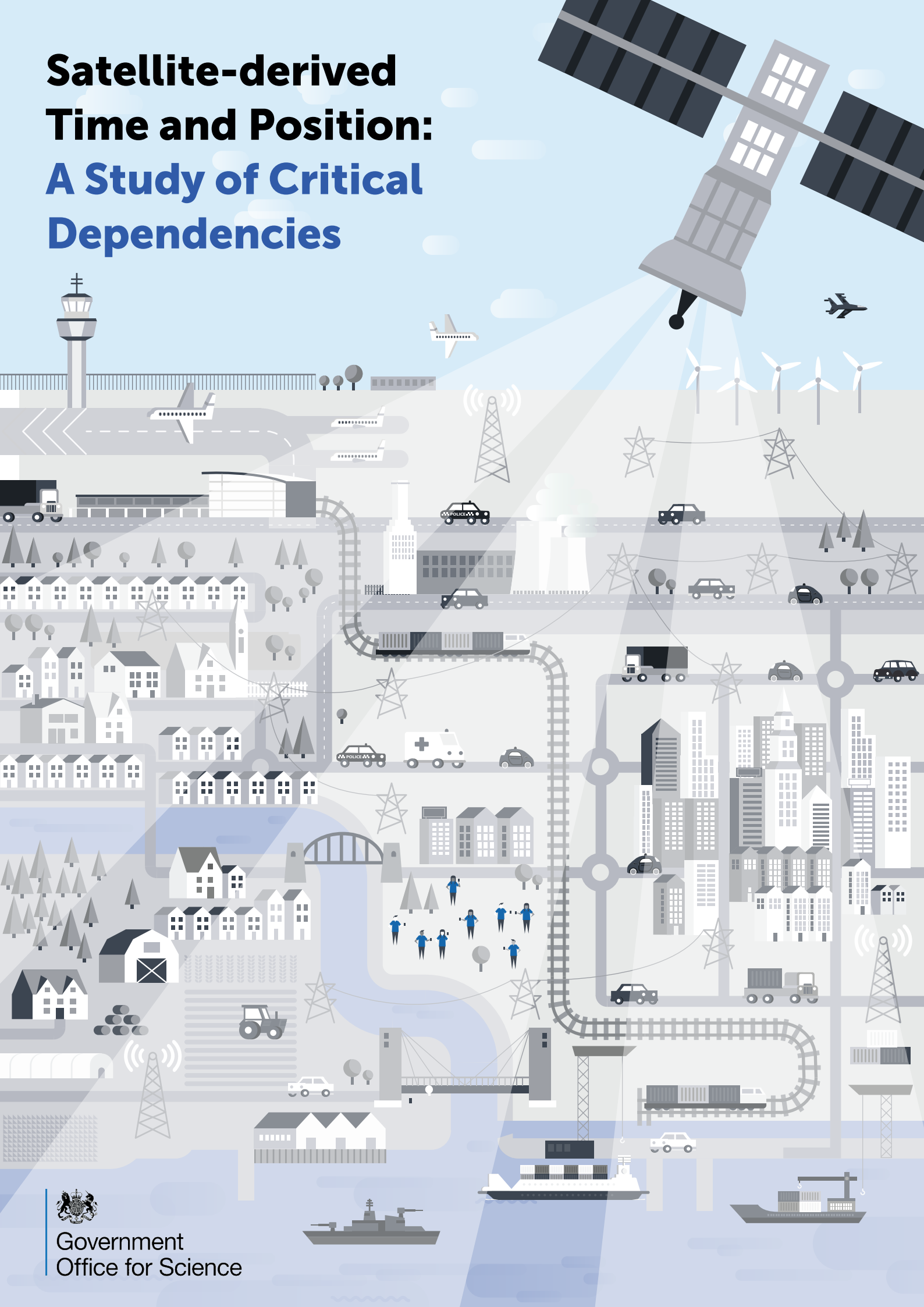
Satellite-derived Time and Position: A Study of Critical Dependencies



Government
Office for Science

Contents

Foreword

Global navigation satellite systems (GNSS) are often described as an “invisible utility”. Signals transmitted from far above the Earth enable communications systems across the world. They enable the movement of goods and people, and facilitate the global supply lines that underpin our economy. They help to maintain electricity supply and support our emergency services.

These examples merely hint at the many and varied ways in which GNSS has become integral to our daily lives – and this importance will only increase as new technologies and innovative applications capitalise on the accurate time and position information that GNSS provides.

However, our awareness of GNSS is out of step with our actual dependence upon it. In some sectors, the vulnerabilities of GNSS to both natural and ground-based interference, including through malicious attacks, are poorly understood. In others, there is insufficient protection against disruption, reducing our collective resilience to a loss of these systems.

It is in our national interest, as this report makes clear, that we recognise the precise nature and extent of our dependence on GNSS. We must take steps to increase the resilience of our critical services in the event of GNSS disruption, including by adopting potential back-up systems where necessary.

These are, of course, global challenges which present opportunities for the UK. Our science base has broad expertise in the disciplines that are driving research and development in high-integrity position, navigation and time (PNT). We are home to pioneering satellite companies as well as firms offering world-leading PNT technologies and services. We should take full advantage of these skills and experience to ensure that we improve our resilience to disruption.

This independent review represents a vital step in understanding the UK’s dependency on GNSS and recommends to Government a number of measures to improve our resilience. Importantly, it also recognises that innovation will be key to realising, fully and safely, the economic and societal benefits offered by GNSS. The Government will give all due consideration to its findings.

Oliver Dowden CBE MP
Minister for Implementation

Executive Summary

Introduction

In the smartphone age, we can glance at a screen to check the time, know our position or work out how to get from A to B by the most convenient route. Some 20,000 km above us, circling the Earth at several kilometres per second, are multiple satellites that can give time accurate to billionths of a second and position accurate to a few metres. Chip-sized receivers in phones pick up signals from these satellites – doing away with the need to wear a watch or carry a map, let alone read the stars.

So effective are global navigation satellite systems (GNSS) at delivering two essential services – time and position – accurately, reliably and cheaply that many aspects of the modern world have become dependent upon them. Alternative means exist for deriving time and position, but – for the majority of users, at least – they cannot compete on price or convenience.

Each satellite is equipped with a series of highly precise atomic clocks. When four or more satellites are in view, a receiver can calculate the distance to each satellite by measuring the time delay between signal transmission and receipt. From this, a GNSS-embedded device can derive accurate time and its own position with metre-level accuracy, enabling navigation.

Computer networks, electricity transmission, broadcasting and telecommunications all require highly accurate and synchronised time across a geographically distributed network. All of them can depend on timing derived from GNSS. In addition to synchronisation, a GNSS typically distributes a timescale that can be closely correlated to Coordinated Universal Time (UTC), the international time scale. Traceable time – the ability to verify continuously when events take place – is fundamental in contexts such as financial trading, to enable regulatory oversight and analyse market anomalies.

Transport systems, supply chains and the general population – anything or anyone on the move, in other words – have all experienced significant benefits from the positioning and navigation capabilities of GNSS.

A number of UK services rely on satellites for both time and position. Emergency services, for example, require both accurate time for their communications and accurate position for locating the closest resource to an incident and signposting the most efficient route to reach it. Similarly, transport systems and supply chains use GNSS for navigation and GNSS time to enable communication.

While some technologies can achieve greater accuracy than GNSS over a small area, it is the accuracy combined with global coverage of GNSS that singles it out. Indeed, the capability of GNSS has exceeded the requirements of many of the most demanding technical applications. Numerous applications derive time from satellites to a far greater accuracy than they actually require, taking advantage of availability, relative ease of deployment and affordability — a receiver costing a few pounds offers the same accuracy as a high-end atomic clock costing tens of thousands of pounds. Although the costs of launching and operating a constellation of satellites are considerable, investment is returned as much as fivefold in societal benefits and enterprises supported[1].

As a consequence, GNSS receivers are now deeply embedded in countless systems and applications. GNSS has become the dominant engineering solution when building systems requiring position and timing. It has already transformed our daily lives and is set to become an integral part of beneficial applications in the future.

However, despite all of the advantages that GNSS brings, there are drawbacks. Both satellites and their signals are exposed to the effects of space weather, while the signals themselves are inherently weak and vulnerable to interference. Receivers struggle in built-up environments. Meanwhile, the threats posed by accidental and deliberate interference and cyber-attack[2] are steadily evolving.

Since the advent of low-cost and single-chip receivers, our dependence on GNSS has rapidly increased, yet our awareness of that dependence has lagged behind. Ignorance of the importance of precise time in the modern world and the role of GNSS in this is especially acute. Moreover, given the interdependency of modern networks, a system of systems has developed in which GNSS presents a potential single point of failure affecting multiple services and applications.

Improving the resilience of our position, navigation and time-dependent services – particularly for critical infrastructure and to support future applications – is vitally important.

Aims and approach

The purpose of this report is to lay out the breadth, scale and implications of our reliance on GNSS. It examines this reliance mainly in terms of existing critical national infrastructure (CNI)[3] but also considers future digitally-based infrastructure – such as 5G, electricity system management, autonomous vehicles and the Internet of Things – and other non-critical applications, which GNSS will continue to enable. It explains ways in which CNI operators can manage their dependence on satellite-derived time and position, and contains recommendations for government on how to improve national resilience with regards to use of GNSS.

This report was prompted by a recommendation in a recent Government Office for Science report on quantum technologies: specifically, it advised that we “review the critical services dependent on GNSS timing signals and mitigate the risks by analysing how long they should be capable of operating with back-up or holdover technology”[4].

Since there are also critical services that use GNSS for position and navigation, they are also covered in this report. The report’s overarching purpose, therefore, is to understand the UK’s dependence on GNSS signals and consequent potential for disruption.

Like the report on quantum technologies, this is a Blackett review: an expert-led, independent study, convened by the Government Chief Scientific Adviser, to answer specific scientific and/or technological questions, and to inform policy makers[5].

For CNI sectors, we have sought answers to the following questions:

- what position, navigation and timing (PNT) information is needed for – and to what levels of accuracy, integrity, availability and continuity
- what sources are used to provide PNT information

- whether any standards or regulations exist for their use
- what impacts may arise from losing accurate PNT – and how to identify loss of accuracy
- what redundancy[6] or resilience is in place; and
- what future infrastructure is expected to use GNSS-derived PNT to any extent.

Some challenges in this area require a coordinated international approach, so it is not for the UK government alone to make GNSS more resilient. What matters is ensuring resilient PNT at the point of use. In this context, there are levers that policy makers can and should use to ensure that CNI operators, present and future, plan for potential disruption of GNSS signals and have adequate back-up systems in place.

This report does not seek to prescribe individual technologies but to highlight their capabilities, to indicate where GNSS is vulnerable or falls short, and propose where efforts to improve resilience could be directed.

It starts by examining the origins of GNSS systems and explaining how they work. It then explores uses of GNSS signals and their vulnerabilities, before considering the dependencies of CNI sectors and of emerging applications. The final chapters look at ways to mitigate those dependencies and at approaches for developing standards and regulation in this area.

Recommendations

Improving awareness

GNSS is so prevalent today that it has contributed to a system-of-systems issue, such that even the most vigilant operators of infrastructure and other applications may not be completely aware of the magnitude of their reliance. Even in systems presumed to be independent of GNSS, master clocks and other seemingly independent sources of time – such as some internet time services based on Network Time Protocol (NTP) – are in fact based on GNSS receivers and therefore hold an unseen dependence. This needs to be better understood.

Recommendation 1
Operators of CNI should review their reliance on GNSS, whether direct or through other GNSS-dependent systems, and report it to the lead government department for their sector. The Cabinet Office should assess overall dependence of CNI on GNSS.

Dependence on GNSS remains variable. In general terms, dependence is greater in sectors and markets where use of GNSS presents a simple, cost-effective solution to providing vital information and connectivity (as with smartphones). In these areas, regulation tends to be light and there is less call for formal systems engineering, testing and evaluation disciplines.

Dependence is generally less in safety and critical systems, where regulation and standards exist, and where these disciplines are practised. Equally, GNSS is less common where there are more appropriate alternatives to deliver PNT, or where a system operates in an environment where GNSS cannot function, such as underground or underwater.

A number of groups have highlighted the scale of dependence on GNSS and the issues it raises within certain sectors[7]. In the UK, government resilience planning refers to the threat to GNSS operation from severe space weather, but although this is an important consideration, space weather is by no means the only threat to GNSS; others are much more likely.

Recommendation 2
Loss or compromise of GNSS-derived PNT should be added to the National Risk Assessment in its own right, rather than as a dimension of space weather alone.

Addressing vulnerabilities and threats

When GNSS signals reach the Earth's surface, their power is well below the level of ambient noise. Receivers use an algorithm to discount noise and identify the characteristic signal shape in an internationally recognised frequency band. Despite this, receivers can be overwhelmed by more powerful transmissions infringing on the GNSS frequency band. Demands on the radio spectrum are increasing steadily, with greater sharing of some spectrum bands.

Recommendation 3
The Department for Digital, Culture, Media and Sport (DCMS), with Ofcom, should continue to address the risk of interference to GNSS-dependent users, including CNI, in allocation of radio spectrum to new services and applications[8].

There are also many natural environmental factors that hinder the operation of receivers, such as ionospheric disturbances, reflected signals and severe weather. Particular difficulties arise within man-made environments: urban canyons in cities, for example, cause "multipath effects", where reflected signals are difficult to distinguish from direct signals. GNSS is unavailable indoors or underground where it is impossible to receive the required clean signals.

Orbiting satellites themselves are exposed to natural phenomena such as space weather. Extreme space weather, and in particular a Carrington-level event[9], could disable satellites for a period of days or even permanently, depending on the severity of the event. Such is our dependence on these assets that a recent study by London Economics estimated the economic impact to the UK of a five-day disruption to GNSS at £5.2 billion[10].

GNSS-derived signals are further vulnerable to interference through "jamming" and "spoofing" – once the domain of states, but now within the capability of hackers, criminals, pirates or terrorists. Jamming, either accidental or deliberate, deafens nearby receivers with either noise or unwanted signals. Spoofing involves broadcasting false signals for receivers to lock on to, or introduces incorrect data into receiver software to affect its ability to process and calculate time and position correctly. There is also the possibility of delaying and re-broadcasting of signals to interfere with GNSS receivers.

Jamming and spoofing of GNSS are indiscriminate, with often secondary and unintended consequences. The effects of such interference range between partial and complete loss of PNT services, involving reduced accuracy; jumps in time, position or direction. Where receivers respond by bluffing it can result in "hazardously misleading information" being passed into reliant systems. Systems that are reliant on GNSS for precise time are generally automated, often unattended, and therefore at greater risk if attacked.

The range and scale of these problems are growing. Inexpensive jamming and spoofing equipment or software is readily available online. Where demand for such equipment may previously have come from van drivers seeking to evade scrutiny by their bosses on delivery rounds, it now includes teenagers subverting computer games like Pokémon GO. It includes

criminals attempting to intercept merchandise on the move or to flout financial trading regulations. In 2017, numerous vessels in the Black Sea reported GPS interference, where their on-board receivers were giving their position as inland[11].

All GNSS-enabled services are susceptible to jamming, as well as to software and hardware faults on satellites, in ground-based control systems and in the receivers themselves. Signals reserved for military or defensive purposes come with authentication codes that protect against spoofing. The EU's civil Galileo system[12] will include a "public regulated service" (PRS) for European governments and accredited infrastructure users, which will have similar facilities; the EU is considering mandating use of PRS for CNI sectors. While the availability of additional constellations such as Galileo will reduce dependence on GPS, and bring improved performance, it will not be revolutionary and the problems posed by different sources of interference remain.

With the increasing adoption of automated road user charging and offender tagging services, all based on GNSS, the incentives for disrupting signals are also increasing. There are also increasing examples of more serious near misses – where broadcasters or air traffic controllers have faced the prospect of operating without access to GNSS.

Recommendation 4
DCMS should review, with Ofcom, the legality of sale, ownership and use of devices and software intended to cause deliberate interference to GNSS receivers or signals – to determine whether the Wireless Telegraphy Act 2006 requires revision.

Recommendation 5
CNI operators should assess – with guidance from the National Cyber Security Centre (NCSC) and the Centre for the Protection of National Infrastructure (CPNI) – whether they need to monitor interference of GNSS at key sites such as ports. Where operators do monitor, data should be shared with the relevant lead government department.

Mitigating dependence on GNSS

If GNSS were invulnerable, they would meet the requirements of most sectors. In light of their weaknesses, however, mitigations need to be considered on a case-by-case basis. Solutions vary according to whether a service depends on time or position, or both. They also vary by sector.

For example, precision agriculture and automated shipping container terminals have a similar degree of required positional accuracy, but the requirements for integrity (level of confidence in GNSS operating correctly) are entirely different – and lower crop yields present a different order of problem than a container dropped in the wrong location. This is as true for timing as for position. Quartz oscillators are ideal for some applications, but for distributed time across a network, higher-quality components and additional infrastructure are necessary.

But regardless of sector, the principles of good systems engineering dictate that operators of CNI should give due consideration to the continued operation of their systems in the event of a GNSS failure.

Recommendation 6
CNI operators should make provision – with guidance from NCSC and CPNI – for the loss of GNSS by employing GNSS-independent back-up systems.

Improving resilience

Although it is important to understand the limitations of satellites and their signals, this is only part of the story. Attention should also be paid to ground-based assets. A number of threats can be mitigated through best practice.

Stationary receivers are more vulnerable than mobile receivers because they are more likely to be exposed to interference and for longer. Users can minimise many instances of interference with careful positioning of receiver antennas – beyond line of sight from the ground, with a full view of the sky and away from roads.

The quality of GNSS receivers is highly variable, both in hardware and software. At the bottom end are mass-market components, common in mobile devices, which can easily fall prey to every variety of natural, accidental or deliberate interference, as well as to cyber-attack. By contrast, high-quality receivers used in professional and military applications feature software that checks the veracity of signals. Good quality hardware and diligent cyber hygiene can mitigate against spoofing.

With GNSS so frequently engineered into components for timing purposes to avoid the added cost of holdover oscillators, it is often difficult for users and operators to know what they are getting by way of accuracy and integrity. As a result, they cannot be certain how their system will react to interference, whether their PNT information can be trusted or whether the system can even tell that it has been compromised.

The UK has a cross-governmental PNT group which works on these issues, but its impact on policy has been limited. There has been insufficient attention among policy makers to ensuring resilient PNT for CNI, whether that is current or anticipated.

Recommendation 7
The existing cross-government working group on PNT should be put on a formal footing to monitor and identify ways to improve national resilience. It should report to the Cabinet Office, which can coordinate necessary actions among departments.

Agreed standards promote innovation and resilience, and grow markets in such areas as testing of PNT delivery systems. They enable critical service users to define their needs and providers to specify what they are capable of delivering.

Recommendation 8a
Procurers of GNSS equipment and services for CNI applications – with guidance from the relevant lead government department and organisations such as NCSC and CPNI – should specify consistent requirements encompassing GNSS and PNT system issues of accuracy, integrity, availability and continuity, as well as requirements specific to the immediate equipment, system and application.

A number of government departments are already or are likely to become customers for GNSS-based services and associated equipment. There should be a coordinated approach across government to make procurement and assurance coherent.

Recommendation 8b
Government should ensure that, for GNSS and PNT equipment, a coordinated approach is taken to performance standards, terminology, validation criteria, independent testing and evaluation procedures, and the accreditation of test facilities. It should work with industry, trade associations, accreditation bodies and organisations that develop and set standards.

Poorly implemented legislation, regulation and standards can damage a market, introduce costs and harm competition. In the event of legislation or regulation being needed to make critical services dependent on GNSS more resilient, government should again ensure that anything introduced in one sector is consistent with what is being done elsewhere.

Recommendation 8c
Government should adopt a facilitating role to ensure that legislation and regulations relevant to PNT and GNSS are appropriate and proportionate, and that due consideration is given to the needs of different sectors.

The UK has strengths in testing and validation of PNT equipment, as well as the design and manufacture of jamming protection systems.

Recommendation 9
The Department for Business, Energy and Industrial Strategy, in partnership with Innovate UK and the cross-government working group on PNT, should map PNT testing facilities and explore how industry and critical services can better access them.

Preparing for the future

Dependence on GNSS is a dynamic situation, not just because of evolving vulnerabilities and threats but also because of the rapid evolution in applications. Timing-dependent services will increase in number, with greater demands for accuracy, availability, continuity and integrity.

To realise the benefits of intelligent and efficient balancing of power generation with customer demand, for instance, smart grids will require much more precise time synchronisation than conventional grid systems – in the order of nanoseconds[13].

In clearing the electromagnetic spectrum to prepare for 5G, there is pressure on broadcasting systems to move from multi-frequency networks to much more precise single-frequency networks. In doing so, broadcasting is becoming increasingly dependent on GNSS for accurate timing and frequency references.

5G networks will themselves be moving more data, faster, and so will be increasingly dependent on precise timing and synchronisation. Given the scale of infrastructure required in an evolved 5G network, GNSS will likely provide this. In turn, the Government's 5G strategy suggests that autonomous vehicles will use 5G, among other technologies, to negotiate obstacles and communicate with other vehicles.

On the position and navigation side, aviation growth, for example, has been underpinned by a mix of PNT technologies – terrestrial radio-navigation and inertial systems – as well as GNSS, although the level of dependency on GNSS is increasing. This overall trend of using a mix of technologies is expected to continue as other sectors, such as autonomous transport and delivery systems, encounter positioning and navigation needs which cannot be met by GNSS alone.

Global demand already exists for technologies that secure current services and support the development of new applications. UK expertise in GNSS augmentation, anti-jamming, metrology and quantum technologies are illustrative of a range of domestic capabilities necessary for multi-disciplinary research and development in PNT.

Recommendation 10
Growing demand for time and geo-location create opportunities for the UK to leverage its academic and industrial expertise in these areas. UK Research and Innovation should invite the research community and industry to develop proposals to achieve greater coordination among existing centres of excellence.

Chris Whitty
Interim Government Chief Scientific Adviser

Mark Walport
Government Chief Scientific Adviser
(2013–2017)

References

1 London Economics 'The economic impact on the UK of a disruption to GNSS' 2017. Available at https://londoneconomics.co.uk/blog/publication/economic-impact-uk-disruption-gnss/

2 The Department for Culture, Media and Sport has recently consulted on the UK's approach to the European Commission's Network and Information Systems Directive, issued to ensure that operators in key sectors including energy, transport and digital infrastructure are resilient to the growing number of cyber threats.

