connected with acquisition and signal lock behaviour.

Receiver bugs – In some sectors such as military and aviation, the design requirements for a GNSS receiver may be prescriptive and demand certification testing. In other sectors, there are no external requirements to meet, and units need only pass the manufacturers' production test regime. It is unlikely any such receiver would be completely free from software bugs that might somehow affect the performance of the unit. There are particular system circumstances where bugs might be unearthed, such as the handling of satellites labelled unhealthy, the behaviour of receivers when tracking non-standard codes, and the behaviour when signals are stronger or weaker than usual. Depending on the design and configuration of the receiver, different behaviour may be expected if one satellite is in error, or a jamming signal causes a jump in one range measurement, but not others. Receiver future proofing is also key to ensure that the firmware is capable of handling changes in the GNSS system.

Overlay vulnerabilities

In time, users will become increasingly dependent on the various overlay systems that are required to enhance the performance of GNSS, which potentially introduces more vulnerability into the system.

Space based augmentation systems – The SBAS systems (EGNOS, WAAS, etc.) are likely to become vital to aviation and other users who need high integrity for non-precision approach to landing. SBAS is dependent on a small number of geostationary communication satellites that carry a piggy-back navigation payload. When these satellites fail, it may mean the loss of availability[13]. SBAS is not operated as a military system, and may have more vulnerability to attack. SBAS signals are just as vulnerable to ionospheric disruption as GNSS signals.

AGPS – The use of external Ephemeris data to speed the acquisition of a GPS receiver (Assisted GPS) brings in new vulnerabilities from the availability and quality of the assistance information. A bad Ephemeris data-set from AGPS could make a GPS receiver yield hazardously misleading information, which could in future have widespread effects.

4.2 Propagation channel vulnerabilities

Atmospheric vulnerabilities

For ground based users the GNSS signals must pass through the atmosphere, which causes a variety of generally deleterious effects. If the atmosphere were invariant in time and space due allowance could be made, but unfortunately the atmosphere is highly variable over many temporal and spatial scales.

The lowest and densest region of our atmosphere, containing our weather systems, is called the troposphere. Here weather systems can affect GNSS signals causing modest variations in signal delay which can be largely mitigated using a model. Hence the troposphere introduces an error term, rather than a threat.

The ionized upper region of the atmosphere known as the ionosphere can also cause disruptions to GNSS signals and if uncorrected introduce the largest errors in GNSS. The variability of the ionosphere, especially at high and low latitudes and at times close to the peak of the sunspot cycle can be highly problematical. This variability of the ionosphere is one manifestation of space weather. (This is a general term describing variations in the sun, solar wind, magnetosphere, ionosphere, and thermosphere, which can influence the performance and reliability of space-borne and ground based technologies, and can also endanger human health and safety.) The atmospheric GNSS vulnerabilities include:

Slow variations in total electron count (TEC) in the ionosphere – The signal from satellite to ground is delayed in proportion to the total electron count along the signal path and has to be removed or calibrated out. Variations in TEC are caused by the sun's effects on the ionosphere, albeit indirectly. The Earth's diurnal rotation, the sun's 27 day rotation and the sun's activity cycle of 11 years each cause the electron count to rise and fall. Superimposed on these cyclic variations are less easily characterised tidal and other variations. These all introduce a slowly varying error in GNSS range measurements, which can be mitigated using model estimated corrections, DGPS corrections or more completely using dual frequency GNSS receivers.

Fast variations in total electron content - Indirectly, these occur as a result of solar flares and CMEs. The resultant ionospheric gradients cannot always be corrected by SBAS and other differential systems. SBAS can detect that this

Northern Lights over Tromsø, Norway. The Northern Lights can become much stronger and be visible at much lower latitudes than normal during periods of high solar activity, particularly, solar storms.

has occurred (integrity) and consequently there are no safety critical issues due to erroneously relying on GNSS, though SBAS signals can also be disrupted by ionospheric effects. Mitigation is still possible through the use of dual frequency GNSS receivers.

Scintillation in ionosphere - Small scale perturbations in the ionosphere can cause the GNSS signals to break up causing signal multipath. GNSS receivers see rapid variation in both signal phase and amplitude and if not designed robustly, GNSS receivers can lose signal lock. Scintillation most often occurs over the equator and near the poles, but can occasionally be more widespread. The WAAS network was disabled for 30 hours during the solar storm in Oct/Nov 2003[14]. More disturbances are predicted through 2010-2013 as the solar cycle reaches its peak.

Carrington events – If a large CME aligns with the Earth, a super-storm could arise with a major and long enduring impact on space and ground electronic infrastructure. The last such event was in 1859, and experts suggest that the probability of such an event is of the order of once in 200 years.

Deliberate modification of ionosphere – Nuclear explosions in the upper atmosphere can cause similar effects to solar storms, potentially affecting the operation of GNSS for weeks due to propagation anomalies. More particularly, these events would put the satellites at high risk of malfunction through being immersed in a high energy particle environment.

Multipath vulnerabilities

Multipath describes the situation when a receiver picks up reflected signals as well the normal signals direct from the satellite. GNSS signals can reflect off relatively distant objects, e.g. buildings, and cause gross errors in position accuracy if the receiver falsely locks onto this reflected signal instead of the direct signal. More subtle errors are caused when the reflective objects are closer and direct and reflected signals merge together, causing lower precision code and carrier phase measurements. Multipath is ubiquitous and a very well known phenomenon to scientists and receiver manufacturers who have introduced all kinds of measures in receivers to mitigate the effects, such as multipath rejecting antennas, receiver filtering and processing techniques. Multipath can still sometimes cause surprising errors of tens to hundreds of metres to unprepared users, and it is also one of the most significant barriers to future adoption of autonomous car navigation using GNSS. Multipath can be significantly reduced through antenna and receiver filtering and processing techniques. Nevertheless, multipath is considered in this study as more of a *characterisable error source* than a *threat* to GNSS users.

4.3 Accidental interference

Harmonic emissions from commercial high power transmitters, ultra wideband radar, television, VHF, mobile satellite services and personal electronic devices can interfere with the GNSS signals. Depending on the magnitude and frequency of the transgressing signal, there may be complete loss of lock by receivers. An example of this effect was noticed in 2002 when a poorly installed CCTV camera in Douglas, Isle of Man, caused GPS within a kilometre to be blocked.

One specific form of accidental jamming may occur when a (typically old) GPS antenna rebroadcasts the signal on account of poor impedance matching in the amplified signal path from the low noise amplifier, and this interferes with reception in an adjacent antenna. To avoid this risk, antennas should be mounted as far apart as possible and never closer than about 2m.

4.4 Deliberate interference

There are three distinct forms of deliberate interference with GNSS signals: jamming, spoofing, and meaconing.

Jamming is the most likely activity which will impact a conventional industrial use GPS system. Meaconing (delaying and rebroadcasting) and spoofing (false signal) which effectively rebroadcasts erroneous satellite ephemeris are currently less common than jamming, although as mentioned above accidental meaconing could be caused by the proximity of a GPS antenna with poor impedance matching.