3 Defined as those facilities, systems, sites, information, people, networks and processes necessary for a country to function and on which daily life depends. In the UK, there are 13 critical national infrastructure sectors: chemicals, civil nuclear, communications, defence, emergency services, energy, finance, food, government, health, space, transport and water. Several sectors have defined sub-sectors. Emergency services for example can be split into police, ambulance, fire services and coast guard.

4 Government Office for Science 'The quantum age: technological opportunities' 2016. Available at https://www.gov.uk/government/publications/quantum-technologies-blackett-review

5 These reviews are named for Patrick Blackett, the Nobel Prize winning physicist, who served as a key military adviser during the Second World War and was a pioneer in operations research.

6 In an engineering context, redundancy involves duplication of critical components or functions in a system to increase its reliability, usually in the form of a backup.

7 Royal Academy of Engineering 'Global Navigation Space Systems: Reliance and Vulnerabilities' 2011. Available at http://www.raeng.org.uk/publications/reports/global-navigation-space-systems; London Economics 'The economic impact on the UK of a disruption to GNSS' 2017. Available at https://londoneconomics.co.uk/blog/publication/economic-impact-uk-disruption-gnss; US Department of Homeland Security 'National Risk Estimate: risks to U.S. critical infrastructure from Global Positioning System disruptions' 2015. Available at https://rntfnd.org/wp-content/uploads/DHS-National-Risk-Estimate-GPS-Disruptions.pdf; Li-Baboud Y and others 'Timing Challenges in the Smart Grid' US National Institute of Standards and Technology 2017. Available at https://www.nist.gov/publications/timing-challenges-smart-grid

8 Ofcom 'Space Spectrum' 2017. Available at www.ofcom.org.uk/__data/assets/pdf_file/0030/96735/Statement-Space-Spectrum.pdf

9 The Carrington Event of 1859 was an exceptionally powerful geomagnetic storm.

10 London Economics 'The economic impact on the UK of a disruption to GNSS' 2017. Available at https://londoneconomics.co.uk/blog/publication/economic-impact-uk-disruption-gnss/

11 Hambling D 'Ships fooled in GPS spoofing attack suggest Russian cyberweapon' New Scientist 2017. Available at www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon

12 The Government recently stated in the Brexit White Paper that the UK has played a major role in developing the EU space programmes Galileo and Copernicus thus far, and that it would welcome agreement to continue to collaborate with its European partners on major science, research and technology initiatives.

13 Li-Baboud Y and others 'Timing Challenges in the Smart Grid' US National Institute of Standards and Technology 2017. Available at https://www.nist.gov/publications/timing-challenges-smart-grid

Chapter 1: Overview

Global navigation satellite systems have made precise positioning and atomic-accuracy time ubiquitous. The smartphone revolution is visible to all, but behind the scenes there has been a similar revolution in professional electronics. Computer networks, communications and broadcast systems rely on GNSS.

This has happened with little thought being given to what happens if the satellite system fails. The military originators of GNSS were well aware of its vulnerabilities and ensured that they did not become critically dependent on it, but the consumer and professional use of GNSS has grown unfettered by such concerns, with the result that we now have a critical dependence on GNSS.

Radio ranging

Within a decade of the invention of radio, mariners and aviators were using it to obtain bearings. By 1945 it became possible to accurately measure distance as well as direction. For example the Decca system, developed for the D-Day landings, created a stable pattern of signals giving a position accurate to within a few hundred metres. Over the following decades there was a heavy investment in radio navigation infrastructure, notably the LORAN (LOng RAnge Navigation) system, enabling the establishment of a network of international airways and greatly improved navigation at sea.

From Sputnik to GPS

Within days of the launch of Sputnik in 1957, American scientists were tracking it by monitoring the radio signals it broadcast. Once the orbit was known, they found they could use the same signals to fix their own position. Within a few years they had created TRANSIT, the first GNSS. The TRANSIT system used a constellation of satellites transmitting very stable signals, based on onboard clocks. By observing the apparent change in frequency of successive passing satellites (the Doppler shift), a stationary or slow-moving receiver could determine its 2D position to within tens of metres.

During the 1960s the USA continued to develop satellite navigation for its submarines, long-range bombers and ICBMs. To provide 3D navigation for fast moving vehicles, better clocks were needed, and in 1967 the US Navy Timation project tested the feasibility of atomic clocks in space. A proliferation of US Navy and Airforce projects followed until, by 1973, rising costs forced the decision to create a single system.

This became known as the Global Positioning System (GPS). By 1994 the GPS constellation of 24 orbiting satellites was complete. The project had cost more than $5 billion. Maintaining the constellation requires the continuous procurement and launch of satellites, and by 2016 there had been 72 satellite launches. Users typically achieve accuracies of a few metres.

Initially GPS was a military system giving civil users access to degraded services – accuracy of a few tens of metres – but after Korean Airlines Flight 007 was lost in 1983 because of a navigation error, Ronald Reagan signed an executive order allowing the civilian use of GPS. In 2000 the “selective availability” that degraded the civil use was turned off, giving civil users an accuracy of a few metres.

An unforeseen consequence was that the move highlighted US dominance in the field. The USSR had developed its own system, GLONASS, but that was not maintained effectively after the Soviet era. Other nations also saw a need to have their own systems as a matter of sovereignty. The existing international coordination of frequencies made it easy for receivers to be multi-constellation: making use of all available signals.

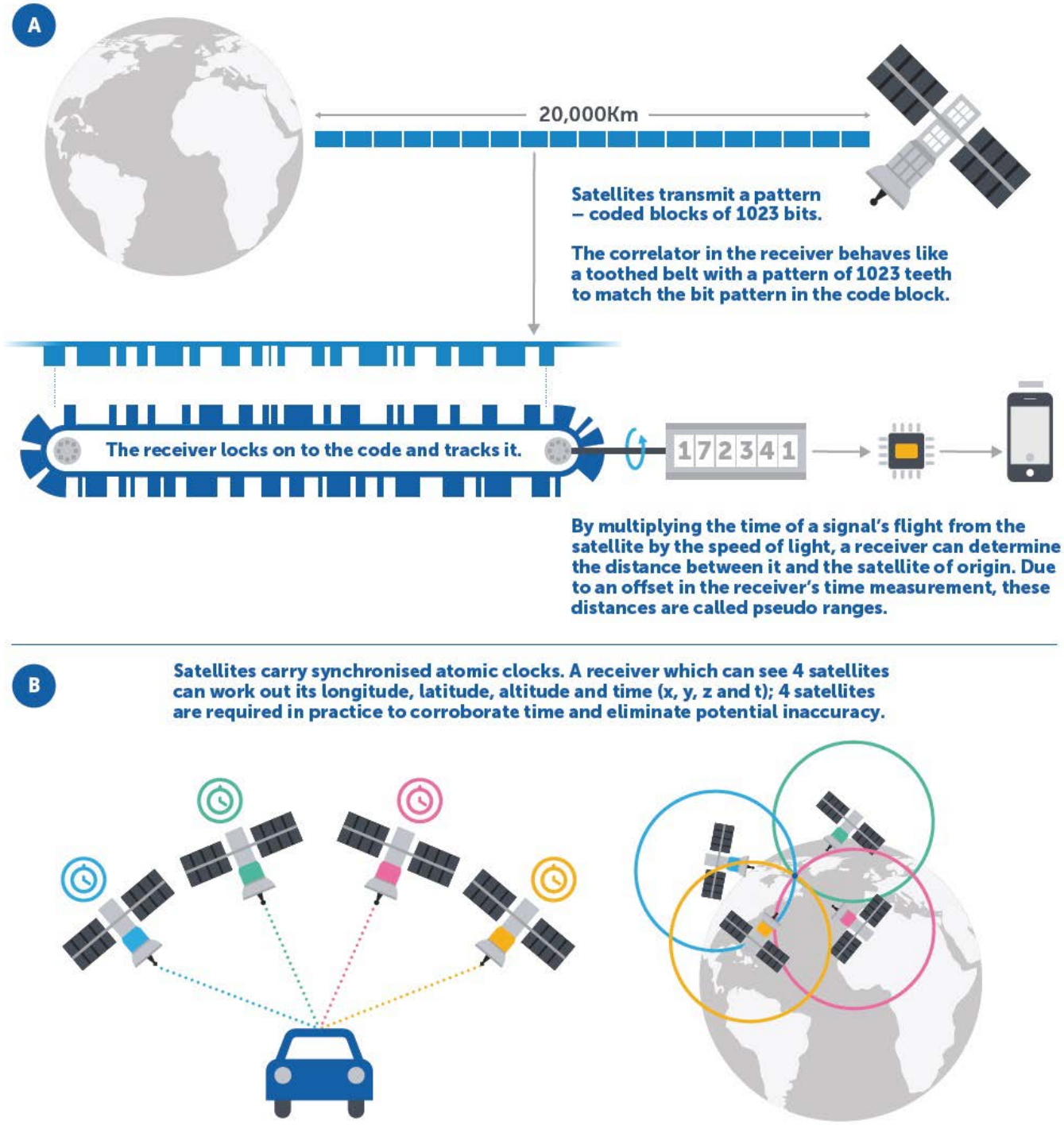
The designers of GPS chose high frequencies requiring only small antennas and digital signal structures that enabled receivers to be miniaturised, so today they have become ubiquitous in smartphones. By 2020 it is estimated that 80% of the world's adult population will have access to a smart phone and so access to GNSS.

How it works

All GNSS satellites in a constellation carry atomic clocks that are synchronised to UTC by the network's ground stations. A receiver measures the time of arrival of satellite signals, and because radio waves travel at a known speed (the speed of light) the time of arrival indicates the distance between satellite and receiver. Light travels a metre in about three nanoseconds (billionths of a second), so to fix a position to within a hundred metres requires time measurement accuracy to within three hundred nanoseconds.

The receiver needs to calculate four things: latitude, longitude, altitude and time. This can be done if it can see at least four satellites, as there is only one position and time for which all four signals make sense (Figure 1.1).

Figure 1.1
GNSS time and position work a little like a toothed belt. GNSS satellites do not transmit single timing pulses but instead spread the pulse over a coded sequence of 1023 bits, each bit forming a tooth in the belt. As well as timing, information about the satellite's position is also encoded in the signal. All GNSS satellites transmit on top of each other but they each have unique codes, and the receiver's ability to track these blocks of bits means it can extract time from very weak signals (weaker than background noise, in fact). It also enables GNSS satellites to transmit on the same frequency, each using a different code, to conserve radio spectrum. If the receiver can see four or more satellites, there is only one position and time for which these measurements together make sense and a fix can be obtained.



Time and space

How accurate is GNSS? The crudest GNSS timing devices can achieve microsecond-level timing. Scientific applications of high-grade GNSS receivers are accurate below one nanosecond. A smartphone operating under normal conditions can determine its position to within 10 to 20 metres or better. At the other end of the scale are high-quality devices such as NASA's space-based Blackjack receiver. This has been used to calculate the orbit of the Jason-1 spacecraft to a radial accuracy of better than 10 millimetres.

How it is used

GNSS is used for position, navigation and timing (PNT):

- *Position.* A surveyor may want an accuracy of less than a centimetre; a hill walker would be content with several tens of metres. Both will want the information in a form they can use and share, consistent with maps and charts using the same coordinate system.
- *Navigation.* Early GNSS receivers provided a position, and the user – using a paper map – had to determine how to get to the destination. Now this navigation function might be carried out by a smartphone with in-built digital maps and access to traffic information. GNSS provides the position, speed and direction of travel.
- *Timing.* A GNSS receiver costing tens of pounds can do the job of an atomic clock costing tens of thousands of pounds. That is why GNSS time signals have become an essential part of communications networks, broadcast and financial systems – for example in timestamping data records or in enabling two communications systems to stay in step.

Users' underlying need is for PNT services, not GNSS specifically – but the ubiquity and low cost of GNSS has expanded the market for these services. This market is evolving, as technologies make new applications feasible. In the future, position and navigation needs will be dictated not only by humans but by automatic systems such as driverless cars.

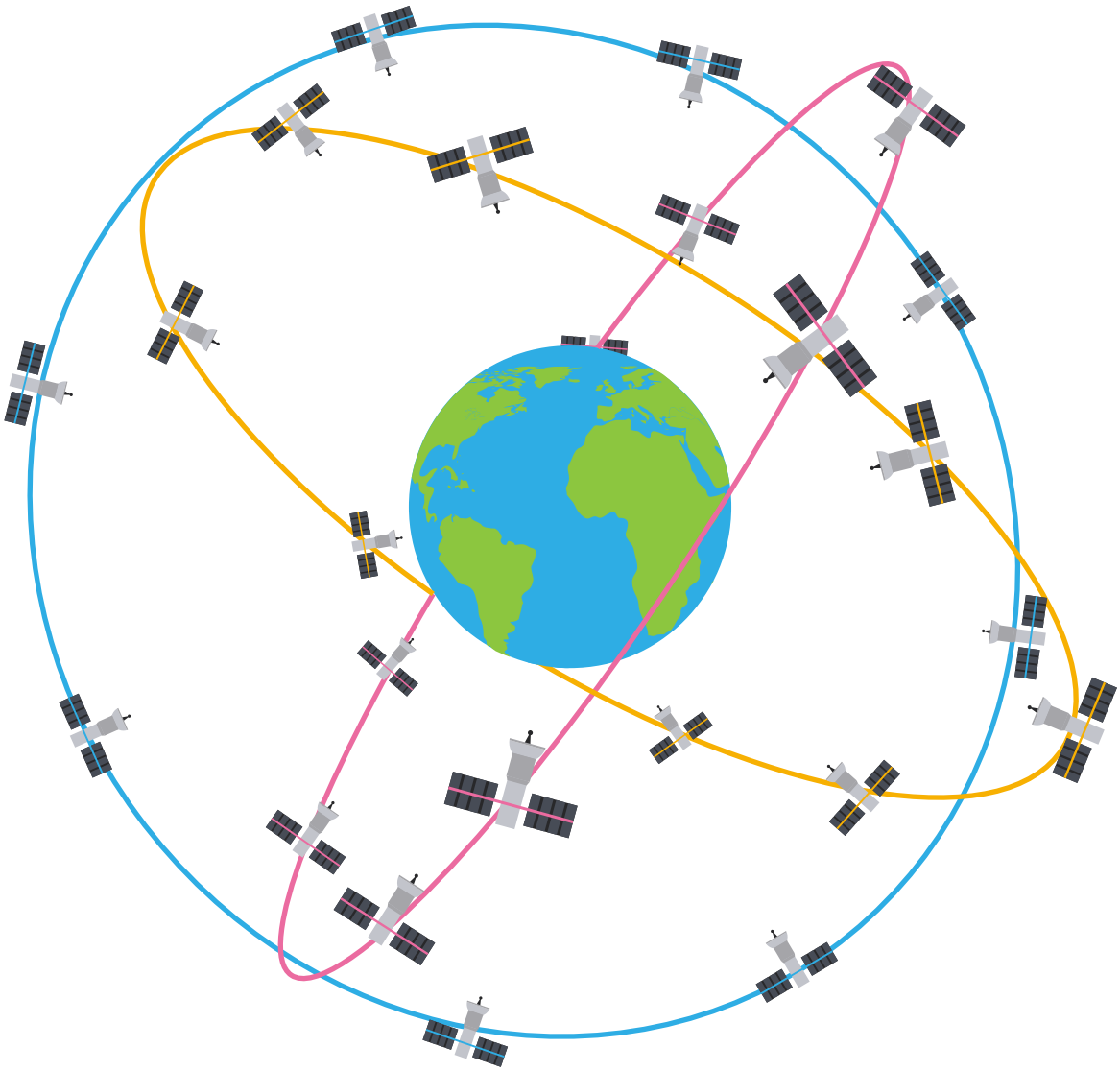
Timing applications are evolving too. GNSS not only provides an accurate time of day for timestamping but an atomic tick that is very stable over long periods. This can be used to keep communication systems and information systems synchronised, as well as providing a frequency reference for radio systems. The drive to transmit larger amounts of data and the growth of high-frequency financial trading is increasing our dependence on the atomic tick of GNSS.

Constellations

Communications satellites are placed in geostationary orbits 36,000 km above the equator, where they orbit in step with the Earth's rotation and so appear motionless in the sky. However, geostationary satellites are not visible in polar regions, so to give global coverage GNSS satellites are put in inclined orbits at lower altitudes (typically around 20,000 km). Constellations of these satellites are designed to ensure that a user can see enough at any time to be able to fix a position.

There are now two GNSS constellations in operation and two nearing completion. GPS has 27 satellites on six orbital planes, while Russia's GLONASS has 24. Europe's new Galileo system is expected to be complete by 2020, when it will have 30 satellites (including six spares), as in Figure 1.2. The Chinese BeiDou system will extend to 35 satellites.

Figure 1.2
The satellites of the Galileo constellation will be strung out along three inclined orbits at an altitude of 23,222 kilometres. Each satellite will take about 14 hours to orbit the earth.



Each constellation may transmit in more than one frequency band. GPS has bands known as L1 (1575.42 megahertz) and L2 (1227.60 megahertz), among others.

Even before these constellations are complete, receivers will be making use of the additional satellites. Modern GNSS receivers are designed to listen out for every satellite their software knows about. A multi-constellation receiver today will already be using far more than 30 satellites at any one time. This has had some impact on the accuracy of the position solution. More noticeably, it has improved the performance of GNSS in cities, where satellites can be obscured by tall buildings. It has also made the system more fault tolerant and has enabled receiver designers to improve the integrity of the system.

Galileo vs GPS

The designers of Galileo have had the benefit of almost 40 years of GNSS experience, and have endeavoured to design a new system without some of the known deficiencies of GPS and GLONASS.

Galileo will offer an encrypted navigation service for applications that require higher immunity to disruption. But the fundamental design constraints are unchanged. Satellites have limited power and the received signals are weak, so Galileo suffers from many of the same vulnerabilities as GPS. It should also be noted that GPS has not stood still, the replacement of satellites and upgrade of ground elements having provided opportunities for technology insertion and improved performance.

Augmentation

Ordinary GNSS has several shortcomings. Variations in Earth's ionosphere can delay the radio signals in an unpredictable way, which creates uncertainties of several metres in GNSS positions. Other problems affect integrity and reliability. A multitude of systems and people are needed to keep the overall system accurate and usable, resulting in a system of great complexity prone to human error and cyber-attack. In cities, buildings can block or reflect GNSS signals. Space weather can disable satellites.

Many of these problems can be addressed using methods that augment basic GNSS. Multi-frequency receivers, for example, correct errors from the ionosphere. They measure ranges on two different frequencies, and because the atmospheric delay is different on each frequency, they can calculate its size and compensate accordingly.

Augmentation uses additional receivers to compare signals. These can check for consistency, to provide warnings of errors and failures to users needing high-integrity solutions. They can also correct errors, to provide improved accuracy, using the technique of differential GNSS.

In the simplest form of differential GNSS, a monitor station measures the difference between its known, fixed position and the position given by GNSS, and transmits this error correction to a nearby user on a radio link. These corrections are most accurate if the monitor and user are making measurements through the same piece of atmosphere, and can give positional accuracy down to about one metre. Some of these networks are ground-based augmentation systems (GBAS). Others use monitor stations spread over a wider area and provide users with accuracy and integrity information via satellite, and so are known as satellite-based augmentation systems (SBAS).

Even higher accuracy can be achieved by the real time kinematic (RTK) technique. This extends differential GNSS with sophisticated receivers that can lock on to the satellite carrier signal, which has a wavelength of about 20 cm. By measuring the phase of this wave, RTK can provide accuracy down to a few centimetres or even millimetres.

Precise point positioning (PPP) is a similar technique that compensates for errors created by the lower atmosphere as well as those from the ionosphere, and also for errors in satellite clocks and orbits. It even allows for the effect of tides. Unlike RTK it does not require a nearby

reference station, as corrections are calculated using a widely scattered network of stations. PPP reaches accuracies of about 10 cm.

Measures of performance

Anyone wanting to use GNSS for a specific task will need to know:

How accurate is it?
Accuracy is the largest error one would see between what the receiver is displaying (position and time) and the true value.

Is the GNSS receiver misleading me?
Integrity is a matter of confidence in the displayed position or time. The equipment should raise an alarm if the error in what is displayed exceeds an acceptable level (known as the alert limit). For critical applications the risk of the equipment failing to raise an alarm is an important consideration. This is termed integrity risk: the probability that at any moment the measurement error exceeds the acceptable level without an alarm.

Will it be there when I need it?
Availability is affected by many factors: the reliability of the equipment; geography and where the signals can be heard; and the logistics of maintaining and replenishing parts of the system including the satellites.

Can I finish the job I have started?
Continuity is the probability that a task can be completed without GNSS dropping out.

How quickly does it tell me if something is wrong?
Time to alert is the maximum interval before the user is warned of a performance problem.

It is easy to become obsessed with accuracy and neglect other factors. While the accuracy of a clock or other instrument usually reflects its overall quality, that is not so for GNSS. With low-cost GNSS chipsets it is possible to make products of amazingly high accuracy but overall poor quality.

So users must specify fit-for-purpose products, not just accurate ones, with requirements for integrity and the other measures above. Specific products and applications may have other requirements, such as working temperature range. An essential measure of performance for a clock is stability, which is how quickly the output frequency drifts up and down. With GNSS it is possible to create an accurate clock with poor stability: the high accuracy is achieved by averaging the wavering clock output over a long period.

Whispering satellites

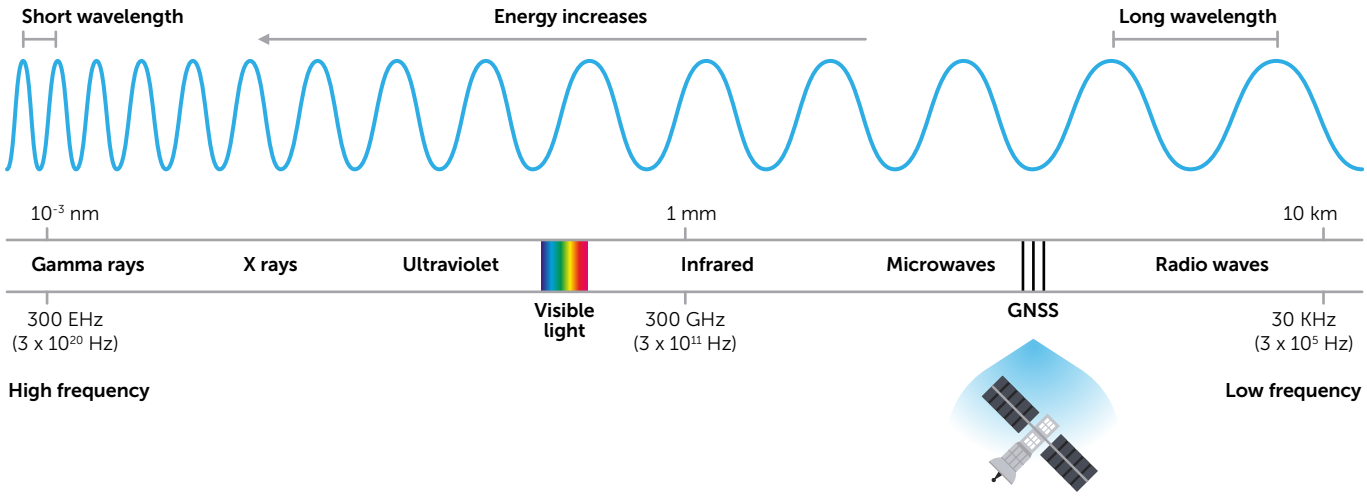
Power is scarce on a satellite, and signals must be broadcast to users across the globe, precluding the use of highly directional antennas. This means that the signal received on the ground is very faint. What is more, satellite whisper must compete with terrestrial noise.

In the 1970s few other systems operated at the high frequencies chosen for GNSS. Today this is not the case, and accidental interference is more common, as is deliberate interference (jamming). Van drivers, disgruntled with their employers tracking their whereabouts, have been known to use jammers, while criminals jam the trackers protecting luxury cars (see Keyless

Car Theft). With such weak signals, even relatively unsophisticated jammers can render GNSS unavailable.

From the outset GPS was designed to be part of an augmented or hybrid system. Military users expected signals to be interfered with and incorporated backup systems to cope with GPS outages. However, GNSS systems have proven so reliable we have become dependent on them. Given the vulnerabilities of GNSS, it is becoming clear that many users require alternative, more resilient sources of PNT.

Figure 1.3
GNSS signals are transmitted in the microwave band. Their specific frequencies are chosen so that they are not absorbed by Earth's atmosphere, but they cannot penetrate buildings, heavy forest canopies or the surface of the oceans. Because the signals are so weak on reaching the Earth, they can be overpowered by spillover from terrestrial transmissions at neighbouring frequencies. In 2004, the US Federal Communications Commission proposed to licence frequencies adjacent to GNSS to communications company LightSquared (now Ligado Networks). When tested in 2011, their mobile signals overpowered GNSS signals.



Keyless car theft

In the past few years, a new kind of car theft has been reported. A driver might park at a motorway service station to stop for a coffee. Returning to their car 20 minutes later, they find it gone. If the car is recovered, there is no sign of forced entry. How can this be?

The answer is a new kind of jammer. Built into smart leather briefcases, these are much more sophisticated and capable than earlier types of jammer, which were mainly used as personal privacy devices by fleet drivers. They cover many different bands. In an 8-channel jammer, for example, three channels are dedicated to GNSS bands; three to the frequencies of key fobs used to lock and unlock car doors; one to the frequency used by hidden tracker devices; and the last to the Bluetooth frequency, which is often used for car park CCTV communications.

The thief wanders around the car park with their briefcase. Spotting a likely target car, they activate the jammer. The driver is unaware that their key fob has not locked the doors. Having got into the car, the thief connects to the onboard diagnostic box and clones the car's key within seconds. Onboard GNSS is then jammed, so the car cannot be tracked as the thief drives it away.

These briefcase jammers, readily available over the internet, make keyless car theft an easy task. So much so that insurance underwriters are refusing to cover some cars because they feature keyless entry and start technology.

What the thief probably does not realise — and does not care about — is that they may be disrupting signals in an area hundreds of metres across. Because these devices transmit at high power, up to three watts, they can easily wipe out GNSS signals, as well as the police communications band (TETRA) and future emergency services bands.

Applications

Today there is a bewildering plethora of applications that use GNSS, ranging from entertainment through to critical infrastructure (Table 1.1 and Figure 1.4).

Mass-market applications of GNSS number in the hundreds and the users in billions. The two main areas are smartphone and in-car navigation applications, based on low-power, limited-functionality chipsets. Professional applications usually involve more sophisticated equipment with high-accuracy outputs, such as surveying equipment and the timing devices used in finance. Safety-critical applications such as aircraft landing systems and rail signalling require the greatest level of resilience.

GNSS applications are pervasive, deeply embedded, critical and dynamic.

- *Pervasive.* We are surrounded by them even though we may not realise they are there. Generations ago, human beings became accustomed to wearing wristwatches and keeping clocks in their houses. People came to rely on time as a fundamental component of the world's infrastructure. In a similar way we are now coming to rely on GNSS.

- *Embedded.* Their role in a technology or service is often far from obvious, so users rely on the technology without understanding or recognising its dependency. The GNSS chipset in a smart phone is capable of measuring the range to orbiting space vehicles that are around 20,000 kilometres away and moving at four kilometres per second, but to a user, the difficult part of positioning and navigation may be squinting at a smartphone screen under reflective glare.

- *Critical.* The role played by GNSS can be fundamental to the operating concept. If the GNSS component fails, then the system may fail completely. In its infancy, satellite-based PNT was a value-added technology that lent itself to making existing processes more efficient. That has all changed now, as GNSS has become an enabling technology without which many high-tech capabilities would be impossible.

- *Dynamic.* The application domain is not static. New ideas and technologies emerge continually. Key areas include autonomous vehicles, space traffic management and vehicle usage and taxation.

Table 1.1 | Some of the vast range of applications that already use GNSS for timing, position and navigation

Timing (T)

Commercial & civilian
Telecoms
Wireless communications networks
DAB & DTV synchronisation
Railway sensor timing
Financial transactions
Automated Teller Machines
Sub-atomic particle experiments
UTC time transfer
Earthquake seismology event timing
Power grid synchronisation & maintenance

Military
Radar time synchronisation
Communications synchronisation

Position (P)

Legal & enforcement
Fisheries protection & vessel tracking
Border disputes
Environmental protection
Prisoner tracking
Road tolls

Security & tracking
Asset & fleet tracking
Child protection
Theft prevention
Geo-fencing
Prisoner tagging
Tracking & control of hazardous substances

Transport services
Buses
Taxis & cabs
Car insurance pricing

Leisure & entertainment
Photo geocoding
Social networking
Gaming

Precision agriculture
Tractors & combine harvesters
Smart fertilisation

Marine
Hydrographic surveying
Cable laying
Collision avoidance (Suez, Panama canals)
Marine AIS (automatic identification systems)
GPS buoys
ECDIS (electronic chart display & information systems)
Harbour operations, port automation
Container tracking
Dredging
Trawler monitoring of net snagging
Vessel attitude & heading

Aviation
Emergency Locator Transmitters
Air traffic control

Military
Command & control
Battlespace management
Mine warfare
Target acquisition & tracking

Civil Engineering
Grading (earthworks)
Road & construction control
Deformation monitoring & subsidence
Bridges & dams

Surveying & mapping
Geographic information systems
Map production
Topographic survey & setting out

Scientific applications
Earthquake magnitude estimation
Plate tectonics
Meteorology
Space vehicle orbit determination
Space weather (derived ionosphere activity)
GNSS reflectometry & occultation

Navigation (N)

Leisure & entertainment
Geocaching, cycling, hiking
Fishing using GPS
Gaming

Space vehicles
Launch & orbit injection
Trajectory control
Rendezvous & docking
Space-based augmentation systems

Car & pedestrian navigation
SatNavs, smartphones
Smart watches
Aids for visually impaired
Road lane identification

Air
Take off, landing, taxiing
Flight path control, air space management & collision avoidance
Ground-based augmentation systems
Space-based augmentation systems
Drones

Marine
Harbour operations
Inland waterway & coastal navigation
Dredging

Emergency Services
Police, fire brigade, ambulance
Coastguard, lifeboats
Civilian search & rescue

Military
Precision ordnance
Command & control
Battlespace management
Night operations, reconnaissance
Parachute & equipment drops
Combat search & rescue
Aircraft approach & landing
Drone operations

Table 1.2 | New technologies will only increase our reliance on GNSS

Emerging Applications

New telecoms: 5G
Smart intersections
Internet of Things
Autonomous vehicles
Vehicle usage & taxation
CubeSats
Next generation air traffic control
Space traffic management
Commercial guaranteed service level
Next generation regional augmentation systems
Phased array satellite transmissions
Geostationary orbit positioning using GNSS side lobes
Signal integrity
Jamming & interference resilient PNT

Figure 1.4 | GNSS now pervades our society

Critical national infrastructure

Communications. Most applications here use GNSS for timing, synchronisation and provision of reference frequencies. They include fixed line telecoms (including internet provision), cellular telecoms, broadcast digital video and audio, internet data centres and wireless communication networks.

Emergency services. There are two main applications: using GNSS data from a caller's phone to locate the emergency; and navigating there rapidly and successfully.

Energy. GNSS supports the transmission of electricity across the country through the National Grid. The requirement is for time synchronisation.

Finance. Financial transactions, often driven by algorithmic trading, require timestamps at millisecond to microsecond level. This form of precision timing also requires traceability for audit purposes. Time derived from GNSS can be used for synchronisation and made traceable as a source for timestamping.

Food. Precision agriculture enables dramatic improvements in yield, but the main dependency at the national level is that of just-in-time supply chains.

Transport. Road, rail, air and marine transport all rely heavily on GNSS. In turn, the country as a whole relies on the distribution and travel networks enabled by these sectors.

Emerging applications

Although hardly in their infancy, GNSS applications are still developing (Table 1.2). On the road there are developments in autonomous vehicles, smart intersections, vehicle usage and taxation; in the air, next generation air traffic control and drone applications. High-altitude, long-endurance aircraft, which may form a key service provider in internet signals, require GNSS. In space, the huge proliferation of satellite launches necessitates space traffic management, and the only proven technology to support that in positioning and navigation is GNSS. The Internet of Things depends fundamentally on knowledge of location supported by GNSS.

Systems of systems

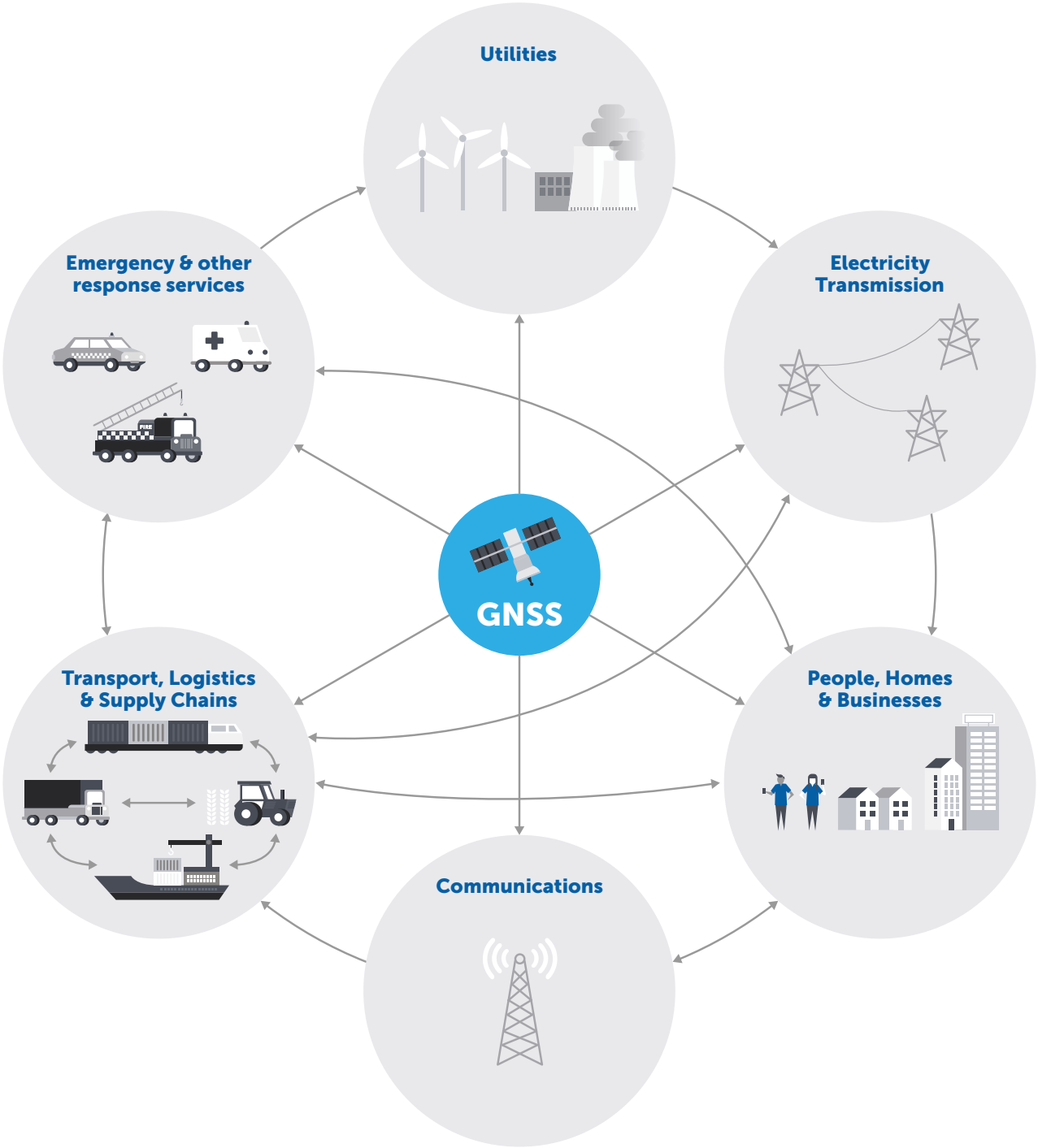
Because GNSS applications are so pervasive, they occur in many systems that depend on one another (Figure 1.5). Consider the electricity system that powers our homes, businesses and practically all modern services. Accurate time from GNSS receivers allows the grid to determine if there is a fault, where it is and where to employ circuit breakers. In turn, the grid powers our communications systems, which themselves use time from GNSS to operate.

Transport weaves another web of dependence. Trains, planes, ferries, buses and lorries use GNSS to determine their position and to navigate, and use telecoms to report their locations to fleet management systems. Intricate logistics are required to operate the just-in-time supply chain that ferries our food from all over the world, on to our roads and into the shops and ultimately our homes; and every stage, from global to local, relies on GNSS for time or position. When one of these systems fails, invariably the engineers sent to repair the fault will use GNSS to find their way to the site of the problem.

Our vulnerability to GNSS failure is increased because of such systems-of-systems interactions. If a problem with GNSS were to cause a major power outage, our ability to coordinate a

response could be diminished, our capacity for moving people and goods reduced and our emergency responses hampered.

Figure 1.5
The uses of GNSS are linked together to form complex systems of systems



Conclusion

PNT applications are becoming more sophisticated and more deeply embedded in complex automated systems. In a more automated world, with fewer human operators to intervene in the event of a failure, GNSS alone may not prove adequate as a sole source of PNT.

Chapter 2: Threats and Vulnerabilities

All GNSS receivers are vulnerable to natural and man-made interference. They can be easily jammed and open-signal receivers can also be deceived. The impact of these threats can be highly variable, and the impact on GNSS-reliant systems of systems is hard to assess, with only rigorous system analysis providing the complete answer to such questions. As time and position are handled alongside each other in a receiver, the vulnerabilities described in this chapter apply equally to receivers used for timing applications and for position determination.

External threats

Jamming

GNSS signals have such low power that even a weak interference source can cause the receiver to fail or to produce hazardously misleading information[1]. Interfering signals may come from natural sources, malfunctioning electronics or deliberate jamming.

An often quoted means of defending against interference is to use a receiver that can use more than one GNSS constellation or frequency band simultaneously. This may be true for accidental interference, but all GNSS transmit in a single, relatively narrow radio band, so if it is easy to build a small and effective jammer for the L1 band of GPS, it is just as easy to build one for GPS L2, Galileo E6, GLONASS L1 or Beidou B1. Indeed, pocket sized jammers covering all major GNSS frequencies have been openly available over the internet for several years. Owning a GNSS jammer is not illegal in the UK, although its use would break the terms of the Wireless Telegraphy Act (see Jammer legality).

Jammer legality

Under the Wireless and Telegraphy Act (2006) it is an offence to deliberately transmit within the GNSS frequency band without a licence or exemption notice. So the use of jamming devices is an offence – but possession of a device is not. This means that courts have to prove intent to use, which can be difficult.

Jammers are also subject to the Electromagnetic Compatibility Regulations 2006, which specify that electrical and electronic apparatus placed on the market or taken into service in the UK do not cause excessive electromagnetic interference or are adversely affected by it. As jammers by their nature cause considerable electromagnetic interference, it is likely that most do not comply with the regulations and therefore they cannot be legally placed on the UK market. But there is still some uncertainty; and this would not ban ownership, only sale.

For comparison, US federal law prohibits the marketing, sale and use of a transmitter designed to block, jam or interfere with wireless communications. Jammers can only be used by the federal government. Australia also prohibits possession and operation of jammers. Should we make it illegal to own a jammer in the UK?

The last 15 years have seen a dramatic proliferation of GNSS jamming systems: from the preserve of the military, through criminal groups, to the point where jammers are now sought and owned by everyday citizens seeking to hide from a perceived risk of being tracked during their day-to-day lives (see SENTINEL).

SENTINEL

Since 2010 the research platform SENTINEL, run by Chronos Technology, has been monitoring GNSS frequencies for jamming and interference. Its outdoor sensors typically detect several incidents of interference each day. Comparing data from different locations can reveal the likely sources.

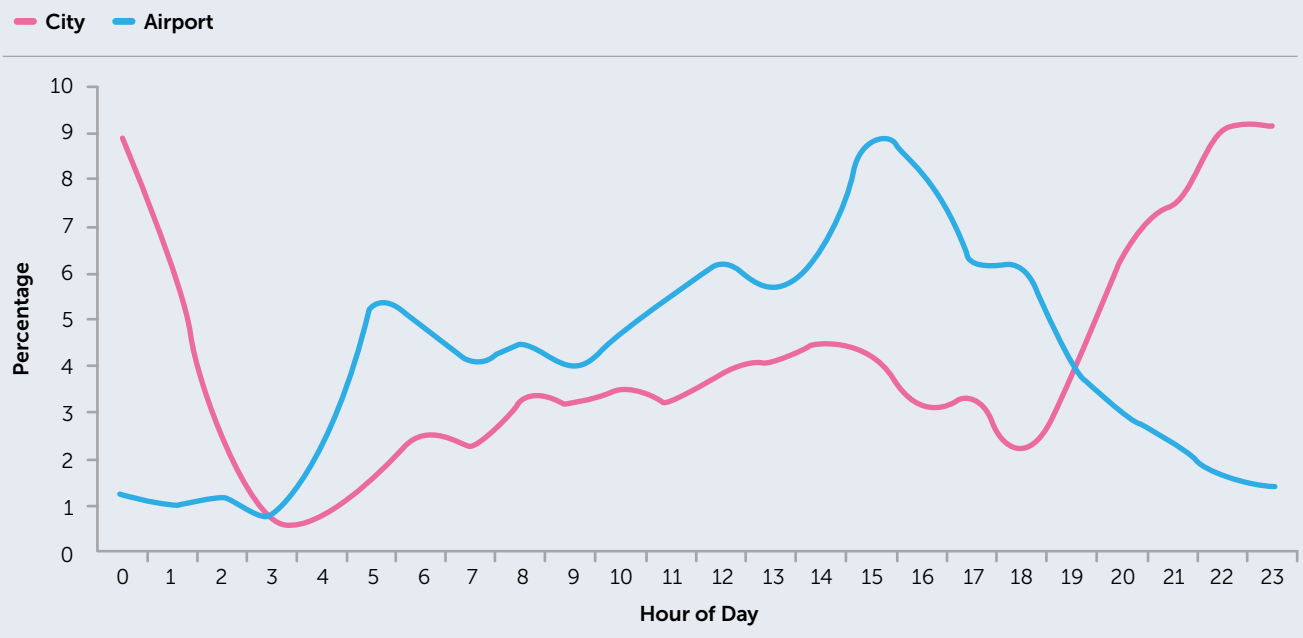
About 20 sensors were deployed originally, and two that gave particularly interesting results were maintained. One is on a building roof in the City of London, where GNSS receivers are used to supply critical timing information to financial organisations and telecoms network providers. The second is by a motorway near a suburban airport, where light aircraft often use GNSS to navigate.

From February 2013 to February 2017, both of these sensors recorded almost the same number of interference events per day (4.6 city, 4.8 airport), but events in the City last four times as long on average. This suggests that the interference is coming from vehicles with jammers: because of slower-moving traffic and the ability to park up in the City, they would naturally remain close to the detector for longer.

The City location also sees fewer events during normal business hours (see graph), probably owing to congestion charges, which reduce traffic between 7am and 6pm, whereas the airport sensor sees an increase during working hours that fits the pattern of normal motorway traffic.

So GNSS interference is happening, and SENTINEL's observations imply that it is caused by in-vehicle jammers. The levels of interference detected mean that GNSS receivers in the vicinity could cease to operate, or operate at diminished levels of accuracy, affecting users and systems that rely on them. The actual impacts on local GNSS users have not been made public knowledge.

Percentage of jamming incidents at different times of day recorded at the City and airport locations.



Spoofing

A more subtle threat stems from the open nature of the GNSS signals used by civilian receivers. The standards defining these signals are published to the world to allow as many manufacturers as possible to build receivers. These same standards can also be used to build devices that generate false signals to deceive or spoof a GNSS receiver into generating an incorrect or inaccurate position and/or time output[2]. The impact of spoofing could vary greatly depending on the nature of the system being attacked.

In the last few years, the advent of small, cheap, software defined radios has put the technology needed to generate spoofing into the hands of hobbyists. At the same time, moves to use GNSS location for activities such as road charging, and the use of location-enabled mobile phones in games such as Pokémon GO, have generated incentives to develop spoofing systems (see Pokémon GO and Ingress).

The threat of spoofing should be considered a game changer – with any open-signal GNSS receiver now being wide open to deliberate manipulation.

Pokémon GO and Ingress

Ingress and Pokémon GO are augmented reality games which overlay computer graphics and real-world scenes using a smart phone's camera and sensors. Ingress, launched in 2013, sets two factions against one another in a global competition to capture "portals". The locations of portals are submitted by players, and are typically places of interest. Every statue, monument or significant public work of art has at least one portal associated with it. Pokémon GO was launched in 2016. The aim is to capture, train and battle creatures called pokémon, which appear on screen as the player moves around in the real world. As of March 2017 Pokémon GO was attracting more than 65 million players each month.