The crudest form of jamming simply transmits a noise signal across one or more of the GNSS frequencies, to raise the noise level or overload the receiver circuitry and cause loss of lock. Circuits and assembly instructions for GPS jammers are widely available on the internet, and commercial jammers can be bought for less than £20. Commercial jammers are increasingly sophisticated: some are designed to fit into a pocket, some into car lighter sockets; most jammers are designed to block GPS, GLONASS and GALILEO (even before GALILEO is operational), others incorporate jamming of all cellphone frequencies as well, using multiple antennas. Jammers have been recovered by UK police, examined forensically, and shown to be very effective.

Powerful jammers are also commercially available, up to at least 25W transmitted power. A selection of pictures of commercial jammers from internet websites is shown in Annex C.

Noise jamming can be overcome to some degree by adaptive antennas and noise filtering in well-designed receivers, but some jammers are now transmitting GNSS codes rather than noise, to bypass the filters.

Commercial receivers behave unpredictably in areas where there is noise jamming. Trials by DSTL and Trinity House have shown receivers giving false information rather than reporting an error: sometimes the errors are too large to be misleading (ships' positions shown to be many miles inland, with speeds approaching Mach 1, for example) but there have also been many instances of hazardously misleading information (HMI) where vehicles' positions are offset by a few tens or hundreds of meters, and courses and speeds are incorrect by a few degrees and a few knots. The consequences of HMI could be serious if, for example, ships are navigating in low visibility and broadcasting their (GNSS-derived) position to other vessels.

A report on a Trinity House / DSTL jamming trial is reproduced in Annex D.

Jamming can be split into 4 broad areas: Accidental, Criminal, Red Team Deliberate and Blue Team Deliberate (where Red Team is a generic term for 'enemy/criminal' and Blue Team for 'friendly forces').

Accidental Jamming is most likely to be caused by harmonics from other RF signals which sit on the weak GPS signal-from-space. This will typically be localised and potentially manageable once identified. This may be mitigated by moving the GPS antenna to screen out the problem and is less likely to be an issue for a GPS timing system.

Criminal Jamming is caused by people who are looking to defeat GPS tracking systems. They may be car thieves, road toll evaders, tracker evaders, drivers seeking to avoid commercial mileage limits or to avoid their bosses' knowledge of their movements, etc. This will typically be indiscriminate and both moving and stationary. It may be fairly low power just to defeat the localised vehicle location

system but the car thief is unlikely to be concerned with managing power levels to minimise impact on additional nearby GPS reception. This is unlikely to be a problem for most GPS applications if the jamming event is of short duration and localised.

Red Team Jamming (e.g. Terrorist) is deliberate and may be targeted at some specific aspect of critical infrastructure, possibly but not necessarily timing systems. It will be indiscriminate, more likely to be high power and may occur at a number of locations simultaneously. This is more likely to be a problem and the impact will be dependent on the back-end filtering and antenna design.

Blue Team Jamming is deliberate – generally to defeat a perceived threat of covert tracking. It will probably be low power and have a similar impact to criminal jamming. However there would be an impact if they parked for long periods near critical infrastructure which used GPS timing – for example a TETRA** base station.

** Terrestrial Trunked Radio (TETRA) is a digital trunked mobile radio standard developed by the European Telecommunications Standards Institute (ETSI). The purpose of the TETRA standard was to meet the needs of traditional Professional Mobile Radio (PMR) user organisations such as Public Safety, Transportation, Utilities, Government, Military, and Oil & Gas companies. www.tetramou.com/

5 Resilience to disruption of GNSS services

5.1 Position and navigation

Many strategies are available for checking, enhancing or replacing the position and navigation services provided by GNSS. Many of these are usable only in a limited range of applications: for example, determining position by clock and sextant is usable on the open sea, but not realistic for train protection or control of agricultural machinery.

Alternatives include map or feature matching, inertial navigation (INS), odometry/pedometry, dead reckoning, radionavigation beacons (NDB/VOR/DME), eLORAN, and triangulation from cellular telephone, radio or television transmitters.

Enhanced LORAN (eLORAN) is designed to provide PNT that is accurate enough for most applications and guaranteed to be independent from GNSS.

The topology of cellular phone masts and other communications transmitters has not been designed to provide convenient triangulation, and coverage is very variable. Research by the General Lighthouse Authorities has concluded that such signals cannot provide PNT of sufficient coverage and accuracy to provide adequate backup for marine purposes in the event of loss of GNSS PNT.

5.2 Timing

Back-end filtering is a critical aspect of a GPS timing receiver which will define susceptibility to jamming and interference. To simplify this element – consider four types of oscillator which are effectively used as flywheels, Temperature Compensated Crystal Oscillators, (TCXO), Oven Controlled Crystal Oscillators (OCXO), Rubidium (Rb) atomic clocks and chip scale atomic clocks (CSAC).

TCXO[†] – Temperature Compensated Crystal Oscillator is a low cost (cents/pence) component. The TCXO forms part of a phase locked loop or the basis for a numerically controlled oscillator to offset or compensate for inherent aging and offset. The TCXO will track the GPS off-air signal but will have no ability to 'hold-over' in the event of loss of GPS signal. Recent developments in back end signal processing means that very low cost GPS timing systems fit for purpose in terms of instantaneous stability are available as super-components for a few pounds.

OCXO[‡] – Oven Controlled Crystal Oscillator is a more expensive oscillator (£10s-£100s) with various levels of hold-over stability – usually more stability is more expensive. Like the TCXO the OCXO forms part of a phase locked loop or the basis for a numerically controlled oscillator to offset or compensate for inherent aging and offset but considerably less than the TCXO. The OCXO will track the GPS off-air signal and will have reasonable hold-over performance (of the order of hours depending on stability specification) in the event of loss of GPS signal.

[†] Quartz varies in frequency with temperature. This variation is typically linear at ambient temperatures and a TCXO makes use of this property to compensate for accuracy based on knowing the temperature.

[‡] At higher temperatures e.g. ~80ºC the variation with temperature flattens off. Putting the quartz resonator into a single or double oven minimises the impact that external temperature changes have on the frequency stability.

Rb Atomic – Rubidium Atomic Oscillator is a much more expensive oscillator (£1000+) and forms the heart of major telecom network timing infrastructure. Rb brings considerable improvement in holdover - moving the ability of the infrastructure to withstand GPS outage from days to months.

CSAC - Chip Scale Atomic Clocks are just emerging from the R&D labs with first commercial deliveries recently announced. These will offer stabilities better than Rb along with power consumption less than a tenth and in a package footprint smaller than the current miniature Rb oscillators. This represents a clear paradigm shift in technological innovation and this is a technology to watch since it promises an ability to withstand outages for many months.

In terms of mitigation, one can also consider the use of two oscillators in a 1:1 resilient architecture (usually OCXO and Rb) and then managing the mean time to repair (MTTR) to under 24 hours in the event of failure to ensure that system failures are extremely unlikely[§].