Cheating is rife. Players often appear on the map when there is nobody physically present. Most of these cheats use software to fake a GPS signal, without any external effects. But only days after the game was launched, detailed guides appeared that describe a more worrying method of spoofing Pokémon GO[3]. Using fairly cheap software-defined radios and some simple tools that are now publicly available, the authors were able to move around any location in the world by broadcasting a fake GPS signal, which their phone picked up. If left unshielded, such a signal could affect a large area around the real location of the spoofer.

At present, there is probably little physical spoofing like this, but its low cost and relative ease – and the availability of detailed guides – means that it may become more commonplace.

Niantic Labs have since updated Pokémon GO to ban sudden apparent changes in player locations. This addresses the issue of players randomly spoofing around the globe, but it does not stop more subtle spoofing.

Meaconing

This is a form of deceit similar to spoofing. A meaconing system receives genuine GNSS signals, amplifies them and re-transmits them towards a receiver. If the receiver locks onto this signal, it will show a position corresponding to the meaconing system's receive antenna with a delayed time output.

Meaconing may be accidental. Low-powered repeater systems are commercially available and are used legitimately, under a light-touch Ofcom regulatory framework[4], to send GNSS signals into environments such as aircraft hangars that would otherwise be screened from direct reception. If such a system is installed incorrectly, or if the power level is set too high, the repeated signals can result in interference to other GNSS receivers in the area[5].

Space weather

Changes in the sun's electromagnetic and particle output can affect both satellites and technology on the ground. Geomagnetic storms vary from small to large, and the larger the storm the higher the impact. Superstorms occur every 100-200 years and can have severe consequences for a number of technologies.

For GNSS the main effect is a disturbed ionosphere, which reduces the accuracy of position and timing. These disturbances occur mainly at high and low latitudes and less at mid-latitude locations such as the UK. Generally, the receiver and system architecture can mitigate ionospheric disturbances, for example through the use of multi-frequency receivers (Chapter 4). The effects of ionospheric disturbances are more problematic in high-precision GNSS receivers, but depend on the application. Examples of high-precision systems are augmented GNSS systems for aircraft navigation and landing, such as the US Wide Area Augmentation System (WAAS) and the European Geostationary Navigation Overlay Service (EGNOS). During the large geomagnetic storms in October 2003, vertical navigation guidance was unavailable from WAAS for approximately 30 hours due to ionospheric disruptions. For high-precision systems such as EGNOS and WAAS one or two events would be expected per solar cycle (11 years) at UK latitudes. In the event of a superstorm, the output from many types of receiver would be significantly degraded or even unavailable for up to three days.

Occasionally, brief bursts of radio waves from the sun can jam receivers. The effect of a solar radio burst on GNSS was first seen on 5 December 2006 when there was enough radio energy to interfere with receiver operation for 10 to 20 minutes over the entire sunlit side of the Earth. The December 2006 burst was the largest on record and caused a WAAS loss of vertical guidance for 15 minutes. During a superstorm many solar radio burst blackouts can be expected.

Storms are also associated with a flood of energetic charged particles which can damage or permanently disable GNSS satellites. Every care is taken to design the satellites to withstand this (GPS satellites in particular are hardened) and so far there has been no loss of a GNSS satellite to charged particles. In the event of a superstorm, a reasonable working assumption is the loss of 50% of the satellite fleet, with many subsequently recovered after a few days.

The vulnerability of GNSS systems to extreme space weather events, and the resultant impact on all users of such systems, was detailed by the Royal Academy of Engineering in a 2013 report[6] which notes that the unmitigated loss of GNSS resulting from a superstorm would have severe social and economic repercussions[7].

Receiver vulnerabilities

Receiver makes and models vary enormously in their susceptibility to jamming and interference. This is often not appreciated and is rarely tested before systems are purchased, deployed or integrated. Occasional testing[8] of civilian GPS receivers at the Defence Science and Technical Laboratory (Dstl) has shown that the worst receivers on the market fail when the interference level rises barely above the natural background radio noise. In contrast, the best receivers can offer up to 10 times as much resistance to interference. This variability is seen across all market sectors, from the cheapest hiker's handheld receiver to top-end professional timing systems. Price may not be a good determinant of performance in this case.

Testing at Dstl has also shown that when jammed, only a few receivers cleanly stop producing position and/or time solutions and provide a warning to the user of what is happening. Many others produce erroneous position and velocity outputs in response to simple jamming without properly warning either the operator or connected systems (see Chaos on the bridge, below). Again, this has been seen in many types of receiver across many price points.

When spoofed, some receivers may stop working altogether. Researchers at Carnegie Mellon University simulated a spoofing attack that made the receiver believe that GPS satellites were all at the centre of the Earth[9]. This resulted in a major software failure within the receiver, causing it to stop working. Such a failure may require a complete reset to factory default settings, a procedure that may not be readily available to the operators of many embedded receivers. As receiver design and manufacture is essentially an uncontrolled and unregulated worldwide industry, it cannot be ruled out that such vulnerabilities are deliberately inserted into receivers at manufacture.

The manufacture, selection and integration of GNSS receivers are essentially unregulated in many sectors (Chapter 5). Regulations do exist to ensure they do not interfere with other nearby radio receivers, but not to ensure the robustness and resilience of the GNSS receivers themselves. Instead, the vulnerability of a receiver is left to the user to determine. This can require rigorous and very long-winded testing for each individual receiver make, model and software version. No comprehensive database of such vulnerabilities exists and no large scale commercial testing service is readily available. A widespread testing programme is unlikely to be practical for all but the most critical applications — and as yet the UK has no requirement to test GNSS receivers before integration in many critical applications.

Chaos on the bridge

The effect of GPS jamming on a ship can be dramatic. During a test in 2009 on board the Trinity House vessel Galatea, a tiny jammer with less than one thousandth of the power of a mobile phone caused the electronic chart displays to show false positions. As a result, the autopilot steered the ship quietly off course. The automatic identification system reported those incorrect positions to other ships manoeuvring nearby and to the vessel traffic service ashore. The jammer also caused the satellite communications system to fail. The ship lost its distress safety system, there to raise alarms and guide rescuers. The helicopter deck stabilisation failed. Even the ship's clocks went wrong. And the usually reliable fallbacks, radar and gyrocompass, both gave warnings, as they too use GPS inputs.

Many vessels now have tens of GPS receivers that may all fail together when a jammer signal appears, often raising audible alarms. A ship's officer is faced with multiple simultaneous failures. The alarms cannot identify GPS jamming, so the cause is unknown. There is a conflict between dealing with this cacophony of alarms and suddenly switching to old-fashioned, non-satellite means of navigating the vessel. In low visibility or at night that is not possible without a well-prepared navigation team.

A backup to GNSS solves these problems. Galatea was later equipped to switch automatically and seamlessly to eLoran navigation and timing when GNSS failed.

Other risks

Leap seconds

The time standards used to synchronise most GNSS signals are continuous, whereas the UTC time standard, which forms the basis of most clocks used in society, has occasional leap seconds inserted to adjust for fine differences between the slowing rotation of the Earth and our rigid 24-hour definition of a day. When a leap second occurs, the time output of a GNSS receiver will appear to have an extra second inserted. Some systems reliant on this GNSS-derived time may not have been programmed to understand the concept of a leap second. This can result in failure or incorrect operation in the reliant system. Receiver operation through and after a leap second can be easily tested using a GNSS signal simulator system.

Week-number rollovers

The data messages used to transfer current date and time from the satellites to the GNSS receiver have data fields of limited length. These fields will eventually reset from their maximum value back to their minimum, which can result in the date generated by a poorly programmed receiver appearing to be offset from truth by 1023 weeks, or nearly 20 years, in the specific case of GPS. The next GPS week-number rollover is due on 6 April 2019. Receiver operation through and after a week-number rollover can also be easily tested using a GNSS signal simulator system.

Withdrawal of service

For all GNSS, there is some risk that the nation or entity operating the satellites will either cease to maintain the constellation or actively switch off all open signals used by civilian receivers. The risk is reduced by international commitments to provide open services, but the possibility of such a withdrawal (for example under extreme financial pressures) cannot be ruled out.

Deliberate reduction of signal accuracy

In the early days of GPS, the accuracy available from open-signal civilian receivers was deliberately degraded to around 100 metres. The US government has stated[10] that the next-generation GPS satellites, which will begin launching from 2018, will not have this ability to degrade signals. It is not known whether other GNSS constellations include such features as reserved modes. Again, international commitments to maintain GNSS provision should mean that this risk is low.

Cyber-attack

A successful cyber-attack on the systems used to control the satellites, or on the signals between the control systems and the satellites, could result in severe disruption and possibly

lasting damage to the satellites and hence to the operation of GNSS. Receivers that take and use signals from many different GNSS constellations could be resilient to such an attack on one constellation if they have been programmed to anticipate a system corruption of this type. Dstl testing of these multi-system GNSS receivers has shown wide variability in response to diverging position and time solutions between constellations. Some receivers will bias their outputs to one preferred constellation, some will produce a solution midway between, and a few will try to identify and isolate the faulty signals.

Satellite errors and failures

While each GNSS operator monitors the health and transmission quality of its satellites, it can take some time, possibly up to many tens of minutes, before an error is corrected or the satellite is taken out of service. Errors in the data transmitted by the satellites are another risk (see A glitch in time).

A glitch in time

At 2am on 26 January 2016, hundreds of timing equipment alarms went off in a UK telecom operator's national control centre. Unacknowledged alarms were each sending out more alarms demanding attention.

We now know that an error of 13.7 microseconds[11] in the timing signal was caused by an erroneous upload of data, following the retirement of the oldest satellite in the GPS fleet[12]. The error lasted several hours.

At the telecom operator, resilient system architecture (including atomic clocks used for timing holdover) meant that network operations were not disrupted. Once the root cause had been identified, a software patch was uploaded, but it still took four days to clear alarm logs and get services back to normal.

As well as telecoms, other critical infrastructure was affected, including a loss of digital radio services[13] in the UK, disruption to digital TV in Spain, and problems with public safety communications in the USA.

Multipath and urban canyon effects

Modern cities are full of obstructions that mask some satellite signals and reflect others over multiple paths to the receiver antenna. This can stop receivers from working, or cause them to produce poor quality outputs. The use of multi-constellation GNSS receivers can help to alleviate the masking of satellites, but even they fail under the most extreme urban conditions. It is technically possible to program receivers with algorithms to mitigate multipath reflections, but once again the most extreme conditions will defeat such measures.

Near-channel radio interference

Occasional testing by Dstl has shown that many civilian receivers have poor radio frequency filtering on their antenna inputs, meaning that they are vulnerable to strong signals on nearby frequencies. If local high-power services, such as personal mobile communications systems, are authorised to operate on these frequencies, interference to poorly designed receivers is highly likely. This has been seen in the US with communication signals transmitted by the LightSquared system[14].

Effects of other GNSS

Although increasing the number of GNSS and satellites can help to mitigate many of the vulnerabilities listed above, there comes a point where more and more signals in the same frequency band inevitably increases the background radio noise floor, making it harder to receive individual satellite signals.

Space debris

The amount of space debris is increasing and because relative velocities tend to be very high, even a small piece of debris could destroy a satellite. Fortunately, GNSS satellites operate at an altitude where there is currently a low risk of collision with such debris. This needs to be monitored and, as the number of GNSS satellites increases, rigorous procedures to remove old or failing satellites from orbit will need to be followed to maintain this situation.

Anti-satellite missiles and electromagnetic pulse

GNSS satellites could be attacked by an anti-satellite missile, or by the detonation of a nuclear weapon at high altitude causing damage through a high-intensity electromagnetic pulse. Either of these events would be a major act of war.

Systems-of-systems vulnerability

GNSS is at the heart of diverse systems and networks on which we have become highly reliant. A serious disruption to GNSS would be magnified many times as it forms a common point of failure within such systems of systems, which range from individual radio and computer networks to UK society as a whole.

The circumstances that cause failure of an individual GNSS receiver are becoming more widely understood and appreciated, but the vulnerability of GNSS-reliant systems of systems is often not understood at all, even by those with the most intimate knowledge of the construction and maintenance of those systems. Arguably the most vulnerable systems are those that use and trust the outputs of a GNSS receiver in a fully automated and unverified manner. Such systems are often those that use GNSS for timing applications.

Systems of systems could be designed to evaluate and adapt to the quality of the position and timing information available. That would require them to maintain metadata – for example every position or time output would come with information describing how it was derived and from what sources. Today, such metadata rarely exists, and where it does exist it is rarely passed on through the system in any meaningful manner.

References

1 Last D and others 'Demonstrating the effects of GPS jamming on marine navigation' 3rd GNSS Vulnerabilities and Solutions Conference, Baska, Croatia 5-8 September 2010. Available at http://www.professordavidlast.co.uk/cms_items/f20100909163023.doc

2 Psiaki M L and Humphreys T E 'GNSS Spoofing and Detection' Proceedings of the IEEE, 2016; Kerns A J and others 'Unmanned Aircraft Capture and Control via GPS Spoofing' Journal of Field Robotics 2014: volume 31, pages 617-636; 'UT Austin Researchers Successfully Spoof an $80 million Yacht at Sea' UT News 2013. Available at https://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea

3 We declare the grandmaster of pokemon go GPS cheats' Hackaday 2016. Available at http://hackaday.com/2016/07/26/we-declare-the-grandmaster-of-pokemon-go-gps-cheats/; Kiese S 'Gotta Catch 'Em All! – WORLDWIDE! (or how to spoof GPS to cheat at Pokémon GO)' Insinuator 2016. Available at https://insinuator.net/2016/07/gotta-catch-em-all-worldwide-or-how-to-spoof-gps-to-cheat-at-pokemon-go/

4 'Authorisation regime for GNSS repeaters' Ofcom 2012. Avilable at https://www.ofcom.org.uk/__data/assets/pdf_file/0029/47783/condoc.pdf

5 Steindl E and others (2013) 'The impact of interference caused by GPS Repeaters on GNSS receivers and services' European Navigation Conference 2013, Vienna, 22-25 April 2013

6 'Extreme space weather: impacts on engineered systems and infrastructure' Royal Academy of Engineering 2013. Available at http://www.raeng.org.uk/publications/reports/space-weather-full-report

7 See also London Economics 'The economic impact on the UK of a disruption to GNSS' 2017. Available at https://londoneconomics.co.uk/blog/publication/economic-impact-uk-disruption-gnss/

8 Briggs P, unpublished research

9 Nighswander T and others 'GPS software attacks' Proceedings of the 2012 ACM conference on Computer and communications security, pages 450-461

10 White House, statement by the press secretary. Available at https://georgewbush-whitehouse.archives.gov/news/releases/2007/09/20070918-2.html; GPS.gov 'Selective Availability'. Available at http://www.gps.gov/systems/gps/modernization/sa/

11 'GPS SVN23 Timing Anomaly 26 Jan 2016' Chronos technology 2016. Available at http://www.chronos.co.uk/index.php/en/telecom/351-cs-support/1611-gps-svn23-timing-anomaly-26-jan-2016

12 Kovach K and others 'GPS Receiver Impact from the UTC Offset (UTCO) Anomaly of 25-26 January 2016' Proceedings of the 29th International Technical Meeting of The Satellite Division of the Institute of Navigation, 2016. Available at http://www.gps.gov/systems/gps/performance/2016-UTC-offset-anomaly-impact.pdf

13 'BBC, Chronos Report on Lengthy Disruptions Caused by GPS Timing Problem' Inside GNSS 2016. Available at http://www.insidegnss.com/node/4839

14 Working group of the Federal Communications Commission 'Final report' 2011. Available at http://cody.inlandgps.com/pub/LightSquared/PDFs%20of%20FCC%20Filings/20110630%20-%20TWG%20Final%20Report.pdf

Chapter 3: Sector Dependencies

Sector dependencies on GNSS range from total (requiring GNSS to operate at all) to low (being only inconvenienced by loss of signal). Here we look at selected sectors where GNSS is already playing a major role, or has the potential to do so. Several are elements of critical national infrastructure: telecoms, emergency services, energy, finance, food and transport, with dependencies on time, position or both (Table 3.1)

Table 3.1
Sector dependency on time and position

	Telecoms	Emergency Services	Energy	Finance	Food	Transport
Time	✓	✓	✓	✓		
Position		✓	✓		✓	✓

Graphs throughout the chapter show required performance for accuracy and integrity risk (the probability at any instant that an unacceptably large error occurs without an alarm being raised, see Chapter 1, Measurement of performance). High integrity corresponds to low values of integrity risk, just as high accuracy means low uncertainty in position or time. So areas close to the origin of each graph indicate more stringent requirements for accuracy and integrity.

Telecoms

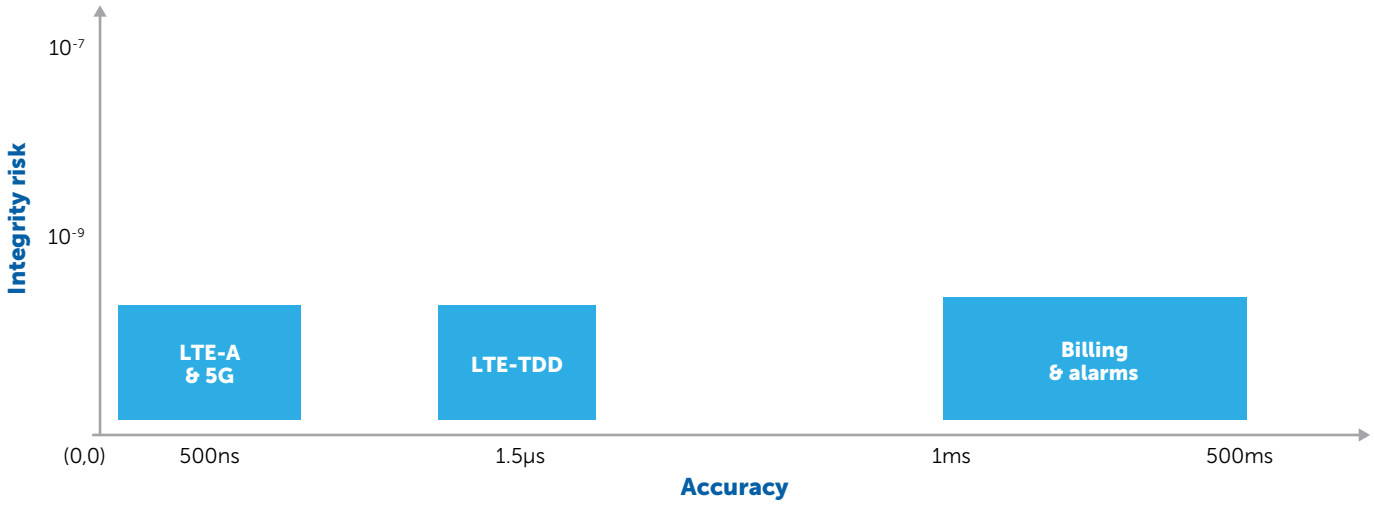
Telecoms use precise timing or stable frequency to synchronise communications networks. A stable frequency meeting International Telecommunications Union standards allows terrestrial telecoms to work across different carriers, and transport services error free. In the case of mobile technology, a frequency stable to 15 parts per billion allows 2G, 3G and 4G mobile base stations to operate and transmit at the correct radio frequency, phones to lock to that frequency and calls to seamlessly transfer between base stations.

Usually in the UK this frequency signal is transported across the terrestrial or core mobile network from a few central nodes. These nodes derive frequency either from GNSS, with quartz or rubidium clock holdover, or from caesium primary reference clocks.

New packet-based technologies have created challenges in carrying frequency-based synchronisation across the network. Meanwhile, some new mobile services need not only a stable frequency but also very tight timing. For example, LTE based on time division duplex modulation (TDD) requires time slot alignment of about 1.5 microseconds. Newer versions of mobile technology such as LTE-A allow handsets to receive from more than one base station, which will potentially require accuracy better than 1.5 microseconds, possibly down to 500 nanoseconds. The next generation of mobile technology, 5G, may have requirements in some cases of 500 nanoseconds or better.

The industry has evolved standardised techniques to transport accurate timing through the newer packet technology. Two technologies called Precision Time Protocol (PTP) and Synchronous Ethernet (SyncE) have emerged over the past 10 years. Together they allow high-performance frequency and time signals to be transported over a wide area. Network technology is being extended to carry high-performance timing (10s to 100s of nanosecond accuracy) to potentially millions of end points.

Figure 3.1
Accuracy and integrity requirements for telecoms



Dependency

Typically, the UK telecoms industry has not deployed GPS at mobile base stations (as the industry has in the USA), so our dependency today is low. But in the future, TDD based applications such as 5G may try to save money by using GNSS without backup as a source of frequency outside the core network – at mobile base stations and other nodes, collectively known as the edge[1].

Depending on the application and its implementation, the impact of a threat to GNSS may then be anywhere on a scale of inconvenient to catastrophic. Telecoms exchanges, base stations and data centres are static, and so make relatively easy targets for jamming or spoofing. Table 3.2 summarises the impact of losing GNSS if deployed at the edge.

Table 3.2
Telecommunications: disruption, impact, alternatives and trend – if GNSS is deployed widely

Disruption	Impact	Existing alternatives to GNSS	Future trend
Loss of frequency traceability due to interference or jamming	May range from inconvenient to catastrophic	Embedded atomic clocks and PTP transport through the network. Other alternatives include terrestrial radio navigation systems	Dangerous dependency on GNSS may increase
Loss of time traceability due to interference or jamming	May range from inconvenient to very serious. May cause problems with phones and other devices connected to the network. Certain base station services would be degraded	As above	
GNSS system failure or error in operation	May include all of those described above. May also cause operational problems through the flood of alarms confusing operational staff, potentially prompting bad decisions	As above	

5G

5G is a catch-all term for the new International Mobile Telecommunications network infrastructure for 2020 and beyond[2], including:

- Ultra-high capacity for urban environments, using very small cells
- Ultra-high performance for ultra-high definition video streaming and virtual reality, using millimetre wave signals
- Ultra-low latency for time-critical applications such as finance, gaming & telemedicine
- High availability and integrity for safety-critical applications such as automated driving

Future 5G systems will depend on much more accurate timing and positioning than 3G and 4G. The latest standard proposes minimum requirements for time alignment error of between 65 and 260 nanoseconds, depending on application. There is a danger that companies will embed GNSS in 5G systems, even though it will struggle to deliver this accuracy in a resilient, always-available manner. So engineers planning the new national 5G network are looking at other options such as network-based timing and eLoran.

Internet of Things

The growing network of connected devices is known as the Internet of Things (IoT). The networks used for IoT devices do not depend on GNSS, but some applications require position, such as sensors embedded in infrastructure for structural monitoring, and vehicle condition monitoring and fleet management.

Where precise position is required, such as strain monitoring, a transient or localised GNSS denial of service or degradation may disturb the measurement process, leading to unnecessary investigative action and a small reduction in efficiency.

Where the device is mobile and needs to be tracked, disruption of GNSS may have a larger impact. It could damage performance, create alarms and undermine business decision making. Where GNSS is being used to track people for security reasons (for instance to create a geofence), then there is a risk of exposing all concerned to potential harm.

Financial services

GNSS, and specifically GPS, has become the primary time source in financial services. It is used for:

Clock synchronisation. Stock exchanges check the GPS timestamp of received electronic share trading transactions against their own clocks to ensure that the orders are “fresh”. If the time difference is above a given threshold, they are rejected.

Performance monitoring and service level tracking. In recent years, latency of trading (the time taken to perform an operation) became a key competitive tool. The ability to measure your own and others’ performance accurately attained a new value, driven by minimising latency and the “race to zero”.

Regulatory controls. Perhaps the single largest cause of increasing GNSS dependence has been European and international regulation. From the need to timestamp all reportable events, such as trades, to the forensics of market abuse, accurate time is becoming essential to the operation of a stable financial market.

ATM and credit card transactions. ATM networks need accurate time to provide a clear record of transaction and to aid in fraud investigations, correlating to the time on local CCTV and other devices. One documented case where clocks were not synchronised led to a wrongful arrest[3].

Dependency

Historically, the downside risk of GNSS disruptions has been small, so there is very little awareness or quantification of the risks around GNSS. But dependency is increasing.

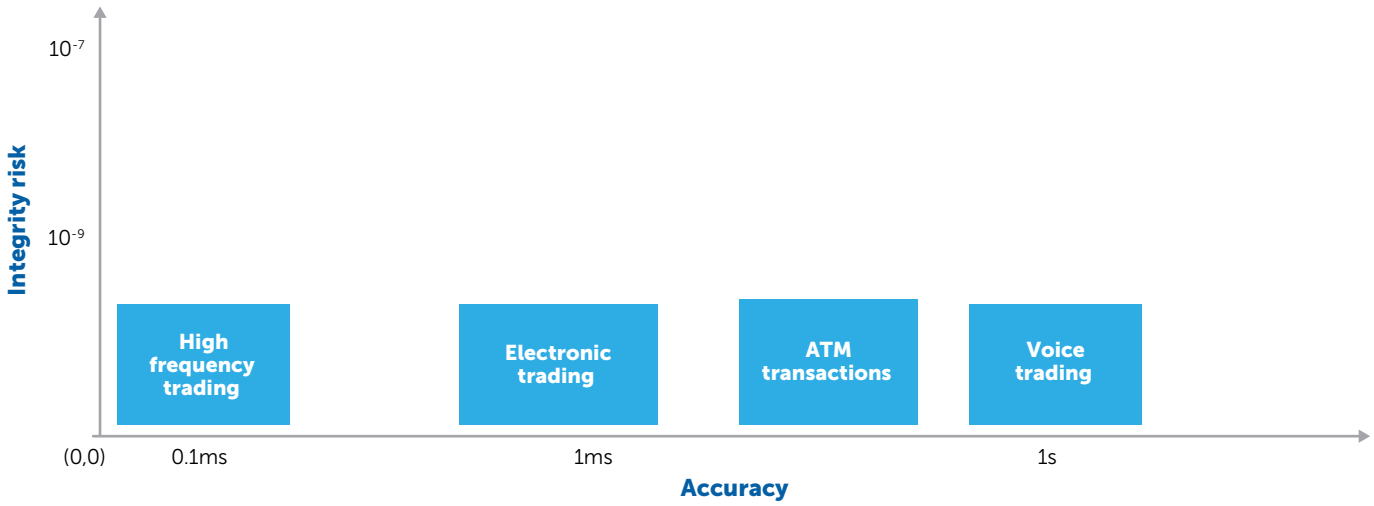
In 2007, a directive from the European Securities and Markets Authority (Markets in Financial Instruments Directive or MiFID) brought increased transparency and competition to financial markets, ushering in a new era of electronic and algorithmic trading (where computer models make investment decisions). The speed and frequency of share dealing changed by many orders of magnitude, as trading venues were now completing deals in hundreds of microseconds. This has challenged the forensics and audit capability of regulators.

Now that directive is being updated. Due to come into force in January 2018, MiFID II sets new guidelines and includes tight demands on timestamp accuracy[4]. All firms must now synchronise their clocks to the international timescale, UTC, and ensure that their timestamps never deviate by more than a defined amount, which can be as low as 100 microseconds.

Firms will need to demonstrate that their timestamps for all reportable events are traceable to UTC (Figure 3.2). A chain must be traced from the timestamp through software, hardware, network infrastructure and the time source feeding the infrastructure (invariably GNSS) and back to the laboratory defining UTC. Systems must be monitored continuously to ensure that their calibration has not changed. Other regulators around the globe are watching Europe, and it is likely that this will become a standard accuracy level globally in the next few years. Timestamping in software in particular is a challenge.

These strict new requirements mean that financial markets are now much more dependent on having a resilient time source, traceable to UTC.

Figure 3.2
Timing accuracy and integrity requirements in finance



Threats and impacts

Over the past few years, time synchronisation failures have caused several problems, sometimes forcing exchanges to close, for example. While these have not been traced to GNSS, they highlight the importance of timing (see also Table 3.3).

- On 18 November 2015, Barclays was fined $150 million for withholding foreign exchange trades for a few milliseconds, to assess whether the trade would be profitable for the bank due to currency swings over the millisecond duration[5].
- On 26 August 2013, Deutshe Boerse's Eurex derivatives platforms shut down for an hour due to a time synchronisation glitch[6].
- On 5 June 2013, Thomson Reuters caused the US's Institute for Supply Management manufacturing data to go out to high-frequency traders 15 milliseconds before it was supposed to, resulting in $28 million in shares changing hands[7].
- On 1 August 2012, Knight Capital lost $440 million in 30 minutes due to a runaway algorithm[8].
- On 15 February 2011, the London Stock Exchange (LSE) allowed normal trading to continue for 42 seconds after the official close, when the market should have entered the closing auction at precisely 16.30. LSE clients said the slight delay meant that orders destined for the auction were mixed with normal trades and they were left unclear which trades had been executed.

Timing is also necessary for regulators to investigate anomalous market crashes or rallies, and cases of fraud. Their forensic capability would be severely affected if a GNSS disruption resulted in timestamps with poor resolution and accuracy. Recent incidents where this kind of investigation has been important include:

- On 7 October 2016, the British pound suffered a mini flash crash, losing 6% of its value in two minutes[9].
- On 26 September 2016, Bank of America Merrill Lynch agreed to pay $12.5 million to settle allegations that it failed to stop 15 large, faulty trades that allegedly caused stocks to move abruptly causing mini flash crashes[10].
- On 6 May 2010, a US stock market flash crash wiped billions off the value of the shares of several organisations[11].

Table 3.3
Financial services: disruption, impact, alternatives and trend

Disruption	Impact	Existing alternatives to GNSS	Future trend
Localised jamming at data centre	Synchronisation and connectivity failures. Trading interrupted, delayed or shut down; risk of financial losses	Holdover clocks, or traceable network sources	GPS is already the primary time source, with dependency on GNSS expected to increase without awareness and understanding of the vulnerabilities and their mitigation
GNSS broadcasts wrong time	Synchronisation and connectivity failures, alarms.Trading interrupted, delayed or shut down; risk of financial losses; opportunity costs; market sentiment and volatility affected	Multisource comparison to detect the problem; switching to traceable network sources	
GNSS timing spoofed	Time differentials and connectivity failures. Market manipulation; fraudulent trading, loss of forensic capability; risk of financial losses; market sentiment and volatility affected	Alternative sources compared at a high enough precision and accuracy level to detect anomalies	

The ubiquitous use of GPS for timing, coupled with a lack of system calibration and monitoring, creates a market where no common clock exists at the microsecond level, increasing the risk of instabilities in the market. A 2012 Foresight report[12] highlights these effects and recommends the implementation of high-resolution, traceable timestamps. Loss, degradation or spoofing of GNSS could cause failures or instabilities, potentially resulting in mini crashes, unless mitigation is implemented.

Energy

The energy sector covers oil and gas exploration, mining, power generation, energy distribution and energy infrastructure monitoring. GNSS position, navigation and timing are increasingly important throughout the sector (Figure 3.3).

Oil and gas

Sub-metre accuracy is needed for rig positioning, and for oil and gas exploration by seismic survey. This is often achieved with precise point positioning (PPP) services (Chapter 1, Augmentation), where GNSS error correction products are provided by third parties. Transmitting these products to users requires a suitable communication system, so a disruption of the communications system would render the service unavailable. Such a communication system may itself depend on GNSS timing (see Telecoms section).

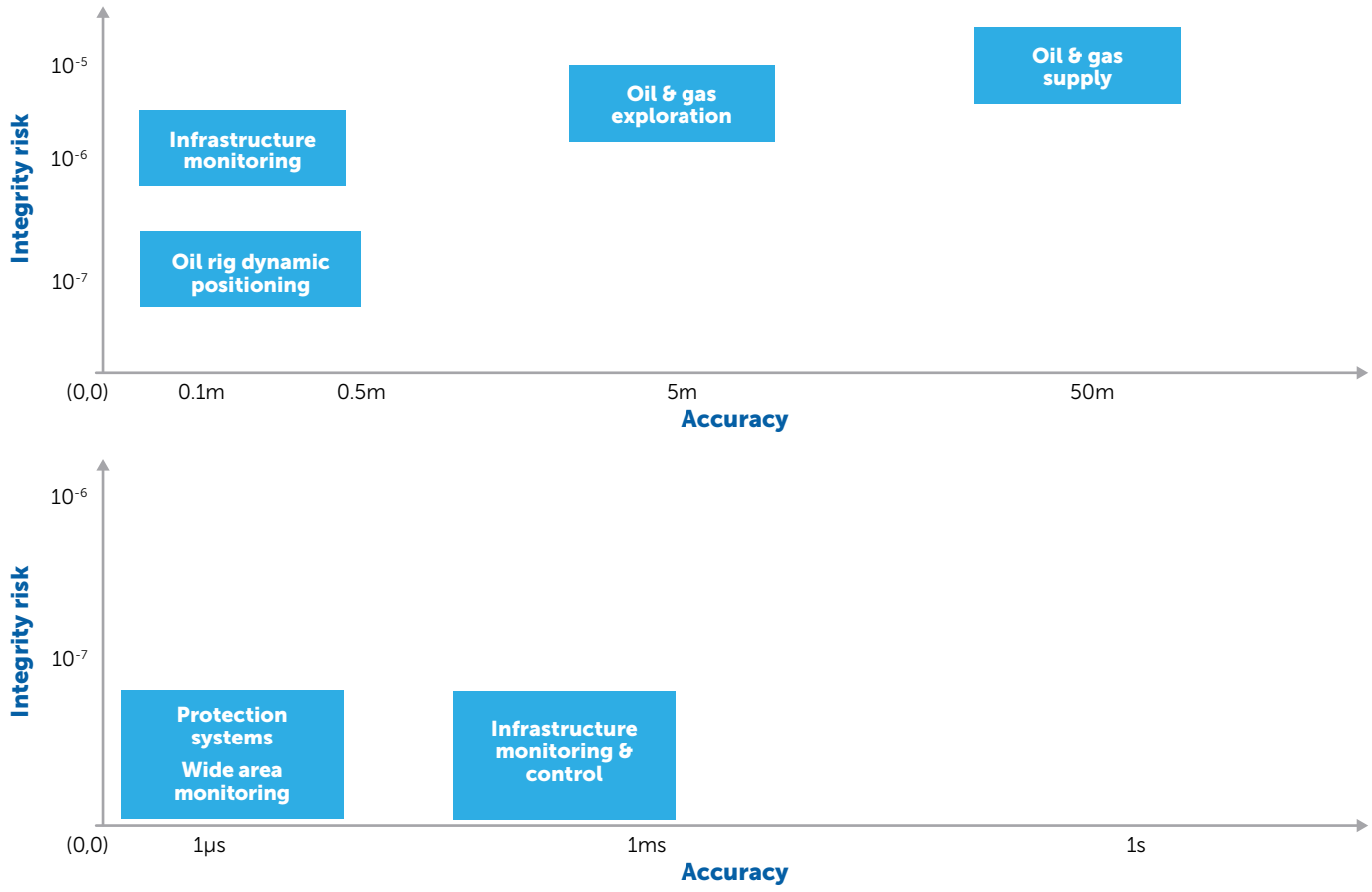
Several other applications require less stringent positioning accuracy of about one metre. They include appraisal drilling to determine the area of the site for exploration, delineating boundaries, identifying hazards, positioning pipelines, maintenance and repair.

The transport of personnel to and from platforms using helicopters is a hazardous operation, and helicopter accidents have been increasing, particularly at night and in bad weather. However, some countries including the UK have begun to use augmented GNSS for helicopter navigation, reducing the number of incidents and accidents.

Infrastructure monitoring

GNSS is cheaper and easier than terrestrial surveying, and can monitor 24/7. Checking the structural integrity of hydroelectric dams is a key application. Multi-constellation and multi-frequency systems are used to deliver very high positioning accuracies, to centimetres or millimetres, with integrity, continuity and availability.

Figure 3.3
Accuracy and integrity requirements in the energy sector



Power transmission and distribution

Power networks are becoming increasingly stressed, owing to replacement of conventional generation with intermittent renewables, the difficulty of building new overhead lines and the need to extract more value. As a response, they are now using GNSS timing to become more efficient. Devices known as phasor measurement units measure voltage and current thousands of times per second. In order for the information they provide to be valid, measurements must be timestamped with one microsecond or better accuracy using GNSS receivers. These synchronised measurements are used in real time for power system protection, generator control, frequency and voltage control, load shedding and intentional islanding (continuation of power supply by a generator in the event of a grid outage), to enable a wider envelope of secure operation. The use of GNSS for these applications is essential to ensure a fast response to unexpected events, and avoid conditions that could destabilise the system.

National Grid have used GNSS synchronised clocks as primary timing sources for more than 15 years. If GNSS is lost these clocks switch into holdover. However, the quality of the existing units means that they will drift relatively quickly (two milliseconds in a couple of hours being a typical value). But new substation infrastructure meeting international specification IEC 61850 requires a timing accuracy of one microsecond, so during extended losses of GNSS this requirement is quickly violated, with the potential of disruption in power supply. If a GNSS outage were to coincide with extreme weather such as strong winds and lightning strikes, that could disrupt supply to parts of the country and have a severe impact on other critical infrastructure.

When GNSS is lost National Grid often has to manually staff affected substations, expending considerable effort to ensure that equipment and health of the power system is monitored locally. In a nationwide GNSS outage it would be very difficult to staff all substations, and staffing key sites would take several hours to implement.

In summary, loss of GNSS timing could cause major disruption to power supplies unless we act to improve resilience, by investing in technologies to replace, supplement or provide backup to existing systems.

Threats and impacts

Space weather could lead to power grid failures by disrupting GNSS timing. Oil and gas rigs can cause a few particular problems for GNSS: the structure can mask signals or cause multipath errors, while electronic equipment can generate interference. Because of their strategic and commercial value, offshore platforms may also be targets for deliberate interference from terrorists. Table 3.4 details the effects of disruption of GNSS.

Table 3.4
Energy: disruption, impact, alternatives and trend

Disruption	Impact	Existing alternatives to GNSS	Future trend
Offshore exploration operators receive misleading GNSS positioning information, or none	Exploration undertaken in the wrong location, or unable to operate. Potential for environmental damage and considerable economic impact	Reversion to expensive alternatives including conventional surveying methods, use of inertial navigation systems or other radio navigation systems. Only a problem if the disruption lasts for hours or more	Dependency on GNSS to increase to total, with the danger that vulnerabilities are not all understood, and mitigation measures are not put in place
Oil rig receives misleading GNSS position information	Could be serious, for example increased risk of helicopter accidents	As above	
Power distributors receive misleading GNSS timing information, or none	Difficult or impossible to synchronise power grid. May cause local blackouts, with serious social and economic impacts	Taking time from national standards laboratories	Dependency on GNSS to increase considerably. Need to be aware of vulnerabilities and develop and implement mitigations

Emergency services

The ambulance, police and fire services use GNSS positioning and navigation to locate emergencies (Table 3.5), and timing to provide message timestamps. They also depend on GNSS timing for communication. Here we focus on the ambulance service to illustrate GNSS dependence across all the emergency services.

In the UK, 14 ambulance trusts operate around 10,000 emergency ambulances and a similar number of patient transport vehicles, along with air ambulances, motorbikes, community first responder vehicles and other medical response services. Collectively these vehicles and individual responders are known as mobile assets. They all use position, navigation and communication technologies that depend on GNSS positioning and timing.

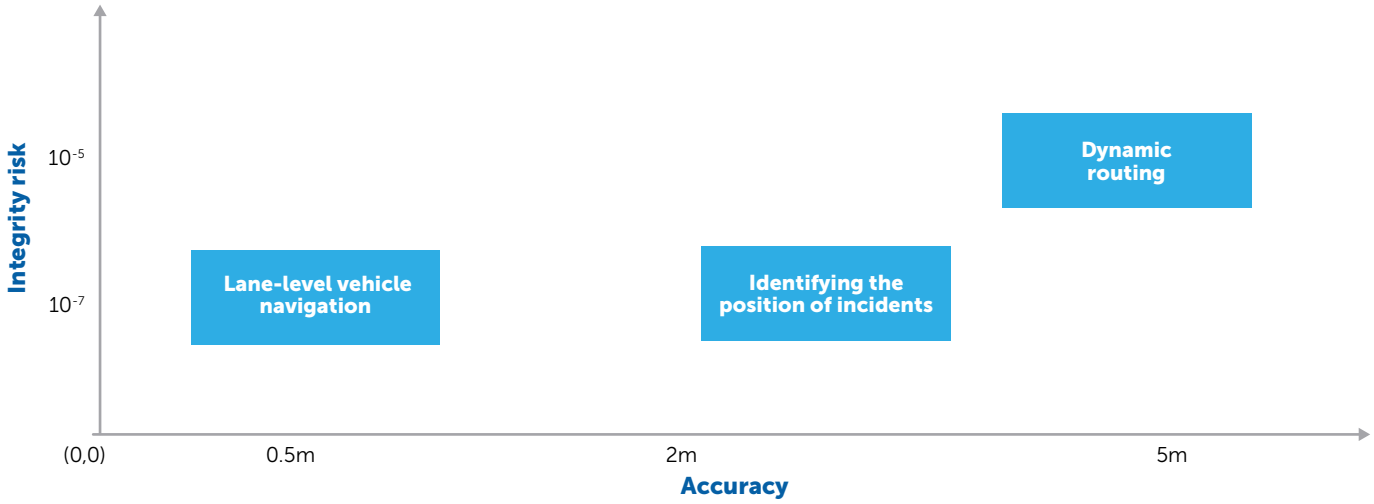
They communicate using mobile phone and TETRA radio networks, which are vulnerable to loss of GNSS timing; and every vehicle has its own computing and communications platform that includes a PNT system based on a GNSS receiver. Overall the ambulance service dependency on GNSS is best judged on its ability to perform its tasks: being able to locate patients, advise them, provide medical care and transport[13]. There are two main areas where these tasks could be hampered by a disruption to GNSS.

First, loss of communication between control centres and mobile assets would damage the ability of the service to perform its tasks. This dependency may increase in the future, as there is interest in providing treatment at the most appropriate point, which means ambulances may become more like mobile surgeries that provide treatment at the incident rather than transport to the hospital[14]. That would depend on good, high-bandwidth communications to support remote staff.

Second, GNSS positioning and navigation allows more effective and efficient tasking and transit of resources. Its absence would have severe and life threatening effects, but will not disrupt service provision as severely as a loss of communication.

Ambulances, their personnel and other care staff often operate in challenging environments where GNSS coverage is marginal and sometimes non-existent. Such areas can include urban, indoor and underground environments. These operational areas require non-GNSS-dependent solutions (Chapter 4).

Figure 3.4
Positioning accuracy and integrity requirements for emergency services



Threats and impacts

The threats to GNSS, such as interference, jamming, spoofing and meaconing, have consequences for the ambulance service ranging from inconvenience to almost total disruption.

Position and navigation

The impact of a disruption varies depending on what aspect of GNSS is lost, as shown in Table 3.5.

Table 3.5
Emergency services: disruption, impact, alternatives and trend

Disruption	Impact	Existing alternatives to GNSS	Future trend
Control room loses live tracking of asset	Job allocation difficult and asset progress less visible. Incorrect allocation of most appropriate asset and increased delays	Asset and control will both be aware of GNSS loss, so other responders may be sent out as backup, and voice contact used to communicate	Dependency on GNSS is already established, but increasing threat will require augmentation with inertial and alternative terrestrial systems
Mobile asset loses position awareness and navigation capability	Difficulty in finding incidents and hospitals. Serious potentially life threatening delays	Use of on-board electronic maps for manual navigation, and voice contact with control room	
Control room receives misinformation from GNSS	Incorrect job allocation; asset progress misleading. Delayed response with potentially life threatening consequences	Control room operators monitor live job progress and anomalies are likely to be noticed, so voice intervention is possible	
Mobile asset receives misinformation from GNSS	Incorrect navigation. Delayed journeys and destination errors, potentially life threatening	Will eventually result in either text or voice contact with control room – sooner rather than later if crews are familiar with local area	

Timing

All data transactions (including positions) are time-stamped with GNSS derived tags for audit and assessment purposes requiring 0.5s accuracy at best; this is important when litigation arises or adverse publicity needs addressing.

Of wider concern is the role of timing in communication (see Telecoms for accuracy and integrity requirements). Ambulance services use mobile phone networks for asset position and status reporting, incident data and patient information transactions, and some telemetry may use 4G – all of which is vulnerable to loss of GNSS timing. The TETRA network is used as backup when no mobile network is available; however, it can only handle low volumes of data, and is also GNSS dependent. Ambulance services in challenging terrain run several mobile

phone network SIM cards and TETRA, while experiments with satellite communications have also been conducted. The mobile equipment automatically selects the appropriate network invisibly to the user and compensates for small outages due to limited mobile coverage, using acknowledgement and repeat protocols. These systems would not be resilient to a serious disruption of GNSS, which is a major concern.