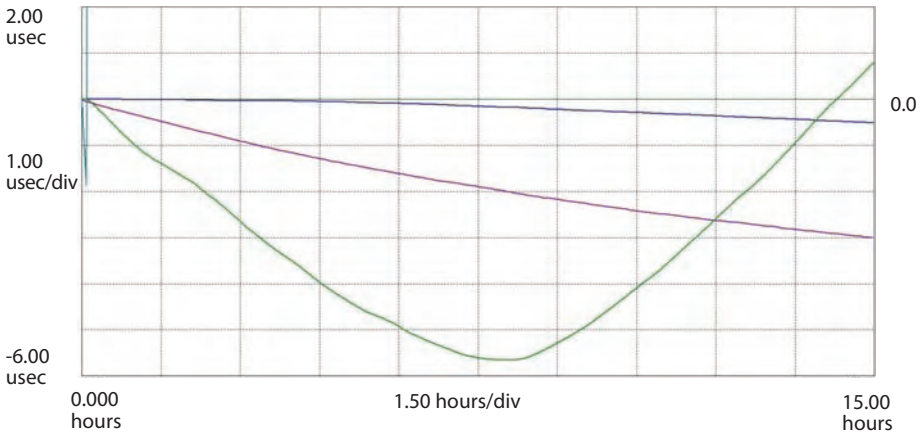


Figure 1 - Comparison of time error in holdover between TCXO (cyan), Low Stability OCXO (Green), High Stability OCXO (Magenta) and Rb (Blue) based GPS timing receivers.

5.3 Vulnerability mitigation

Many receivers incorporate Receiver Autonomous Integrity Monitoring (RAIM). Where more than four satellites are visible and usable, a RAIM-equipped receiver will use the additional signals to calculate pseudoranges that should be consistent with those already calculated. In this way, the receiver can detect and report a problem with a satellite or with the signal integrity. If six or more satellites are available, the receiver may be able to exclude a faulty signal from its calculations and to continue to provide accurate PNT.

In the case of ground and space segments, failures are relatively unlikely but have been recorded (although operators respond by improving the system in turn), and upgrades or unusual events can still throw up problems. Some of these system problems could have serious consequences across the globe. The availability of more than one GNSS (e.g. Galileo to augment GPS) provides a robust mitigation against single system failures, if the contingency is properly handled in the receiver, for example using RAIM, SBAS and other overlay systems.

[§] With MTTR of 24 hours, MTBF – Mean time between failures at the system level approach 100s if not 1000s of years. Given 1000+ elements in a network (not unusual with mobile base stations) – the likelihood of a failure that affects the network could be quite high even with this apparently extraordinarily high MTBF.

Receiver design errors harbour the potential for a systematic failure across whole user sectors, particularly where receivers have been deployed into safety critical applications when they have not been designed for such.

Ionospheric storms pose a threat to GNSS. Through judicious engineering decisions and upgrades to transmitted signals, GNSS systems will, in the future, be more resilient, and extremes of space weather will generally be troublesome rather than dangerous. However, we note the following very important exceptions (with probabilities based on historical evidence):

- High precision applications (such as autonomous and semi-autonomous aircraft landing and precision drilling from oil rigs) operating at UK latitudes will have reduced availability perhaps one to three times per annum in the years close to the peak of the solar cycle. History would also teach us to expect still higher precision and integrity requirements in the future which will, in turn, increase the risk again.
- High precision applications operating at high and low latitudes will have reduced availability many times per annum in the years close to the peak of the solar cycle. In these regions of the world the impact of space weather is more problematical.
- Carrington Event - Both general and high precision applications, operating anywhere in the world will have reduced availability for a significant period (many days), perhaps once per century.

In all cases reduced precision and even outages may occur, but the integrity sub-system should ensure, for example, safety of life.

We also note that:

- Ionospheric scintillation impacts are significantly worsened by intentional or accidental jamming.
- Navigation loss can be mitigated by deeply integrated GNSS-inertial navigation systems.
- Resilience to ionospheric effects will be somewhat improved through the use of signals from multiple constellations

Nevertheless, all GNSS signals share the same frequency band (L-band) and hence have a common vulnerability to the ionosphere.

Some limited measures against interference can be taken within the GNSS receiver itself. Many receivers could be configured to detect interference through monitoring the received signal strength indicator, flagging up a warning if this is suspected. Some checks in software could be implemented to detect basic signal spoofing. Some military GNSS receivers use more radical measures against jamming in their design, such as a very high dynamic range in the signal input capability, and the use of smart antenna arrays that can detect and attenuate jammer signals, but these are unlikely to be adopted in civilian receivers owing to the power requirements and additional cost.

In the USA, the JLOC network has been established to detect jamming nationwide. They are currently registering thousands of incidents of jamming each day – many of them legitimate use by authorised agents. A related European project has recently been funded. The *PRS and Operational Tool to Evaluate and Counteract Threats Originating from Radio-sources* (PROTECTOR) study addresses the problem of detecting interference from radio sources in L-, S-, Ku-

and C-bands and improving the resilience of Europe's Galileo and EGNOS GNSS systems. A recently published article[15] has proposed a cellphone-based network for detecting and locating sources of GNSS interference.

In the UK, the Technology Strategy Board is supporting a project (GAARDIAN) to create technology for a mesh of PNT interference detection & mitigation sensors (IDMs) which will be deployed in the vicinity of PNT dependent infrastructure and applications. These sensors will monitor the integrity, reliability, continuity and accuracy of the locally received GPS (or other GNSS) and eLoran Radio Navigation signals on a 24x7x365 basis creating an alarm network for both natural and intentional interference to GNSS signals. If the system detects an anomalous condition, users can be alerted to the problem and investigate.

In December 2010, a follow on project was announced. SENTINEL, which is funded by The Technology Strategy Board and the Engineering and Physical Sciences Research Council, will deploy trial GNSS interference detection probes in a controlled manner to research a service to address the detection of deliberate or accidental signal jamming and also to detect, quantify and discriminate between interference and natural phenomena and assess the impact of unusual multipath in the vicinity.

6 Conclusions and recommendations

6.1 Reliance on GNSS for PNT is high and increasing

The use of GNSS for a variety of purposes has become so convenient and ubiquitous that there is a strong tendency among users to treat it as a given. At every level, examples of reliance on GPS for positional, navigational and timing uses without fully tested and exercised non-GPS back-ups have been observed. In the great majority of cases, the loss of these services in an individual application will cause only local or isolated inconvenience, but the possibility exists for wider, single mode or common mode failures with more serious consequences.

Although it is currently rare for safety critical systems to be wholly reliant on GNSS, related services that are otherwise independent may have GNSS as a common point of failure, with consequences for the performance of safety critical tasks. Such conditions occur where, for example in the emergency services, navigation and positional data is required to help perform safety critical tasks efficiently, even though its absence would not interfere with the actual emergency response task once the location of the emergency had been reached. There are also a number of primary safety critical systems being developed in fields such as transport.