The emergency services mobile communications programme is developing a new system for all the services, called the emergency services network. This is based on 4G, which has similar vulnerabilities to other mobile phone communications, but the programme will be attempting to address these vulnerabilities with holdover technology and other methods.

As a last resort, a control room will revert to landlines and sending people to strategic locations. If the event is prolonged, strategies could include the deployment of military communications and amateur radio organisations.

Food and farming

GNSS positioning is becoming important in the food industry, especially in satellite navigation systems used for crop management. This is being driven by falling equipment costs. Farmers can achieve centimetre accuracy in real time using a differential GNSS receiver, antenna, computer and optimisation software. GNSS positions are then linked to maps, databases and geographic information systems, and the information exchanged with farm vehicles.

GNSS applications in agriculture and distribution include:

Yield mapping. Position information on a crop harvesting vehicle can be associated with the local yield, and that information used to control the rate of fertiliser application. Soil fertility maps can also be produced from spatio-temporally referenced samples from the soil, recording data such as pH, potassium, phosphorus or magnesium levels.

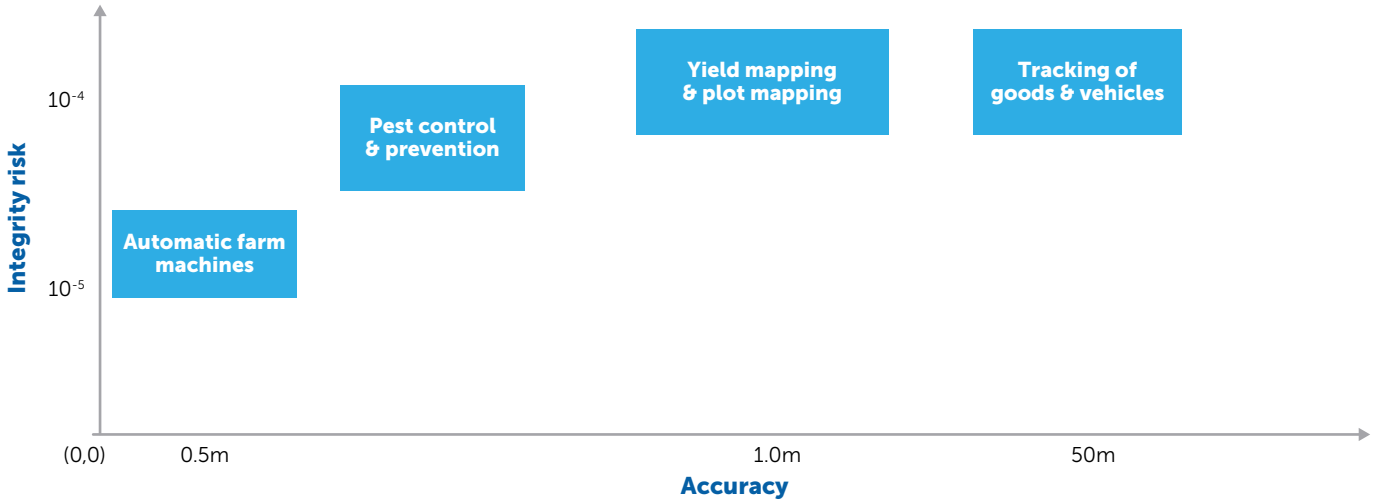
Plot mapping. The size of farm plots can be measured using a GNSS receiver to centimetre level accuracy.

Automatic guidance. Tractors and other farm machines with a GNSS receiver and an on-board computer can be guided automatically, following predefined coordinates without human intervention. Several machines can operate on the same plot, saving time and cost.

Pest control and prevention. GNSS is used to track infestations and identify areas at risk. Sharing this knowledge can provide instant advice on dealing with infestations.

Tracking of goods and vehicles. This can speed deliveries of food, help maintain quality and prevent theft. With position and time tags, documentation on food safety and pesticide application can be tracked. Table 3.6 details the impact that GNSS failure could have on food supply and farms.

Figure 3.5
Positioning accuracy and integrity requirements for the food and farming sector



Threats and impacts

The UK's food supply chain depends on GNSS positioning and navigation to ensure timely distribution and delivery of products. This is critical particularly for perishables. Because many food distributors now use just-in-time supply chains, with little in-built resilience, a disruption to GNSS could hit availability of food to consumers (Table 3.6). The societal and economic impacts of this are potentially severe, including the possibility of civil unrest.

Table 3.6
Food and farming: disruption, impact, alternatives and trend

Disruption	Impact	Existing alternatives to GNSS	Future trend
Automated farm machines lose GNSS signal or receive misleading positioning	If prolonged and over a wide area, could reduce food production	Non-GNSS sensors, human intervention	Dependency on GNSS to increase towards total, with the danger of lack of awareness and understanding of vulnerabilities and their mitigation
Farmers lose GNSS tracking of farm machines, or receive misleading positioning	Delays resulting in potentially large increase in cost of operations	As above	
Food supply chain control centre loses GNSS signal or receives misleading positioning	Delays, damage and lack of security	Non-GNSS positioning system such as WiFi	
Part of the food supply chain loses GNSS signal	Delays, damage and lack of security	As above	

Transport

The use of GNSS positioning by transport is increasing across the board, but the level of dependency differs between aviation, road, rail and maritime – partly because of differing maturity in their definition of standards, with aviation the most advanced.

Aviation

Commercial air transport continues to undergo enormous growth. Aviation entities including manufacturers Boeing and Airbus agree that over the period 2016-2035, we can expect the number of flights to rise about 4.5 to 5% per year globally, and 3 to 4% in Europe[15]. The Department for Transport predicts that air traffic at UK airports will grow at an average of 2% per annum to 2050, implying that by then they will serve about half a billion passengers a year[16].

Traditional ground-based air traffic management (ATM) technologies cannot accommodate this growing demand. In the 1980s the International Civil Aviation Organisation (ICAO) committee on future air navigation systems found that these systems and procedures would not support traffic growth, as they restrict use of airspace because aircraft can only fly along routes equipped with the required ATM systems. If not addressed, this would result in increasing levels of congestion, delays, risk of accidents, pollution and climate change. The committee found that satellite technology, being global in scope, offered the only viable solution.

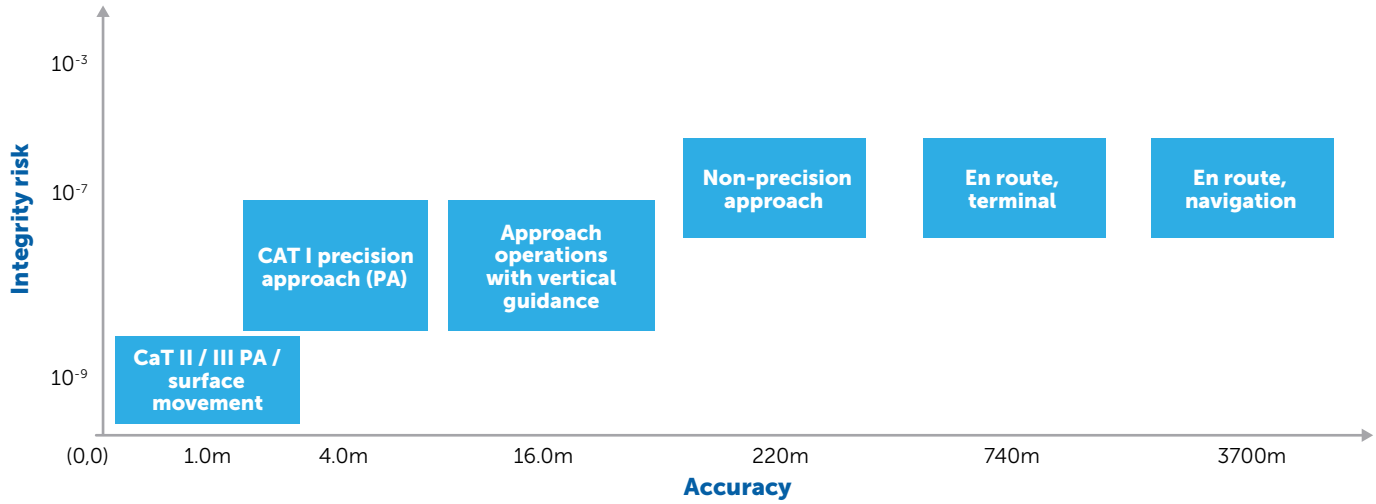
Gate-to-gate aircraft area navigation with GNSS would allow aircraft to follow more efficient flight paths, and fly safely with less separation – enabling flexible use of airspace for maximum capacity and minimum delays. Furthermore, GNSS has the potential to meet the required navigation performance in accuracy, integrity, continuity and availability for all phases of flight.

Seamless global navigation capability would also remove the need for the restrictive variety of ground-based and airborne systems designed to meet specific requirements for certain phases of flight. The use of GNSS should provide many other benefits, including navigational capability in remote areas without traditional navigational aids, and the flexibility to accommodate all air traffic, including general aviation, helicopters and drones – as well as newly developed high-altitude, long-endurance aircraft, which may be used for applications such as providing internet signals.

Dependency

In future, dependency on GNSS will increase to total. GNSS is at the core of new air traffic systems being implemented by Europe's Single European Sky ATM Research (SESAR) programme[17] and the United States' NextGen[18]. The accuracy and integrity requirements are shown in Figure 3.6. The most stringent phase of flight for accuracy (sub-metre) and integrity risk (~10^{-9}) is landing and surface movement. In these systems, different stages of a flight use GNSS with three different forms of augmentation: aircraft based augmentation systems (ABAS), satellite based augmentation systems (SBAS), and ground-based augmentation systems (GBAS). SBAS and GBAS are forms of differential GNSS (Chapter 1, Augmentation); ABAS augments the satellite signal using data from other instruments onboard such as the inertial navigation or reference system. Via the new Automatic Dependence Surveillance Broadcast (ADS-B) system, aircraft broadcast their position, altitude and vector information from the GNSS navigation system to the relevant stakeholders (airline operators, aircraft manufacturers, aviation authorities and providers of air navigation services including air traffic control).

Figure 3.6
Positioning accuracy and integrity requirements for aviation



GNSS has been approved for en-route flight, terminal airspace and the earliest phase of approach, known as category I, which takes planes down to an altitude of 60 metres (Figure 3.7). In 2012, the first operational approval of GBAS was given for installation at Newark Liberty International Airport, paving the way for GNSS-guided approach to landing by commercial aircraft. By 2015, many airports were using this GBAS-based category I capability (Table 3.7).

So far, commercial aircraft at major airports do not use GBAS for the remaining and most stringent phases of flight (category II/III approach – which cover the final phases to touchdown – and surface movement). This is because some positional errors remain that could compromise safety (see Threats and impacts, below). Research is underway to address these challenges and complete the quest for GNSS-based gate-to-gate operations.

The European Commission has mandated19 the implementation of required navigation performance (RNP), a satellite-based navigation standard, for some operations in many terminal airspace areas including the London Airspace from 2024. For these operations, aircraft will be required to have GNSS for navigation.

Meanwhile, augmented GNSS is already being used for landing at small airports where there are no conventional landing aids. Aviation also relies on GNSS-dependent ground transport, baggage systems, information systems and communications networks. Failures in any of these systems would not affect safety but could disrupt the global aviation network.

Figure 3.7
Status of GNSS use in different phases of flight

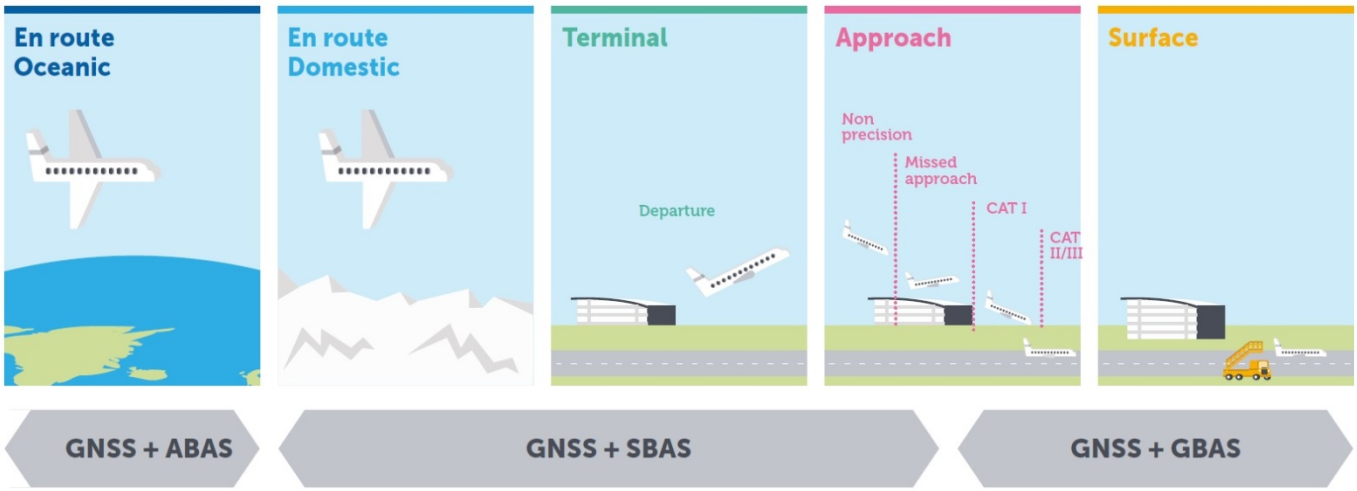


Table 3.7
Airlines using GNSS with ground-based augmentation systems, and airports where GBAS approaches are flown on a regular basis. There are plans to implement GBAS at Heathrow, Melbourne, Oslo, Rio de Janeiro, Chennai, Dubai (UAE), (India), Gimpo (South Korea) and St. Helena (UK)

Airline	Airports
Air Berlin	Bremen, Malaga
British Airways	Newark
Cathay Pacific	Houston, Sydney
Delta	Houston, Newark
Emirates	Frankfurt, Houston, Sydney, Zurich
United	Houston, Newark
Lufthansa	Frankfurt, Houston
Qantas – Sydney	Sydney
Swiss Air	Zurich
TUIfly	Malaga
Various Russian airlines	Domodedovo, Pulkovo, Tyumen, Ostafyevo, Nogliki and others

Threats and impacts

Some GNSS measurement errors are not accounted for by the differential corrections of SBAS and GBAS. Before GNSS can be approved for the remaining phases of flight, these must be understood and appropriate techniques for their mitigation developed. Table 3.8 lists potential disruptions and consequences.

For landing and surface movement, better ways of dealing with multipath errors are still to be developed. Space weather can give errors of tens of metres in GBAS, whereas for safe and smooth touchdown planes require sub-metre accuracy and very high integrity – especially in the vertical dimension. Removing this threat to safety requires more effective monitoring of integrity, which GBAS is still to supply.

Jamming could affect many aircraft simultaneously. There have already been several incidents. For example, on 23 November 2009, a trial GBAS system at Newark's Liberty International Airport shut down due to interference from an unknown source. It happened again on 23 March 2010, but by now specialised detection equipment had been deployed, and the source was identified. The jammer's vehicle was pursued and the device surrendered. In November 2013, a New Jersey truck driver was prosecuted for using an illegal GPS jamming device to hide from his employer, after it wiped out GNSS at Newark.

Table 3.8
Aviation: disruption, impact, alternatives and trend

Disruption	Impact	Existing alternatives to GNSS	Future trend
Aircraft receives misleading position and velocity information from GNSS	Aircraft off the scheduled route and sends misleading information to stakeholders. Potential for collision	Terrestrial systems provide all required PNT so at present there is little or no GNSS dependency	GNSS dependency will increase to total. The ICAO requires that the vulnerabilities of GNSS are understood and mitigations developed
Air traffic control receives misleading information	Airspace congestion, increase in workload including increased communication with pilots, reduced separation minima		
Airlines receive misleading GNSS positioning and velocity information	Delays and cancellation of flights		
Aircraft loses GNSS navigation	Degraded navigation performance. Air traffic control relies on pilots for aircraft situational awareness		
Air traffic control loses GNSS positioning	Increase in air traffic control workload, increased congestion. Potential for increase in delays, incidents and accidents		
Airlines lose live GNSS tracking information	Delays and cancellations		

Road

Intelligent transport systems are revolutionising road transport. For example, they can provide data on location as well as traffic and road status updates, enabling a vehicle to compute optimal routing (Figure 3.8). This redistributes traffic, reducing congestion and its environmental and social impacts. GNSS is increasingly used in these systems because of its low cost and ease of integration with other sensors and databases.

The GSA GNSS Market Report[20] predicts that the road sector will constitute 38% of the GNSS market from 2013 to 2023, so any disruption of GNSS could hit not only transport infrastructure and services, but also the entire value chain from component manufacturers to users.

The report classifies applications into smart mobility (improving efficiency, effectiveness and comfort), safety critical (delivering services in situations that could result in harm to humans or damage to infrastructure/environment), liability critical (applications that have legal and economic consequences) and regulated (applications that must enforce transport policies that arise from national or international legislations).

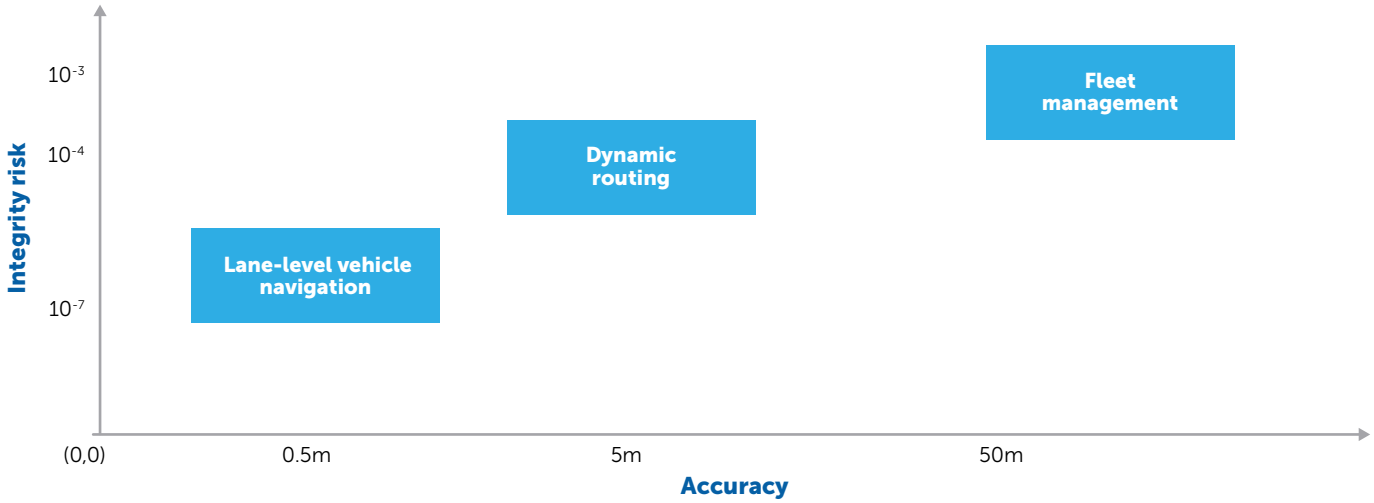
In smart mobility, navigation is the most widespread application. This includes the most familiar use of GNSS, in-car satnav. Data collected from vehicles generates traffic information and allows transport operators to monitor performance – for example, urban bus operators rely on GPS for services including countdown displays. Table 3.9 lists the potential consequences of disruption to GNSS.

Safety-critical applications include tracking of dangerous goods, and one of the fastest-growing segments in automotive electronics, advanced driver-assistance systems. These systems automate, adapt and enhance vehicle systems for more efficient driving and safety – alerting the driver to problems, or taking over a vehicle if necessary.

Road user charging is a liability-critical application, using GNSS information from onboard units to charge tolls based on the usage of roads and to manage congestion[21]. GNSS offers low transaction costs and environmental impact, and additional revenue from value-added services. Germany, Switzerland, Slovakia and Hungary have successfully implemented GNSS-based tolling, with Belgium and Russia launching similar projects, while France, Finland, Bulgaria, Denmark, Holland and Lithunia have declared an interest. Worryingly, this could create a financial motive for jamming and spoofing, with the potential to cause wider impact.

A new regulated application is the enhanced digital tachograph, which will support road enforcers by using GNSS to record the position of a vehicle during the day.

Figure 3.8
Positioning accuracy and integrity requirements for the road sector



Threats and impacts

Particularly in urban areas, buildings and other objects can mask satellite signals and result in multipath errors, disrupting GNSS. Interference, both intentional and unintentional, may block or degrade signals. Jammers known as personal privacy devices cause many cases of interference each month on the UK road networks, with potential for wider impacts. These and other sources of interference are increasing, posing a major threat to the road transport sector.

As well as facing these direct threats, most applications require communication with a central control centre, so a disruption to communication would render them unavailable.

Table 3.9
Road transport: disruption, impact, alternatives and trend

Disruption	Impact	Existing alternatives to GNSS	Future trend
Drivers lose GNSS signal or receive misleading position and velocity information	Delays, higher fuel consumption	Maps and road signs, alternative navigation systems	The level of dependency on GNSS will increase, but operational environment challenges will require augmentation with terrestrial systems and alternative positioning capabilities. Threats posed by other vulnerabilities must be understood and mitigations developed
Fleet controllers/ managers receive misleading position and velocity information from GNSS	Degraded quality of service, such as inaccurate travel or arrival time; undercharging/ overcharging of tolls; wrong location of incidents/accidents; incorrect insurance premiums	Voice radio communication; alternative navigation systems	
Fleet controllers/ managers lose GNSS signal	Not possible to provide normal fleet management services	Voice radio contacts useful for some services; alternative navigation systems	

Rail

Rail transport is expected to grow rapidly in the coming 30 years. The European Commission predicts that by 2050, rail freight across Europe will grow by a factor of eight, and passenger travel[22] by a factor of 12. In the UK, travel in passenger kilometres is expected to increase[23] from 19.3 billion in 2013 to 26 billion in 2030 and movement by freight from 31 to 51.4 billion tonnes[24].

So railway network capacity must be increased. This can be done through the development of infrastructure, such as new tracks and platforms, and a more efficient use of existing infrastructure. Usage can be optimised with intelligent traffic management and control systems, such as the European Railway Traffic Management System[25], which gather train position and other information from train and trackside equipment and share it with all railway stakeholders.

Today, train position is measured by trackside equipment that is expensive to maintain and has high failure rates. GNSS is recognised as an alternative that could support traffic management systems with high-accuracy data, while reducing the amount of trackside equipment and the cost of operation and maintenance to maintain and has high failure rates.