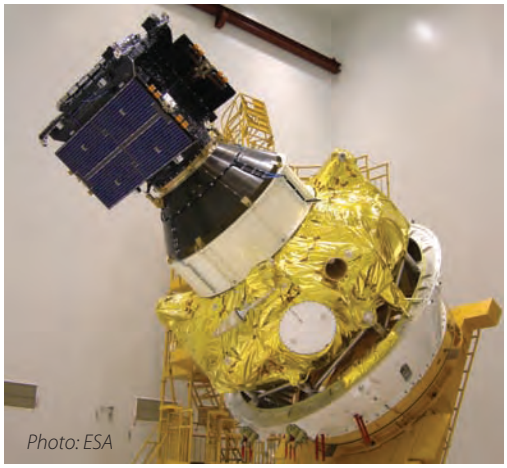
6.2 GPS, Galileo, Compass and GLONASS common vulnerabilities

The risk of a common mode failure affecting an entire GNSS constellation or even multiple constellations cannot be ruled out. The Earth is subject to extreme solar events from time to time and these have the potential to disrupt the GNSS signals, and the satellites themselves. The disruption may be temporary or may cause complete satellite failure. Such super-storm events are not predictable, but studies estimate that these so-called 'Carrington events' will occur with a probability in the order of 1-in-100 per year.

Space Weather events of lesser magnitude will occur more frequently. More than once per decade, at UK latitudes, there may be an interruption to high accuracy GNSS services. There should be no direct safety of life issues if the integrity subsystem informs the users that the navigation solution is degraded, but the absence of the service will have varying levels of impact, which could be mitigated if an alternative navigation system is available.

Risk from jamming is growing. As GNSS becomes more widely used for revenue generation or protection, the rewards from criminal activity aimed at disrupting the system grow. Already it is known that criminals have used GPS jamming in connection with theft of high value vehicles and the avoidance of road user charges[16]. The cost of jamming equipment is low and while users of such equipment are concerned only with the jamming of devices on a single vehicle, the area affected by that jamming signal can be large. It is expected that the introduction of Galileo, with its additional frequency bands and compatibility with GPS will make jamming more difficult, but not significantly so for the determined criminal.

The risk from spoofing is emerging and may become serious.



GIOVE-A mated with Fregat launcher upper stage

6.3 Recommendations

a) Raising awareness and analysing impact

1. Critical services should ensure that GNSS vulnerabilities are included in their risk registers and that the risks are reviewed regularly and mitigated effectively.

2. National and regional emergency management and response teams should review the dependencies (direct and indirect) on GNSS and mitigate the risks appropriately.

3. Services that depend on GNSS for PNT, directly or indirectly, should document this as part of their service descriptions, and explain their contingency plans for GNSS outages (say, of duration 10 minutes, 2 hours, 5 days, 1 month).

b) Policy responses

4. It is already illegal to place GNSS jamming equipment on the market in the EU, as it cannot be made compliant with the EMC Directive. The Directive is transposed into UK national legislation. The use of jammers is also a serious offence under the UK Wireless Telegraphy Act 2006[1]. Ofcom also has the ability to close remaining loopholes by putting in place a banning order under the 2006 Act which would prohibit import, advertisement and mere possession of jammers. The case for this is easily justified given the clear danger to safety of life services, which present a clear priority for Ofcom. We recommend that Ofcom should introduce such a banning order, ideally in co-operation with other European legislators.

5. The Cabinet Office Civil Contingencies Secretariat should commission a review of the benefits and cost-effectiveness of establishing a monitoring network to alert users to disruption of GNSS services, building on the results of the GAARDIAN and similar projects and the US experience with JLOC.

6. The Cabinet Office should consider whether official jamming trials of GNSS Services for a few hours should be carried out, with suitable warnings, so that users can evaluate the impact of the loss of GNSS and the effectiveness of their contingency plans.

7. Widely deployed systems such as Stolen Vehicle Tracking or Road User Charging should favour designs where the user gains little or no advantage from the jamming of signals that are so important to other services.

8. The availability of high quality PNT sources is becoming a matter of national security with financial transactions, data communication and the effective operation of the emergency services relying on it to a greater or lesser extent. Greater cross-government coordination of S&T issues related to national security should explicitly recognise the importance of PNT treating it as an integral part of the operation of national infrastructure.

c) Increasing resilience

9. The provision of a widely available PNT service as an alternative to GNSS is an essential part of the national infrastructure. It should be cost effective to incorporate in civil GNSS receivers and free to use. Ideally it should provide additional benefits, such as availability inside buildings and in GNSS blind-spots. We are encouraged by progress with eLORAN in this context.

10. The Technology Strategy Board (TSB) and the Engineering and Physical Sciences Research Council (EPSRC) are encouraged to consider the merits of creating an R&D programme focused on antenna and receiver improvements that would enhance the resilience of systems dependent on GNSS.

References

1 http://stakeholders.ofcom.org.uk/enforcement/spectrum-enforcement/jammers/

2 www.gao.gov/products/GAO-09-670T accessed 17 February 2010

3 National PNT Advisory Board comments on *Jamming the Global Positioning System - A National Security Threat: Recent Events and Potential Cures* November 4, 2010

4 www.gao.gov/products/GAO-09-670T

5 *GLONASS: As Good as it Should Be?*, E. Rooney, A. Last, Signal Computing Ltd., ION GPS-99 page 1363

6 http://navcen.uscg.gov/pdf/cgsicMeetings/43//09%20PRN-23%2043.PPT

7 www.ion.org/sections/southcalifornia/lavrakas_civil_gps_monitoring.ppt#259,5,What has gone wrong?

8 IBID

9 www.gpsworld.com/defense/news/the-svn-49-story-what-went-wrong-how-it-got-found-and-fixed-7110

10 www.navcen.uscg.gov/pubs/gps/icd200/

11 http://tycho.usno.navy.mil/gps_week.html

12 www.gpsworld.com/gnss-system/news/problems-with-gps-ground-control-software-update-aep-55c-9494

13 www.insidegnss.com/node/2030

14 http://lasp.colorado.edu/education/journalists/solar_dynamics_ws/papers/lowres%20Severe%20Space%20Weather%20FINAL.pdf

15 www.gpsworld.com/wireless/infrastructure/j911-fast-jammer-detection-10720

16 www.guardian.co.uk/technology/2010/feb/22/car-thieves-using-gps-jammer

Glossary

Compass	Developing Chinese GNSS
Galileo	A GNSS planned by the European Union to be an alternative (or supplement) to GPS that is non-military and can provide assured services.
GIOVE	Galileo In-Orbit Validation Element – test satellites launches as part of the Galileo programme.
GLONASS	Global'naya Navigatsionnaya Sputnikovaya Sistema – Russian GNSS which is nearing full deployment..
GNSS	Global Navigation Satellite System – Generic term for space based navigation systems of which GPS and Galileo are examples.
GPS	Global Positioning System – US Military operated satellite constellation and associated ground segments. Although originally conceived for military use, position, navigation and timing signals are fundamental to many civilian applications.
Ionosphere	The region of the atmosphere between around 80km – 600km above the earth. GNSS signals are delayed in the ionosphere proportional to the number of free electrons given off by the sun.
Jamming	Interfering with communications or surveillance
LORAN	LOng RAnge Navigation – a terrestrial radio navigation system using low frequency radio transmitters in multiple deployment (multilateration) to determine the location and speed of the receiver. eLORAN is an enhanced LORAN system currently being deployed.
Meaconing	Re-broadcast of GPS signals in such a way as to create a stronger, but erroneous fix.
Plasmasphere	The plasmasphere, or inner magnetosphere is a region of the Earth's near space environment consisting of low energy (cool) plasma. It is located above the ionosphere.
Pseudorange	An approximation of the distance between the GNSS satellite and a navigation satellite receiver before any corrections are applied.
Spoofing	Broadcast of signals which can appear to be genuine GNSS signals.

Annex A – Current and planned PNT applications using GNSS

Key:

- H, horizontal accuracy;
- V, vertical accuracy;
- S, speed accuracy;
- 3D, all three spatial dimensions.

Aviation applications	Accuracy
En-route navigation	Low (H)
Initial approach, non precision approach and departure	Low (H)
Precision approach (Cat I)	Medium (H) High(V)
High precision approach (Cat II/III)	High (H High (V)
Surface movement	V High (H)
Mid-air refuel	V High (3D)
Formation flying	V High (3D)
Helicopter en-route	Low (H)
Helicopter approach	NI
Automatic dependent surveillance – broadcast (ADS-B)	Low (H) Low (V)
Photogrammetry	V High (H)

Road transport applications	Accuracy
In-car navigation	Low
Fleet management	Medium
Urban traffic control	Medium
Emergency calls	Low
Dynamic route guidance	Low
Selective vehicle priority	Low
Collision avoidance	Medium
Automated highway	High
Road pricing	Medium
Intelligent speed assistance	V High
Lane control	V High

Stolen vehicle recovery	Low
Restraint deployment	High
Trip travel information	Low

Road transport applications	Accuracy
Ocean navigation	Low (H) High (S)
Coastal navigation	Medium (H) High (S)
Inland waterway navigation	Medium (H) High (S)
Tugs and pushers	High (H) High (S)
Icebreakers	High (H) High (S)
Automatic collision avoidance	High (H)
Port approach	High (H) High (S)
Port	V High (H) High (S)
Automatic docking	V High (H)
Hydrography	Low to V High (H) High to V High (V)
Dredging	V High (H) V High (V) V High (S)
Construction	V High (H) V High (V)
Vessel traffic services	High (H) V High (S)
Cargo handling	V High (H) V High (V) V High (S)

Rail applications	Accuracy
Signalling and train control	
Infrastructure data collection	High
End of movement authority	Medium (Terminal) Medium (Busy lines) Low (Rural lines)
Supervision to buffer stops	High
Speed profile calculation	Medium (Terminal) Medium (Busy lines) Low (Rural lines)
Train location	Medium (Terminal) Medium (Busy lines) Low (Rural lines)
Level crossing protection	Medium (Terminal) Medium (Busy lines) Low (Rural lines)
High speed warning	Low
Track-side personnel protection	High
Geographical position of the train	High
Power supply control	High
Advisory station stop	Medium (Terminal) Medium (Busy lines) Low (Rural lines)
Door control supervision	Medium
Train integrity	Medium
Train separation	Medium (Terminal) Medium (Busy lines) Low (Rural lines)
Passenger information systems	
Pre-trip information	Low
On-trip information	Low
Management information systems	
Fleet management	Low
Cargo monitoring	Low
Rolling stock maintenance	Low
Infrastructure testing and inspection	High

Autonomous vehicle applications	Accuracy
Unmanned aerial vehicles	High
Autonomous land-based vehicles	High
Autonomous underwater vehicles	Medium

Timing applications	Accuracy
Network synchronisation	
Communications	Medium
Digital broadcasting	Medium
Power generation and distribution	Low
Other applications	
Satellite monitoring and ground based navigation	Medium
Frequency/time calibration services	High
Maintenance of International time standards	High

Precision agriculture applications	Accuracy
Yield mapping	High
Plot mapping	High
Automatic guidance of farm machines	High

Fisheries applications	Accuracy
Fishing	Low
Yield analysis	Medium
Fisheries monitoring	Low

Oil and gas applications	Accuracy
Exploration	High
Appraisal drilling	High
Field development	High
Support to production	High
Post-production	High

Emergency services vehicle applications	Accuracy
Emergency calls	High
Fleet management for emergency vehicles	High
Dynamic route guidance for emergency services	High
Selective vehicle priority for emergency services	Medium
Search and rescue	
Maritime emergency and rescue operations	High
Aviation emergency and rescue operations	High
Pedestrian emergency and rescue operations	Medium
Personnel protection	
Aid for blind persons	TBD
Persons suffering from Alzheimer's disease	TBD
Transport of the physically handicapped persons	TBD
Protection of very important persons	High

Scientific applications	Accuracy
Geodesy and surveying	V High (3D)
Global reference systems	V High (3D)
Geodynamics	V High (3D)
Geoid determination	V High (3D)
Geographic information system	V High (3D)
Environmental monitoring	V High (3D)
Meteorology	V High (3D)
Climate research	V High (S)
Ionosphere	V High (S)
Bridge/dam monitoring	V High (3D)

The information in this table was provided by the GAARDIAN project and is reproduced with permission.

Annex B – GNSS failure modes and characteristics

Cause	Characteristics	Impact and remarks
Clock jump	This is a clock misbehaviour that results in an abrupt change in the transmitted signal without any notification.	Can result in a range error of up to thousands of metres.
Clock drift	This type of clock misbehaviour introduces a slow ramp type error in the transmitted signal. It is to detect because its signature resembles the typical relative motion of a satellite and GPS receiver.	PRN 23 on 1 January 2004 experienced a clock drift error that grew gradually to a few kilometres.
Incorrect modelling of orbital parameters	Orbital models consisting of satellite orbits and clock parameters are constantly updated by a Kalman estimator maintained at the Master Control Station in Colorado, USA. These are then uploaded to the satellites. Any error in these parameters results in incorrect navigation message. The error in the orbit parameters increases with the time lapse between two consecutive uploads and can be in the form of a slow ramp in the range measurements.	This type of error might be corrected at the next upload normally after eight hours provided the error is detected. Its effect on positioning accuracy depends on the receiver position and geometry of available satellites. It can result in a range error of up to 40 metres.
Radiation damage to satellite payload semi-conductors	The performance of space borne semiconductors will degrade owing to the high energy particle environment. There are two types of phenomenon a) Single Event Upset (SEU) caused by temporary change in the circuitry and b) aggregated ionising dose damage which ages the semiconductors or makes them inoperative. The exposure to radiation varies with the orbit.	Radiation effects can lead to a variety of problems including reduced transmitter power, errors in the navigation data and faults in the operating system more broadly. Semiconductors operating in outer space are radiation-hardened to minimize damage by radiation.
Non-standard	Block IIR satellites are equipped with Time Keeping code (NSC) Systems (TKS) to generate a 10.23 MHz signal. Anomalies can occur in the voltage controlled oscillator of these systems that are shown to be correlated to solar eclipses. This results in the issuance of the Non-Standard Code (NSC). NSC is also generated when TKS loops are open and telemetry data are output by the Navigation Data Unit (NDU).	Generation of NSC acts as a warning to the GPS receiver. A proper GPS receiver design should remove the relevant satellite from the position solution as it is a meaningless measurement. Otherwise the code lock loop could become unstable.
Eclipse related trajectory changes	When a GPS satellite comes out of an eclipse, its trajectory is perturbed due to the effect of changing solar radiation pressure.	This can cause range errors of up to 30 m.
Satellite attitude instability	This results in power fluctuation and changes in the nominal Signal-to-Noise Ratio (SNR).	This can result in either loss of lock or a significant signal acquisition/re-acquisition time.
Increased solar interference	Increased solar noise in extreme circumstances.	In severe cases, loss of lock may occur.
Power fluctuations	The transmitted power fluctuations can make it difficult to lock on to a signal.	Could result in loss of lock.
RF filter failures	Due to filter failure, side lobes may be corrupted. There can be sudden jumps or slow fluctuation in signal frequencies.	This makes it difficult for typical antennae to lock on to signals.