In 2012 and 2016, stakeholders including the European Commission and European Railways Agency signed memoranda of understanding recognising the benefits of GNSS in the European

Rail Traffic Management System[26]. In the UK the implementation of this system is led by the Railway Safety and Standards Board and Network Rail.

Dependency

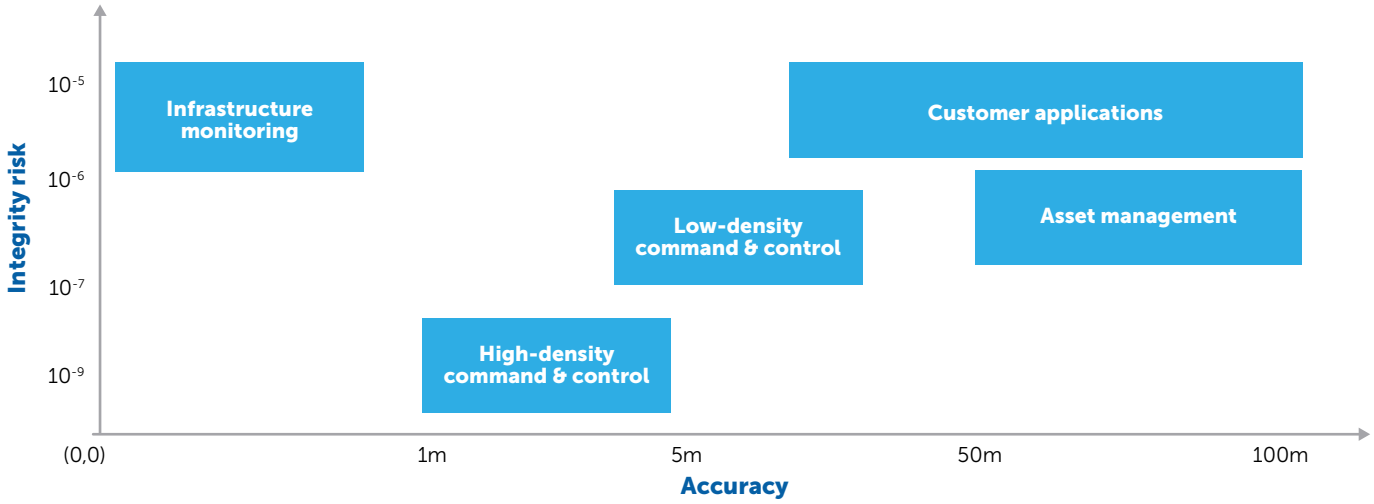
GNSS is expected to support the automation of train operations (Figure 3.9). It will have a role in:

High-density command and control systems. GNSS used to assist train command and control on the main lines.

Low-density command and control systems. GNSS-based signalling system on lines with low to medium traffic.

Asset management. GNSS positioning information is provided to railway stakeholders, supporting fleet management, maintenance work and other functions.

Figure 3.9
Positioning accuracy and integrity requirements for rail



Threats and impacts

GNSS in the railway environment may be disrupted by space weather, jamming and unintentional interference. Obstacles such as trees, buildings and bridges frequently mask GNSS signals, reducing the number of visible satellites. That damages position determination (requiring a minimum of four satellites), integrity (six satellites required to detect and exclude an erroneous measurement) and accuracy. These obstacles also reflect GNSS signals, creating multipath errors that can reach tens of metres.

No minimal operational performance standards have been agreed for railway operations, which prevents certification and makes it impossible to assess whether a system works safely under all conditions. The Next Generation Train Control consortium[27] is investigating positioning requirements for railway operations.

GNSS is increasingly being used to support safety-critical applications, so developing resilience is paramount to the safety of railway operations. Table 3.10 indicates the potential effects of disruption.

Table 3.10
Rail: disruption, impact, alternatives and trend

Disruption	Impact	Existing alternatives to GNSS	Future trend
Railway/train operators lose GNSS signal or receive misleading GNSS information	Disruption of services; delays; cancellations; risk of collisions; environmental consequences if carrying dangerous cargo; legal consequences for liability critical applications (e.g. asset management)	Use of voice communication; reversion to conventional technology/ techniques; alternative positioning and navigation systems	Dependency on GNSS will increase towards total. Need to be aware of the vulnerabilities and develop mitigations

Maritime

In 1967, maritime users were the first community to use satellite navigation for civil applications, through the TRANSIT system, a precursor to GPS. Later, local vessel traffic services using differential GPS were introduced in some coastal regions.

Ships rely heavily on GNSS for navigation in most environments. Figure 3.10 and Table 3.11 show the requirements and list the effects of disruption. GNSS positioning is used widely in traffic management and surveillance, search and rescue, fishing vessel control, port operations and marine engineering, such as dredging and cable laying.

In oceanic navigation there are few nearby objects, so GNSS is immune from almost all masking and multipath, except that generated by the vessel itself. Given the value of some containers, pirates may employ jamming and spoofing. In coastal navigation, there is a higher risk of running aground and colliding with other vessels due to high traffic density. In port approaches and other restricted waterways, navigation requirements are more stringent, given even denser traffic, nearby dangers, and possible multipath errors and interference from land.

In port operations, ships and other structures present multipath and masking effects, and there is great potential for intentional and unintentional interference (Table 3.11). Cargo handling and automatic docking require decimetre positioning accuracy.

Hydrographic surveys and dredging also require decimetre-level accuracy, while construction may require centimetre-level accuracy. For these high-accuracy positioning requirements, the threats emanate from masking, multipath and space weather.

Search and rescue uses positioning for the initial alert, and navigation for tracking and search. Operations must coordinate with the Global Maritime Distress Safety System, which today requires an accuracy of 100 metres for incidents position estimation. That will change to 10 metres in the future. This is a critical operation that requires high-integrity and high-availability positioning and navigation capabilities. Interference is the main threat here.

Figure 3.10
Positioning accuracy and integrity requirements for the maritme sector

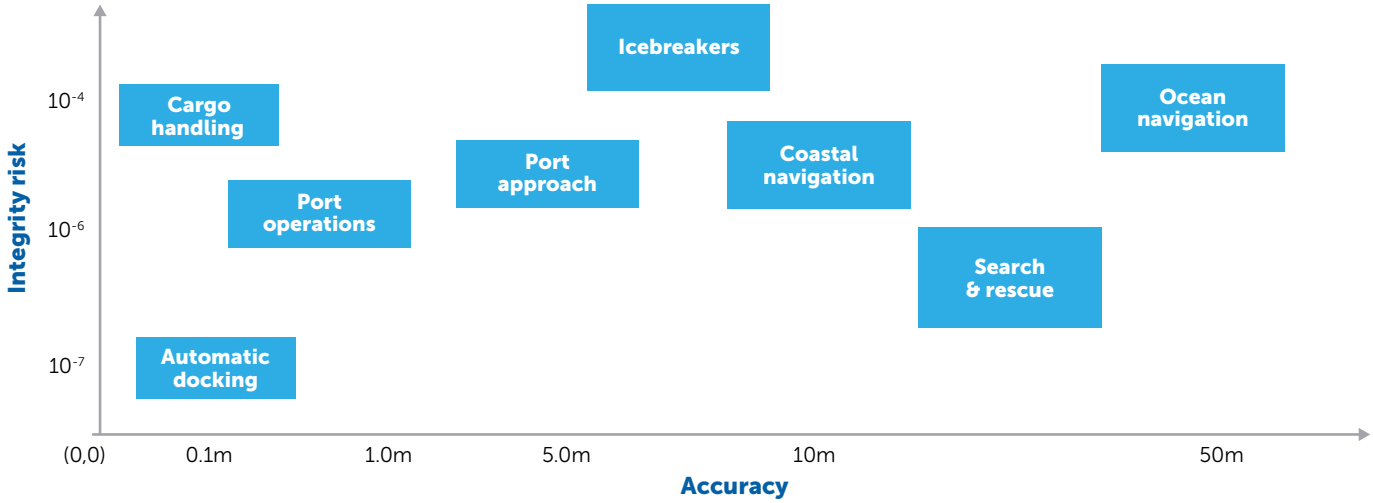


Table 3.11
Maritime: disruption, impact, alternatives and trend

Disruption	Impact	Existing alternatives to GNSS	Future trend
Vessel loses GNSS or receives misleading GNSS information	Delays, higher fuel consumption, risks of collision and running aground	Alternative navigation systems (such as inertial navigation systems and other radio navigation systems); reversion to conventional methods	Dependency on GNSS will increase to total. The vulnerabilities of GNSS should be understood and mitigations developed
Port operators receive misleading GNSS information	Congestion around ports, with increased toxic emissions and noise	As above	
Port operators lose GNSS signal	Delays, higher fuel consumption, risks of collision and running aground	As above	

Potentially critical infrastructure

Sectors that may become critical, either directly or as enablers of critical national infrastructure, include surveying, mass market and emerging areas/future areas (Figure 3.11).

Surveying

GNSS is especially useful for mapping property boundaries at great speed and with a high degree of accuracy. It is also used for large scale topographic surveys, setting out, dimensional control and structural monitoring, enabling such processes to be automated. GNSS positioning is also used in making maps, environmental and urban planning, to support the exploration and extraction of minerals, seabed exploration, estimating tides and currents, and offshore surveying.

The main threats to the use of GNSS for surveying are masking, multipath and interference. The threat posed by jamming is currently small, although for major public infrastructure projects the potential for disruption could be great (Table 3.12).

Table 3.12
Surveying: effect, impact, alternatives and trend

Disruption	Impact	Existing alternatives to GNSS	Future trend
Surveyors/engineers receive misleading GNSS information	Incorrect property boundaries with significant economic and societal consequences; poor design and dimensional control of infrastructure such as building and dams (risk of collapse, injury and loss of life)	Reversion to alternative expensive conventional techniques	Dependency on GNSS will increase considerably. The vulnerabilities of GNSS should be understood and mitigations developed
Surveyors/engineers lose GNSS	Delays, economic costs and societal impacts	As above	

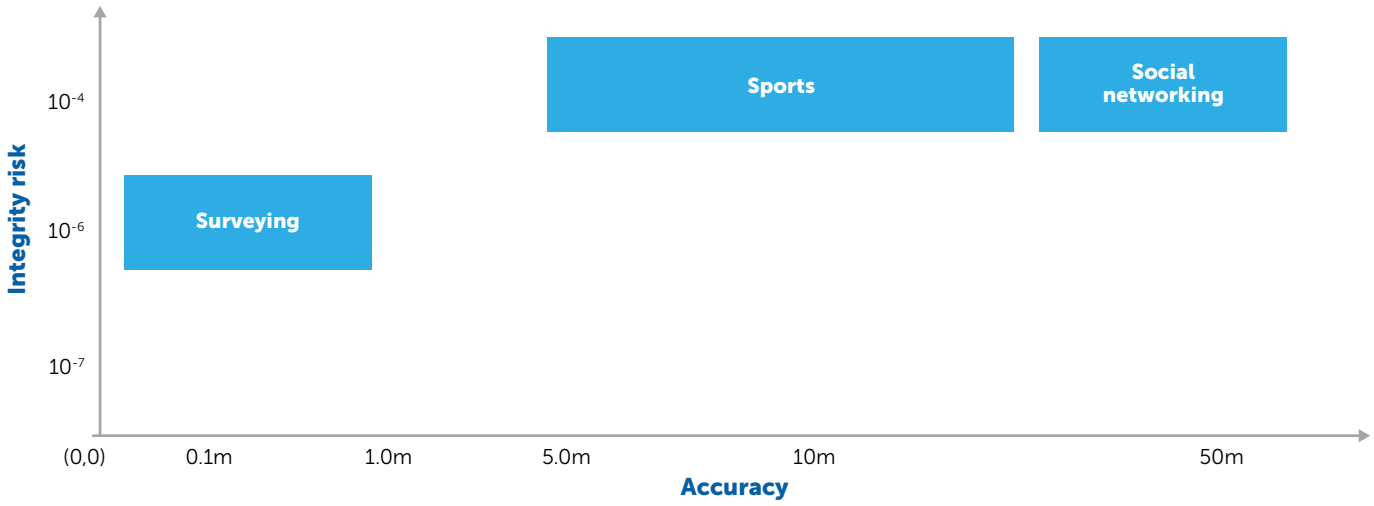
Mass market

The growth in mass-market applications is driven by personal portable devices including smartphones, tablets, tracking devices, digital cameras, computers and sports/fitness accessories.

These devices support a wide variety of applications, including:

- Navigation
- Map-making
- Geo-marketing and advertising
- Safety and emergency
- Workforce management
- Sports
- Games and augmented reality
- Social networking
- Crowd sourcing

Figure 3.11
Positioning accuracy and integrity requirements for surveying and mass-market applications



The main threats are signal masking, multipath and interference. The threat posed by jamming is currently small, although that could change with the proliferation of personal privacy devices (Table 3.13).

Table 3.13
Mass market: disruption, impact, alternatives and trend

Disruption	Impact	Existing alternatives to GNSS	Future trend
Users receive misleading GNSS information	Inaccurate navigation; compromised safety, security and social activities; games/ sports consoles compromised	Alternative positioning and navigation systems such as inertial sensors, signals of opportunity and map matching	Dependency on GNSS to increase to partial (augmented with terrestrial systems/ sensors and map matching) because of the challenging operational environments
Service providers receive misleading GNSS position information	Inaccurate maps, misleading geo-marketing and advertising; difficulty in providing emergency services; social networking and crowd sourcing applications compromised		
Users or service providers lose GNSS signal	Potentially large safety, security, social and economic impacts		

Autonomous road vehicles

The hazards of driving are dynamic. Other vehicles will usually obey the rules of the road, but not always; and more surprises will come from mechanical failure, animals and other unpredictable hazards. Autonomous vehicles will have to be designed to react to these anomalous conditions as safely as possible (Figure 3.12), and an absolute positioning system such as GNSS can only be used as an aid to system operation. Vehicles will also need to operate safely in GNSS-denied environments such as car parks, tunnels and garages. So regional or transient denial of GNSS services should not be a serious problem for future road networks where autonomous vehicles are prevalent.

Drones

Drones are being used for an increasing range of applications such as inspecting infrastructure, border control, environment monitoring, search and rescue, parcel delivery and crop spraying. They may be remotely piloted platforms or fully autonomous systems managed by a dispatch centre. At present most trials involve a human pilot. Drones are anticipated to operate in airspace that is currently unmanaged by national air navigation service providers, but they will contend with general aviation, other airspace users, dynamic hazards such as birds and semi-static hazards such as cranes.

GNSS will be needed to establish a frame of reference for operations, but it will not be enough on its own. Drones will meet many dynamic threats, and must be able to sense and avoid them based on their sensors (Figure 3.12).

GNSS is already being used to define no-fly zones, predicated on the cooperation of drones and drone operators. So drones should be disabled from operating in a GNSS-denied environment, unless special constraints are in force (in-building safety inspections for instance), and should have integrated inertial sensors and intelligent systems that allow for safe operation should GNSS signals be lost. Where such measures are implemented, a transient denial or degradation to GNSS signals will not severely compromise safety.

Applications will have differing GNSS dependencies:

Inspection of infrastructure. In most cases, there will be an operator nearby. Localised disturbance to GNSS may cause some operational inconvenience.

Long-linear infrastructure monitoring for utilities. In most cases drones will fly autonomously along predetermined routes. They are likely to use a high-accuracy form of differential GNSS known as RTK (Chapter 1, Augmentation) as well as multiple receivers, used in concert with onboard inertial guidance. Disruption to GNSS may cause interruptions to operation, damage to infrastructure or personal injury.

Border control and other security applications. These are likely to involve remotely piloted drones, sometimes with long flight duration. Position determination will be important, but resilient communication is the critical requirement, particularly for long flight duration. Loss of either GNSS position or communication could be serious, especially as the drones are likely to be heavy. Failsafe modes will be critical.

Perimeter control applications (for building sites, research parks, power generation facilities) are likely to use shorter duration autonomous drone flights, probably monitored by a control room. Geofencing will be critical, likely to be dependent on GNSS.

In all security related applications, the threat profile is likely to be very high, and drones will need to deploy resilient anti-jamming receivers in concert with other positioning technology to improve the chance of maintaining safe operation.

Environment monitoring, especially maritime, coastal and forests. These applications are likely to be autonomous, with routine or targeted gathering of drone-based sets to complement satellite data. GNSS technology is likely to be important and the likelihood of electromagnetic interference is high, as drones will cover wide areas. So systems must be resilient and able to maintain safe autonomous operation in the absence of GNSS signals.

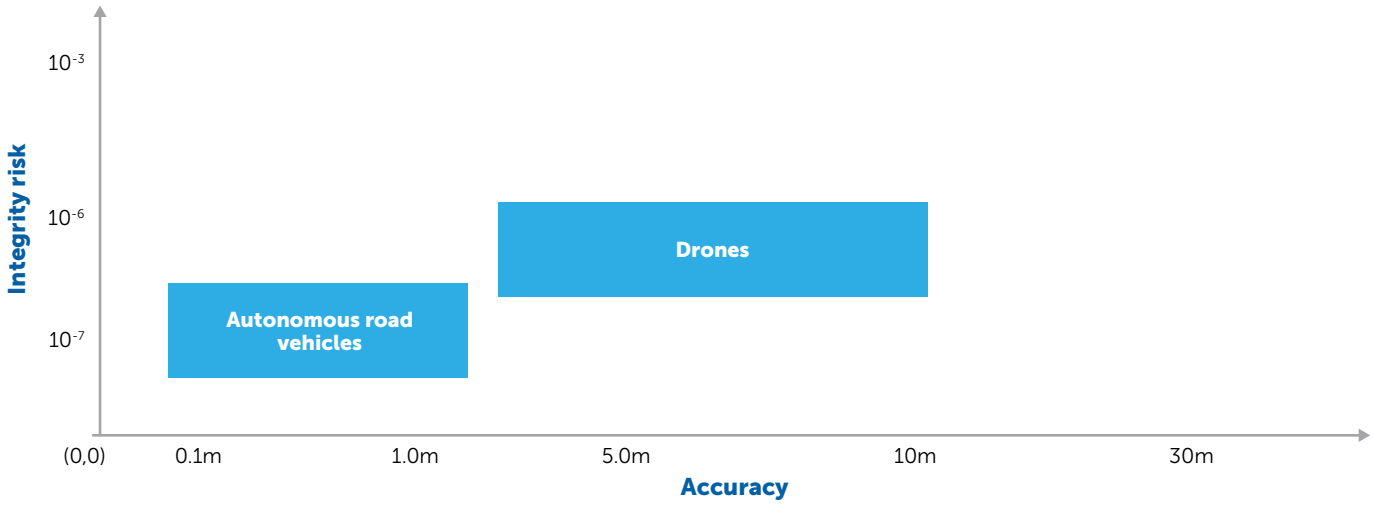
Emergency services and disaster response, such as search and rescue. Drones will often be remotely piloted. GNSS dependency is likely to be high, and implications of degradation to GNSS is almost certainly life threatening.

Freight logistics, such as parcel delivery. Drones are likely to be fully autonomous, with the delivery environment considered an extension of the warehouse. They are likely to encounter many dynamic hazards. Sense-and-avoid strategies will be critical for safe operation, for which GNSS has no purpose (unless the hazard is another drone), but as GNSS will be the main

way to calibrate positioning systems, sustained interference would probably reduce operational efficiency.

Air-taxi services. Due to the high risks involved with carrying a human passenger, these systems will need very high levels of integrity. GNSS may be used, but the safety case for such operations will require extensive testing to ensure safe operations in the event of a loss of GNSS.

Figure 3.12
Positioning accuracy and integrity requirements for autonomous road vehicles and drones



New space

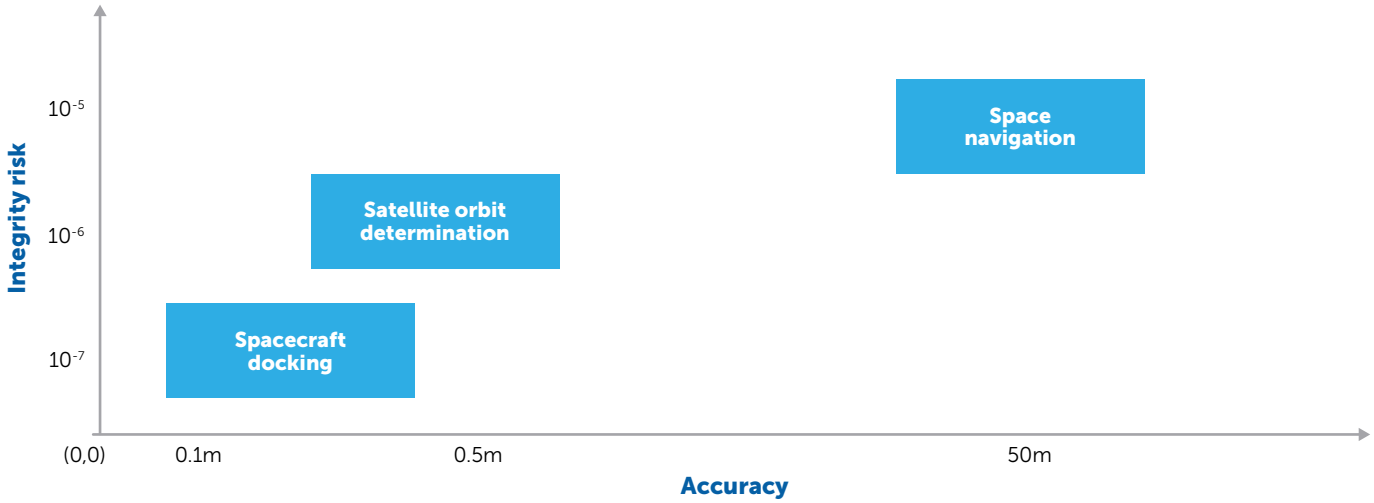
Knowing position is critical for all services delivered from space, but most systems use other means to measure it, so dependency on GNSS is low at present.

In future, satellites in low Earth orbit are likely to depend more on GNSS, in part because the number of satellite launches is increasing rapidly, so space traffic management is becoming more important. GNSS will enable satellites to determine position themselves (Figure 3.13) and reduce dependence on ground-based stations.

The increasing availability of enhanced GNSS signals, with higher power at multiple frequencies, is extending the use of GNSS to satellites in higher orbits as well. This will fundamentally change the approach for determining precise orbits, needed for various purposes such as preventing collision, and capture and disposal of space debris. GNSS will support increased satellite autonomy by providing high navigation performance with minimum ground control and without the heavy onboard sensors now used, reducing costs. This will also improve capabilities for formation flying, improve weather prediction using advanced weather satellites, enable en-route lunar navigation, support space weather observations, and reduce separation minima of satellites in geostationary orbits.