Cause	Characteristics	Impact and remarks
Onboard multipath, onboard interferences and signal reflections	This is due to different transmitting antennae present on the satellite payload.	Due to the increase in the number of signals as a result of GPS modernization, this error might increase in future. This is usually addressed in two ways: (a) Multiple antennae on satellites are positioned in a manner to minimize this error. However, this is complicated by the constraint of maintaining all antenna directions towards the Earth. (b) The multipath error is calibrated on the ground. After calibration as in the case of a typical satellite, attitude error in the range of 10 sec of arc can be present in the line of sight.
Inter-channel bias	These biases are present between different channels on the satellite transmitters due to the differences in the positions of transmitting antennas on the satellite. Furthermore, antenna phase centre error is different for different transmitters.	These errors will have more effect when position solutions are formed using multiple frequencies. Precise calibration on the ground for each channel is required to remove these types of biases. For a typical satellite the error between L1 and L2 antennae phase centres can be half a metre in range, for a Block IIA satellite.
De-synchronization between data modulation and code	This manifests as a constant bias for a particular satellite.	If there is a de-synchronization error of one bit between data and code modulation it can amount to a delay equivalent to a range error of 1.5 sec.
Jamming/intentional interference	This is the generation of a powerful radio frequency in the vicinity of the receiver to either cause loss of lock (jamming) or degrade navigation accuracy (interference). Another way is spoofing which is the intended injection of spurious GPS like signal. A GPS receiver that locks onto such signals will not be able to get meaningful measurements.	Interference from amateur radio operators is a potential threat to GPS signal integrity. Availability of commercial jammers can prevent a GPS receiver from tracking signals.
Unintentional interference	These occur when a GPS receiver is used in the vicinity of an installation that generates radio frequencies in the GPS frequency range.	Harmonic emissions from commercial high power transmitters, ultra wideband radar, television, VHF, mobile satellite services and personal electronic devices can interfere with the GPS signals. Depending on the magnitude and frequency of the transgressing signal, the effect may range from additional noise in signal to complete loss of lock.
Ionospheric errors (I)	The ionized environment extends from 80 km to the satellite altitude and is variable in time and space. It introduces a variable component to the signal delay and phase.	Uncorrected, range errors of typically 10 m can occur in single frequency operation. GPS broadcasts model coefficients in the navigation message which compensate typically 50% of the ionospheric delay during benign conditions. Better performance is achieved from relative positioning. Dual frequency receivers correct virtually all of the ionospheric error.

Cause	Characteristics	Impact and remarks
Ionospheric errors (II)	Amplitude and phase variations (scintillation) occur on all frequencies.	In severe cases scintillation causes loss of lock in carrier and code tracking loops. As a consequence the PNT solution is degraded.
Tropospheric errors	The troposphere extends up to an altitude of about 12 km. The GPS signal is delayed in this layer due to bending and refraction. The error consists of wet and dry contributions.	Uncorrected range errors of ~0.7m can occur In normal conditions, the dry part of the tropospheric delay (90% of the total) can be compensated for by conventional models.
Multipath	These errors are the result of the reception of the GPS signal by the receiver after reflection from surrounding surfaces.	This depends on the operational environment of the receiver and in extreme cases can result in loss of lock.
Receiver problems	Receiver design and development should be according to the standard GPS receiver specification. Departure from these instructions may result in anomalous situations.	Warnings were issued by the US Coast Guard that certain receivers are not integrated properly with other equipment such as AIS (Automatic Identification System), radar, etc.. It might be possible that transmitted satellites are unhealthy but receivers still process their data. An example is carrier phase-only receivers failing to read the NSC. A receiver cannot lock onto NSC hence this will affect the acquisition time in the case of serial receivers and inappropriate utilization of channels in parallel receivers.
Human related failures	GPS as part of cockpit equipment results in overconfidence of the aircrew.	Fatal accidents have been reported.
Low availability	The number of available satellites may not always be sufficient to provide good geometry in all areas of the Earth.	This was reported to have occurred over the UK and the USA in the past decade.
Single-string failure mode	One or both of two critical subsystems – the satellite bus and the navigation payload are operating without backup capacity.	At any time, 16 satellites may be operating in single string failure mode. The non-availability of backup results in the shutting down of the satellite signal in case of failure of the primary critical sub-system.
Leap Second anomaly	This primarily results in a timing error that degrades navigation accuracy.	On 28 November 2003, a leap second anomaly was experienced by many GPS receivers. Receivers might lose track for a second before recovering.

The above table draws heavily on *Failure Modes and Models for Integrated GPS/INS Systems*, Umar Iqbal Bhatti and Washington Yotto Ochieng THE JOURNAL OF NAVIGATION (2007), 60, 327–348. *Used with permission*.

Annex C – Some commercially available jammers

Annex D – Jamming trial example

The following extract from *GPS Jamming and the Impact on Maritime Navigation*, Alan Grant, Paul Williams, Nick Ward and Sally Basker (*The General Lighthouse Authorities of the United Kingdom and Ireland*) is reproduced with permission[20].

The US Global Positioning System (GPS) is currently the primary source of Position, Navigation and Timing (PNT) information in maritime applications, whether stand-alone or augmented with additional systems. This situation will continue in the future with GPS, possibly together with other Global Navigation Satellite Systems (GNSS) e.g. Galileo, being the core PNT technology for e-Navigation – the future digital maritime architecture. GPS signals, measured at the surface of the earth, are very weak. As such, the system is vulnerable to unintentional interference and jamming, resulting in possible denial of service over large geographical areas. The result of such interference could be the complete failure of the mariner's GPS receiver or, possibly worse, the presentation to the mariner of hazardously misleading information (HMI) for navigation and situational awareness, depending on how the GPS receiver reacts to the jamming incident.

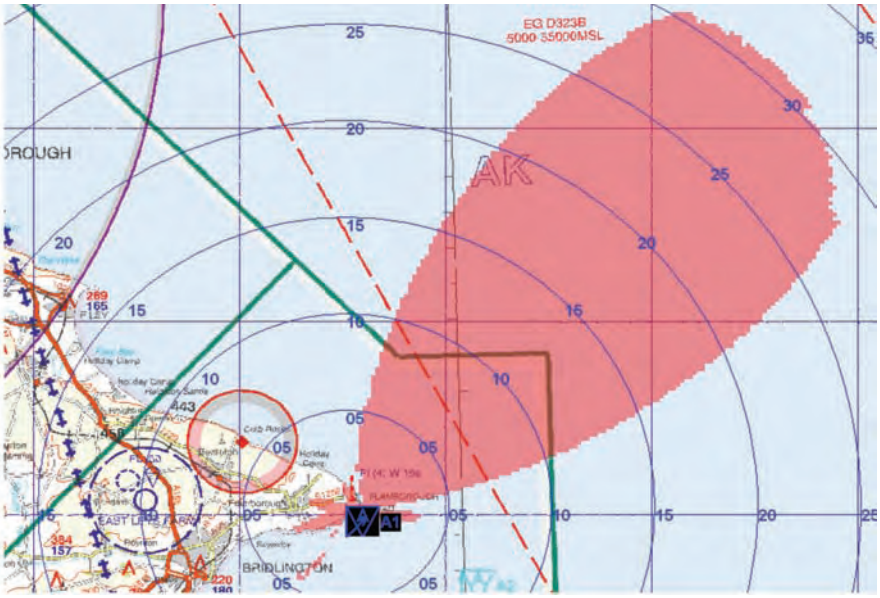
Recognising this, the General Lighthouse Authorities of the United Kingdom and Ireland (GLA), in collaboration with the UK Ministry of Defence (MOD) Defence Science and Technology Laboratory (DSTL), have conducted a series of sea-trials with the aim of identifying the full effects of GPS jamming on safe navigation at sea.

The trial was conducted over several days during April 2008 at Flamborough Head on the East coast of the United Kingdom. DSTL provided a professional low-to-medium power jammer, which was controlled remotely by two VHF transceivers and transmitted a known pseudo-random noise code over the civilian L1 frequency providing a jamming signal over the whole 2MHz bandwidth of L1. Although the unit was capable of broadcasting on the P code, this was not activated. The total power of the signal over the 2MHz bandwidth was approximately 2dBW (~1.5W) of power.

The Coverage area of the GPS jamming unit at 25m above ground level on maximum power of 1.58W ERP is shown in the figure below (Image courtesy of DSTL).

For the dynamic trials, the Northern Lighthouse Board vessel *NLV Pole Star* steered a course back and forth between two waypoints on a path that dissected both the main lobe of the GPS jammer and the two side lobes, but with sufficient length beyond the jamming region to enable the various GPS enabled units to reacquire satellites.

The crew of *Pole Star* was fully briefed prior to the trial and so expecting GPS-enabled systems to fail.



When *Pole Star* entered the jamming zone, numerous alarms sounded on the bridge over a period of approximately 10 minutes. These alarms were all linked to the failure of different functions to acquire and calculate their GPS position, which included: the vessel's DGPS receivers, the AIS transponder, the dynamic positioning system, the ship's gyro calibration system and the digital selective calling system. The crew of the *Pole Star* was able to recognise each alarm and silence them but they were expecting the alarms to sound. In the situation where a crew was not expecting this level of system failure then the distraction caused by so many alarms sounding at once could have had a significant effect. The effect could be made worse depending on the time of day (potentially a vessel's bridge can be single-manned at night, or with one officer and a look-out) or if the vessel is performing a manoeuvre or operation demanding high accuracy and a high degree of human concentration at the time of GPS failure, such as docking in poor visibility.

Some vessels have integrated bridge systems, which enable automatic execution of a passage plan on autopilot. If this system is operating at a time that jamming occurs, then the vessel's course and heading may change without informing the crew, potentially leading to extremely hazardous consequences.

Although the *Pole Star's* crew was expecting GPS failure, problems were experienced. The vessel's Electronic Chart Display & Information System (ECDIS) was not updated due to the failure of the GPS input, resulting in a static screen. ECDIS is the normal mode of positioning on board *Pole Star* (with paper chart backup,) and during the periods of jamming some crew members became frustrated when trying to look at the ECDIS. This resulted in the monitor being switched off!

There are several questions raised by this trial, such as the ability of a vessel's crew to quickly revert to traditional means of navigation and also the extent to which they are able to navigate with these means. Given the greater reliance on satellite navigation, in particular GPS, these skills are not being used daily and are no longer second nature. This trial also raised awareness of the number of alarms that can sound on the bridge and how the sheer quantity can be distracting.

Three additional receivers were installed on the trial vessel two of which were typical marine grade differential GPS receivers, the third was a more expensive dual frequency surveying receiver (configured to operate on GPS L1 only). Data in the form of NME sentences was recorded from each receiver throughout the jamming trial. It should be noted that due to a lack of space on the vessel's mast, antennas for the three receivers were installed on the handrail of the main deck, which meant there was a certain amount of sky obscuration due to the vessel's superstructure.

Over the course of the dynamic trials the receivers were monitored and all of them lost GPS lock. The two differential receivers maintained lock on the medium frequency broadcast from the nearby Flamborough Head DGPS reference station; however as the reference station was also affected by the jamming signal, there were no corrections to apply and their position solution was derived from standalone GPS. When processing the recorded data from the three receivers, the NMEA GPRMC (recommended minimum content) sentence was used as this provides the reported position, speed and time. This sentence also provides an indication of the validity of the data, setting or clearing a single bit flag. The decision to set or clear the data valid flag is one that is made by the receiver. When processing the recorded data from the various receivers only data declared valid was used, which resulted in the two typical marine grade receivers providing erroneous positions as they entered and exited the jamming region. The magnitude of the position error varied, with some small errors, but with others several tens of kilometres away from the true location. Figures 1 and 2 provide the reported positions from one receiver, plotted on Google Earth™. The left-hand plot is from the control run where the jamming unit was disabled; the right-hand plot is from a run where the jamming unit was enabled and erroneous data was observed. The colour of each reported position is an indication of the reported vessel speed at that moment, with blue positions indicating a speed of less than 15 knots; yellow positions indicating a speed of between 16 and 50 knots; orange positions indicating a speed of between 51 and 100 knots and red positions indicating a reported speed of greater than 100 knots.

Figure 2 shows that the number of erroneous positions was significant with the majority of positions coloured red, indicating the reported speed was greater than 100 knots (the greatest reported speed was over 5000 knots). Clearly, if this data was being used as input to a navigation system, whether it was an autopilot or simply an electronic chart the implications are serious. The results shown in Figure 2 were typical from the two marine grade receivers, although it was noted that the effect of jamming was more severe when sailing North with the vessel superstructure between the jamming unit and the GNSS receivers' antennas. Therefore, it may be presumed that the jamming signal was attenuated due to the shadowing effect of the vessel's superstructure and the 'moment of indecision', that period of time when the strength of the jamming signal was comparable with that of the GPS satellites, was greater and resulted in an increased number of erroneous positions. The more expensive survey grade receiver did not provide any erroneous data positions, rather opting to provide no position information when experiencing interference from the jamming unit; clearly this is the preferred situation.

The GPS receivers onboard *Pole Star* were also affected by the jamming signal and also reported inflated speeds, albeit on to a smaller degree. The reported position

on the vessel's ECDIS wandered around and the reported speed also increased above the maximum speed of the vessel. However, the vessel's receiver did stop providing position information quite quickly once the vessel had passed into the jamming area. The implications of providing erroneous positions can be severe and can greatly affect the safety of the mariner and those around them.

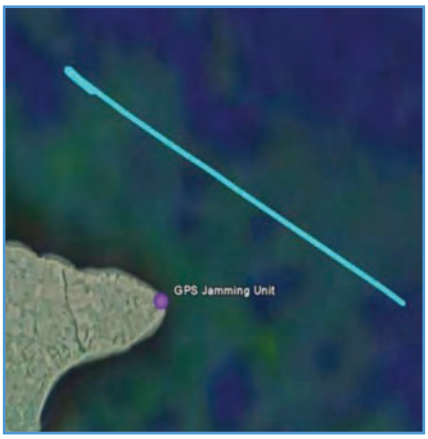


Figure 1: Reported positions with no GPS jamming active

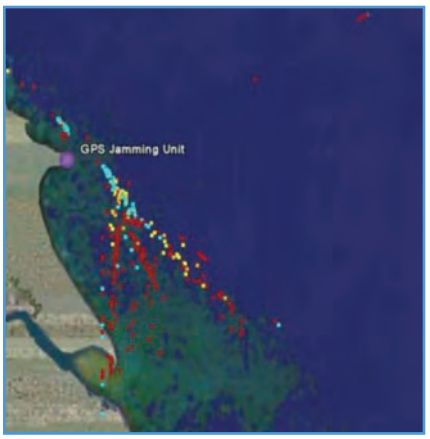


Figure 2: Reported positions with GPS jamming switched on.

Conclusions

GPS is vulnerable and this trial has investigated GPS service denial by intentional interference using low-power jammers. It should be clear that the results can be extended to GPS service denial by unintentional interference. Unintentional sources of interference include spurious harmonics from active TV antennas, damaged GPS antenna cables and ionospheric effects. The latter are correlated with an eleven-year sun-spot cycle and are particularly prevalent at high latitudes. This will bring challenges when arctic shipping routes become available.

The main conclusion from this trial is that GPS service denial has a significant impact on maritime safety:

- On shore – the marine picture presented to Vessel Traffic Services / Management (VTS) will be confused as AIS information with erroneous positions and high-velocities conflicts with the radar information. Further study is needed to determine how VTS operators will respond.
- Aids to Navigation (AtoNs) – DGPS reference stations can be jammed and the impact may result in the absence of DGPS corrections and integrity information broadcast to users over a very large geographical area; AIS used as an AtoN may broadcast incorrect information; and synchronised lights may not be synchronised, thus having an adverse impact on visual conspicuity.
- On ships – navigation, situational awareness, chart stabilisation and DSC emergency communications will be lost if they are based on GPS. Some vessels have integrated bridge systems, which enable automatic execution of a passage plan on autopilot. If this system is operating at a time when jamming occurs then, depending on the system design, the vessel's course and heading may change without informing the watch-keeper, potentially leading to extremely hazardous consequences. At this point, continuation of navigational safety is dependent on mariners' abilities to recognise that GPS

service is being denied and to operate effectively using alternative techniques (e.g. radar parallel-indexing). Increased use of ECDIS will increase the attendant risks.

- On people – People are conditioned to expect excellent GPS performance. As a result, when ships' crews or shore staff fail to recognise that the GPS service is being interfered with and/or there is a loss of familiarity with alternative methods of navigation or situational awareness, GPS service denial may make a significant impact on safety and security. In this trial, despite the fact that the *Pole Star's* crew was forewarned, problems were experienced with the ECDIS. Moreover, the number of alarms that can sound on the bridge can be distracting. Moving to other navigation techniques can cause an increase in bridge workload.

A was unaffected by GPS jamming and demonstrated an accuracy of 8.1m (95%) which is comparable to stand-alone, single-frequency GPS. Consequently, A can be used to detect erroneous positions and high velocities that may be experienced during GPS service denial. Moreover, when GPS is unavailable, A can provide a PNT input to all maritime systems. Finally, in the future e-Navigation environment, the combination of GPS, Galileo and A will provide robust and resilient PNT in order to reduce the impact of human error and to improve the safety, security and protection of the marine environment.

Annex E – Acknowledgements

Working group

Dr Martyn Thomas CBE FREng (Chairman)
Martyn Thomas Associates Ltd

Professor Jim Norton
Independent Director

Alan Jones
Cotares Ltd

Professor Andy Hopper FREng
University of Cambridge

Nick Ward
General Lighthouse Authorities of the UK & Ireland

Professor Paul Cannon FREng
QinetiQ

Neil Ackroyd
Ordnance Survey

Paul Cruddace
Ordnance Survey

Martin Unwin
Surrey Satellite Technology Ltd

Secretariat

Richard Płoszek
The Royal Academy of Engineering

Other contributors

Charles Curry
Chronos Technology Limited

Professor Washington Ochieng
Imperial College, London

FSC
www.fsc.org
MIX
Paper from responsible sources
FSC® C018405

Printed using vegetable based inks on paper from well-managed forests.

The Royal Academy of Engineering

As Britain's national academy for engineering, we bring together the country's most eminent engineers from all disciplines to promote excellence in the science, art and practice of engineering. Our strategic priorities are to enhance the UK's engineering capabilities, to celebrate excellence and inspire the next generation, and to lead debate by guiding informed thinking and influencing public policy.

The Academy's work programmes are driven by three strategic priorities, each of which provides a key contribution to a strong and vibrant engineering sector and to the health and wealth of society.

Enhancing national capabilities

As a priority, we encourage, support and facilitate links between academia and industry. Through targeted national and international programmes, we enhance – and reflect abroad – the UK's performance in the application of science, technology transfer, and the promotion and exploitation of innovation. We support high quality engineering research, encourage an interdisciplinary ethos, facilitate international exchange and provide a means of determining and disseminating best practice. In particular, our activities focus on complex and multidisciplinary areas of rapid development.

Recognising excellence and inspiring the next generation

Excellence breeds excellence. We celebrate engineering excellence and use it to inspire, support and challenge tomorrow's engineering leaders. We focus our initiatives to develop excellence and, through creative and collaborative activity, we demonstrate to the young, and those who influence them, the relevance of engineering to society.

Leading debate

Using the leadership and expertise of our Fellowship, we guide informed thinking, influence public policy making, provide a forum for the mutual exchange of ideas, and pursue effective engagement with society on matters within our competence. The Academy advocates progressive, forward-looking solutions based on impartial advice and quality foundations, and works to enhance appreciation of the positive role of engineering and its contribution to the economic strength of the nation.

The Royal Academy of Engineering promotes excellence in the science, art and practice of engineering.

Registered charity number 293074

The Royal Academy of Engineering
3 Carlton House Terrace, London SW1Y 5DG

Tel: 020 7766 0600 Fax: 020 7930 1549
www.raeng.org.uk