Space weather is the main threat associated with the use of GNSS for these applications.

Figure 3.13
Positioning accuracy and integrity requirements for new space



References

1 Curry C 'Dependency of Communications Systems on PNT Technology' Chronos Technology 2010. Available at http://www.chronos.co.uk/files/pdfs/wps/Dependency_of_Comms_on_PNT_Technology.pdf

2 International Telecommunications Union 'IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond' 2015. Available at https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-I!!PDF-E.pdf

3 Williams R N 'Time Synchronisation in Criminal Cases'. Galleon Systems 2008. Available at http://www.galsys.co.uk/time-reference/basic-ntp/the-importance-of-time-synchronisation-in-criminal-cases.html

4 European Securities and Markets Authority 'MiFID II and MiFIR' 2017. Available at https://www.esma.europa.eu/policy-rules/mifid-ii-and-mifir

5 'Barclays fined $150m over forex trading by New York regulator' Guardian 18 November 2015. Available at https://www.theguardian.com/business/2015/nov/18/barclays-fined-150m-over-forex-trading-by-new-york-regulator

6 Taylor E and others 'Deutsche Boerse's Eurex resumes trading after outage' Reuters 26 August 2013. Available at http://www.reuters.com/article/us-deutscheboerse-eurex-halt-idUSBRE97P0CQ20130826

7 Javers E 'Unraveling Monday's Early Data Release to Traders' CNBC 5 June 2013. Available at https://www.cnbc.com/id/100792260

8 Philips M 'Knight Shows How to Lose $440 Million in 30 Minutes' Bloomberg 2 August 2012. Available at https://www.bloomberg.com/news/articles/2012-08-02/knight-shows-how-to-lose-440-million-in-30-minutes

9 Rodionova Z 'Pound value plunges 6% in 2 minutes in mysterious flash crash' The Independent 7 October 2016. Available at http://www.independent.co.uk/news/business/news/pound-flash-crash-mystery-value-sterling-dollar-euro-new-low-brexit-latest-a7349636.html

10 Barlyn S and Stempel J 'BofA to pay $15.5 million fines for causing 'mini-flash crashes'' Reuters 26 September 2016. Available at http://www.reuters.com/article/us-bank-of-america-sec-idUSKCN11W1VC

11 US Securities and Exchange Commission 'Findings regarding the market events of May 6, 2010' 30 September 2010. Available at https://www.sec.gov/news/studies/2010/marketevents-report.pdf

12 Furse C and others 'The Future of Computer Trading in Financial Markets' Government Office for Science 2012. Available at https://www.gov.uk/government/publications/future-of-computer-trading-in-financial-markets-an-international-perspective

13 Turner J and others 'Ambulance Response Programme, Evaluation of Phase 1 and Phase 2' NHS England 2017. Available at https://www.england.nhs.uk/wp-content/uploads/2017/07/ARPReport_Final.pdf

14 'eHealth at WHO' World Health Organization. Available at http://www.who.int/ehealth/about/en/; 'eHealth' NHS Scotland. Avalable at eHealth http://www.ehealth.nhs.scot/

15 'Boeing Current Market Outlook 2016-2035' Boeing 2016. Available at http://www.boeing.com/resources/boeingdotcom/commercial/about-our-market/assets/downloads/cmo_print_2016_final_updated.pdf; 'Mapping demand 2016-2035' Airbus 2016. Available at http://www.team.aero/files/airbusforecast/Airbus-GMF-2016-2035-MappingDemand-full_book.pdf

16 'UK Aviation Forecasts 2011' Department for Transport 2011. https://www.gov.uk/government/publications/uk-aviation-forecasts-2011

17 Single European Sky ATM Research 'The European ATM Master Plan' 2015. Available at https://www.atmmasterplan.eu/

18 Federal Aviation Authority 'NextGen'. Available at https://www.faa.gov/nextgen/

19 'Notice of Proposed Amendment 2015-01: Performance-Based Navigation (PBN) implementation in the European Air Traffic Management Network (EATMN)' European Aviation Safety Agency 2015. Available at https://www.easa.europa.eu/document-library/notices-of-proposed-amendment/npa-2015-01

20 'GNSS Market Report, Issue 4' European Global Navigation Satellite Systems Agency 2015. Available at https://www.gsa.europa.eu/system/files/reports/GNSS-Market-Report-2015-issue4_0.pdf

21 Ochieng W Y and others 'Technologies to measure indicators for variable road user charging' ICE Transport, 2010: volume 163, pages 63-72.

22 European Commission 'Roadmap to a Single European Transport Area - Towards a competitive and resource efficient transport system' 2011. Available at https://ec.europa.eu/transport/themes/strategies/2011_white_paper_en

23 Ellman L and others 'Rail 2020' The Stationery Office, UK Parliament 2012. Available at http://www.parliament.uk/business/committees/committees-a-z/commons-select/transport-committee/inquiries/parliament-2010/rail-2020/

24 'The Importance of Rail Freight' Freight Transport Association 2008. Available at http://www.fta.co.uk/export/sites/fta/_galleries/downloads/rail_freight/importance_of_rail_freight_0408.pdf

25 'The Future Railway - The Industry's Rail Technical Strategy 2012' Technical Stragegy Leadership Group 2012. Available at https://www.rssb.co.uk/library/future%20railway/innovation-in-rail-rail-technical-strategy-2012.pdf

26 'Memorandum of Understanding (MoU) between the European Commission, the European Railway Agency and the European Rail sector Associations (CER - UIC - UNIFE - EIM - GSM-R Industry Group - ERFA) concerning the strengthening of cooperation for the management of ERTMS. European Commission 2012. Available at http://www.era.europa.eu/Document-Register/Documents/MoU-betweenEC-ERA-and-Sector-Associations-on-ERTMS.pdf

27 http://www.uitp.org/next-generation-train-control-ngtc

Chapter 4: Mitigations

A Royal Academy of Engineering Report of 2011 proposed ways to mitigate threats to GPS[1]. Since then the problem has become even more urgent. Europe's Galileo and other GNSS will help mitigate some of our current GPS vulnerabilities – but not most of them. The UK needs to deploy other forms of mitigation.

The first group of methods set out below provide backup PNT services, completely independent of GNSS. These can provide mitigation in a wide range of circumstances, but they do not remove the need for more specific mitigations.

The second group mitigate vulnerability by making GNSS more resilient. Most of these have a narrow scope and are used in specialised applications. Selecting the right mitigation for each application requires a detailed understanding of how GNSS data is to be used, and the types of threat.

Each method is labelled with its relevance to position (P), navigation (N) and timing (T).

Services independent of GNSS

Terrestrial radio systems (P,N,T)

The enhanced Loran (eLoran) system[2] uses signals from radio masts to provide position, navigation and UTC-traceable timing. Its high-power, low-frequency transmissions do not have the vulnerabilities of the low-powered microwave GNSS transmissions.

Proposed by the US Federal Aviation Administration (FAA), eLoran works in a similar way to GNSS in that the receiver calculates its position from the times at which signals arrive from three or more transmitters. eLoran re-purposes the 100 kHz transmissions from now-obsolete Loran-C stations and adds a data channel. The FAA has shown that it could meet the accuracy, integrity, availability and continuity standards of aircraft non-precision approaches and maritime harbour entrance navigation, and also deliver a precise time and frequency service, plus a wide-area data broadcast[3].

The General Lighthouse Authorities of the UK and Ireland demonstrated eLoran via a prototype system that used nine European Loran-C stations, until their scheduled withdrawal from service at the end of 2015. Operating continuously for three years, it achieved maritime Initial Operational Capability at seven UK ports with accuracies better than 10 metres, while delivering land navigation, timing and data messaging.

Currently, an eLoran station in Anthorn, Cumbria, provides a national UTC-traceable timing service with very similar performance to that of GPS[4]. Its performance is being assessed by critical infrastructure organisations in telecoms and broadcasting, some receiving the signals indoors. The data channel can broadcast differential corrections, GNSS ephemeris data and advisory notices, encryption keys and high-priority messages across a wide area of Europe.

Although eLoran transmissions cannot deliver altitude measurements, in other respects they are a comprehensive PNT mitigation to GNSS vulnerabilities[5]. They are internationally standardised[6], with operational or trial Loran broadcasts in the USA, the UK, Russia, Iran, Korea, India, China and Saudi Arabia. Although the radio transmissions of eLoran are very

different from those of GNSS, the cost of a professional-grade receiver with both capabilities need not be much greater than that of a GNSS-only system.

Time by fibre (T)

Precise timing services require traceability: measurements must be linked back to a reference standard via a continuous chain of calibrations with known uncertainties. Measurements are usually traced to a UTC time source at one of 78 contributing timing centres worldwide[7]. The UK's national time scale, UTC(NPL), is maintained by the National Physical Laboratory.

Time disseminated from a UTC laboratory via optical fibre offers an end user at a fixed location a certified UTC-traceable time signal. Where time is further distributed, the traceability of the chain must be monitored, controlled and subject to service level agreements.

Resilience and redundancy are key to disseminating precise time. Malicious or inadvertent damage to the fibre must be detected and several fibre routes provided. A holdover oscillator at an intermediate point may provide cover for several weeks.

Signals of opportunity (P,N)

Signals of opportunity are broadcasts such as AM or digital radio that are wholly independent of GNSS, and not intended for navigation or timing[8]. A receiver's position can be determined by measuring ranges or bearings from their transmitting antennas. Unlike GNSS, such positioning systems can exploit not only the timing of the transmissions but also their signal strengths and angles of arrival, thereby making position measurements more robust. In urban areas there may be many such transmitters in range.

Because each type of transmission has its own failure modes and propagation characteristics, jamming or spoofing them is much more challenging than with GNSS. Local terrestrial signals do not suffer directly from space weather effects. Smartphones already use WiFi and mobile signals of opportunity.

A disadvantage is that many apparent signals of opportunity are not truly independent of GNSS, being frequency-locked to it. Even those that are independent may be of low integrity. For instance, a navigation user may not learn promptly of service changes; precise transmitter locations must be surveyed or determined by machine-learning techniques; and transmitter frequency stability may not meet navigation standards, so requiring differential operation.

These technologies are good candidates for future research to assess their suitability for specific applications.

Composite or hybrid navigation (P,N)

Before the arrival of GNSS, positioning and navigation employed techniques that included terrestrial radio navigation, visual, inertial, dead-reckoning and map-matching systems. Some of these are still used to complement GNSS. For example, vehicle satellite navigators often use inertial, dead reckoning, map matching and compass techniques to provide turn-by-turn navigation in dense urban areas and in tunnels, so mitigating the loss of GNSS signals[9].

Making GNSS more resilient

Detection, interdiction and early warning

Detection (P,N,T)

Jamming, spoofing and meaconing can be mitigated by systems that monitor the radio spectrum for threatening signals and then alert users or law enforcement authorities. Technically-trained personnel detect threatening signals by using spectrum analysers. Now equipment suitable for use by law enforcement officers is available, and automated sensors linked to cameras can detect GPS jamming devices in moving vehicles. The UK is leading in jammer detection technology.

Space weather forecasting (P,N,T)

The impact of space weather on GNSS can be partially mitigated by forecasting and monitoring. The UK Meteorological Office forecasts events[10] and notifies users of space weather that may cause an increase in background noise level. Current techniques have only a limited ability to predict the effects on GNSS, but the quality of forecasting is improving.

Holdover

Holdover oscillators (T)

Where GNSS provides a stable clock for timing applications, high-performance oscillators can take over temporarily when it is lost. Currently, such devices are usually oven-controlled crystal oscillators or atomic clocks based on rubidium or caesium technologies[11]. The UK, through EPSRC and Innovate UK, is developing a future generation of timing holdover devices that use quantum clocks[12].

Telecoms companies need accurate time and phase to support 4G and 5G networks. This timing, which must be traceable to UTC, is most commonly derived in the core network from GNSS. When GNSS is lost, a holdover clock will take over, but it will gradually drift away from GNSS time; its performance is specified by how long it can maintain a certain accuracy. Many non-telecom timing applications lack clear holdover specifications to guarantee service continuity.

Inertial navigation systems (P,N)

Inertial navigation systems (INS) can provide navigation holdover when GNSS is lost. An INS estimates motion from an initial position using measurements from accelerometers and gyroscopes, and a navigation computer to transform these measurements into position, velocity and orientation. INS are entirely autonomous. They are standard equipment in many military aircraft, ships, submarines, missiles and spacecraft, and common in large commercial aircraft. However, they are rarely used in commercial shipping or other civil transport because of their high cost and uncertain benefits.

INS can give very accurate positions in the short term, but errors accumulate with time. The rate of error growth depends on the quality and cost of the sensors, which are specified as tactical, navigation, or consumer grade[13]. The performance of consumer-grade units is improving rapidly, with low-cost micro-electro-mechanical systems now approaching or even exceeding tactical grade level.

Mitigation at the GNSS receiver

Differential GNSS (P,N)

In differential GNSS (Chapter 1, Augmentation), satellite signals are received by reference stations at known locations. Each such station sends out corrections for propagation delays in satellite signals, so improving the accuracy of receivers in its area. It also warns receivers not to use any satellite that has malfunctioned, so enhancing integrity.

Ephemeris aiding (P,N,T)

When a GNSS receiver is switched on, it attempts to acquire the signals of satellites in view. How rapidly this happens depends on how accurately it can estimate the satellites' positions using a set of orbital data known as an ephemeris. This is transmitted by the satellites and stored in the receiver. In a location where satellite signals are weak (such as a city centre or forest), ephemeris data supplied by an alternative source can reduce the time taken to acquire signals from minutes to seconds. In mobile phones, this data is supplied over the network.

An Innovate UK-funded project is studying an extension to this concept in which ephemeris information is broadcast nationwide over an eLoran data channel (see above) for reception in GNSS-unfriendly locations, for example by utility meters and Internet of Things devices indoors.

Multi-frequency and multi-constellation receivers (P,N,T)

Currently, satellite receivers in critical civil systems are almost all single-frequency, single-constellation devices, which receive only the GPS coarse acquisition code. Newer receivers use signals from more than one constellation on more than one frequency. They can acquire satellites more quickly (see Ephemeris aiding, above) and get a more accurate fix by using more satellites, and they have lower vulnerability to ionospheric delay.

These receivers may be less vulnerable to those simple forms of jamming and interference that target only the L1 band (used by most GNSS including GPS and Galileo). However, cheap commercial jammers for all frequencies of all constellations are readily available.

Multi-constellation receivers may also be used for precise timing, but different constellations employ different versions of UTC, which must be taken into account when combining or switching between them.

Controlled radiation pattern antennas (P,N,T)

A controlled radiation pattern antenna (CRPA) can protect GNSS receivers against interference and some spoofing. It electronically steers an array of internal antenna elements to favour signals arriving from the directions of the satellites and attenuate signals from interferers[14]. CRPAs can be designed to be effective against narrowband, broadband, pulsed continuous wave, swept or spectrally-matched interference, plus certain types of spoofing. They can report the direction of the source of the interference, CRPAs can be very effective and are widely used by the armed services and defence organisations. However, they are much more expensive and larger than conventional GNSS antennas.

Integrity monitoring (P,N,T)

This is an integrity-enhancing technique that protects receivers against the failure or corruption of individual or multiple satellite signals. In GNSS reception, four satellites are sufficient to fix a position and deliver precise time. When more satellites are received, receiver autonomous integrity monitoring (RAIM) can check their individual ranges for consistency[15]. Given five

satellite signals, RAIM blocks reception should any satellite fail the test. With six or more, RAIM can exclude one or more faulty satellites from contributing to the position calculation. Should the whole constellation fail, or its signals be blocked by interference, the receiver will cease to operate. RAIM is mandatory in certain aviation receivers, but is not generally employed in maritime or critical infrastructure applications.

Resilient architecture (T)

When GNSS supplies precise timing to a telecommunications system, UTC traceable time can be distributed to many locations within a fibre network by means of Synchronous Ethernet or by using Precision Time Protocol. This is standardised for telecom networks by the International Telecommunications Union. These techniques enable a few high-quality receiver installations on protected sites to supply a whole network in place of larger numbers of lower-quality, more vulnerable receivers.

Indoor reception

GPS re-radiators (P,N)

In aircraft hangars, workshops and garages, where satellite signals may not be available, re-radiator devices can be installed that receive the signals on an outdoor antenna and rebroadcast them into the indoor space[16].

Mitigation through best practice

Design assurance (P,N,T)

Especially in critical infrastructure, GNSS receiving systems should meet specifications that recognise vulnerabilities. Certification should show that an installation meets stated design assurance standards, such as rejecting potentially interfering signals; using information from non-GNSS sources when GNSS is lost; and recording not only PNT data but also receiving conditions (such as the number and quality of satellite signals), to let the end user assess the data and so accept or reject it.

Testing (P,N,T)

Choosing the right mitigation strategy may require a detailed risk assessment, to characterise the operating environment, identify holdover requirements, and test system components against threat scenarios (Chapter 5).

From June 2017 the European Radio Equipment Directive[17] has included mandatory testing of GNSS products that are to receive CE marking. Tests include adjacent band compatibility and emissions assessments. The aim is to eliminate events of the kinds experienced recently, when thousands of receivers were affected by the GPS timing anomaly of January 2016[18]; or when a GPS-navigated drone crashed in a stadium in San Diego[19]. Testing should also reduce susceptibility to leap seconds, week-number rollovers (Chapter 2) and corrupted ephemeris data[20].

However, the directive does not remove the need for testing for specific applications. Critical services, in particular, must meet higher standards than do many commercial and consumer systems.

Fixed antennas for timing receivers (T)

Precise timing receivers generally use fixed antennas, and many are badly installed[21]. To minimise interference, an antenna should have a clear view of the sky, be at least 20 metres

from other GNSS antennas and not be close to radio sources, especially line-of-sight radio links. They should be installed by qualified and experienced personnel. Antennas must have lightning protection and cable runs that meet high fire safety and other standards.

Table 4.1
Mitigations by sector

Sector	Mitigations
Telecoms	The first line of defence is **resilient architecture** with diverse network routing to high-stability atomic clocks in the core of the network and localised **holdover** at the edge. In the future multiple sources of time will be required for 4G/5G services. Backup to GNSS would be a **terrestrial radio system**. If UTC traceability is required, **time by fibre** could be considered at key locations.
Finance	The **multi-constellation receivers** used today experience common GNSS vulnerabilities, and their different UTC sources hamper traceability. **Holdover** devices provide mitigation, but errors increase with time. **Time by fibre** offers traceability to UTC. Some organisations are considering a **terrestrial radio system**.
Energy	As with telecoms, better **holdover** with atomic clocks is one option, along with GNSS-based Precision Time Protocol (Chapter1). GNSS **integrity monitoring**, or a **terrestrial radio system** backup, would improve timing resilience. National Grid is also considering **time by fibre**.
Emergency Services	Emergency services would benefit from **multi-frequency and multi-constellation receivers** with backup navigation from **inertial navigation** and **terrestrial radio systems**. Emergency service operators' on-screen maps could allow manual shifting of vehicle positions.
Aviation	**Multi-frequency receivers**, improved **space weather forecasting** and **differential GNSS** using Extended GBAS[22] would help mitigate ionospheric effects. A system of interference **detection** stations would mitigate interference and jamming. A **terrestrial radio system** backup would maximise safety.

Sector	Mitigations
Road	Research is underway to identify **signals of opportunity** with high positioning accuracy, independent of GNSS. **Composite or hybrid navigation** can be used in GNSS outage areas. An alternative, intelligent urban positioning, matches the shadows of buildings to 3D maps[23]. Interference can be mitigated using the same detection techniques as for aviation. **Terrestrial radio systems** have been successfully demonstrated on land.
Rail	**Space weather forecasting** will help mitigate ionospheric effects. GNSS positions can be validated using accelerometers, gyroscopes, odometers and trackside radio beacons. **Detection**, in the form of a dedicated trackside augmentation network, could pick up ionospheric anomalies and interference. **Terrestrial radio systems** have been successfully demonstrated.
Maritime	Ships must carry a GNSS-based electronic positioning/navigation system. The only backups may be visual navigation and radar. Harbour and coastal authorities are interested in **detection** of interference using local GNSS monitoring systems. At sea and in ports eLoran meets international standards.

References

1 Royal Academy of Engineering 'Global Navigation Space Systems: Reliance and Vulnerabilities' 2011. Available at http://www.raeng.org.uk/publications/reports/global-navigation-space-systems

2 International Loran Association 'Enhanced Loran (eLoran) Definition Document' 2007. Available at https://rntfnd.org/wp-content/uploads/eLoran-Definition-Document-0-1-Released.pdf

3 US Federal Aviation Administration 'Loran's Capability to Mitigate the Impact of a GPS Outage on GPS Position, Navigation, and Time Applications' 2004. Available at https://rntfnd.org/wp-content/uploads/FAA-Report-2004-Lorans-Capability-to-Mitigate-the-Impact-of-a-GPS-Outage-on-GPS-PNT-Applications.pdf

4 Chronos Technology 'Delivering a national timescale using eLoran' 2014. Available at http://www.chronos.co.uk/files/pdfs/wps/Delivering_a_National_Timescale_Using_eLoran.pdf

5 McCall G 'Assured Position, Navigation, and Timing for the United States' American Center for Democracy 2016. Available at http://acdemocracy.org/assured-position-navigation-and-timing-for-the-united-states/#prettyPhoto

6 International Telecommunications Union 'Technical characteristics of methods of data transmission and interference protection for radionavigation services in the frequency bands between 70 and 130 kHz' 2001. Available at https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.589-3-200108-I!!PDF-E.pdf

7 International Bureau of Weights and Measures (BIPM) 'What time is it?'. Available at http://www.bipm.org/en/bipm-services/timescales/time-server.html

8 Raquet J and Miller M 'Issues and Approaches for Navigation Using Signals of Opportunity' Proceedings of the 2007 National Technical Meeting of The Institute of Navigation, San Diego, CA, January 2007, pages 1073-1080. Available at https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=12&ved=0ahUKEwinjoGaiqLWAhWJLMAKHcg0AJAQFghuMAs&url=https%3A%2F%2Fwww.sto.nato.int%2Fpublications%2FSTO%2520Meeting%2520Proceedings%2FRTO-MP-SET-104%2FMP-SET-104-09.pdf&usg=AFQjCNEogFFBgcIflLeGYEBA7i0Ukx8ZPw

9 Groves P, chapter 13 of 'Principles of GNSS, Inertial, and Multisensor Integrated Navigation Systems' 2nd Edition, Artech House 2013.

10 http://www.metoffice.gov.uk/services/public-sector/emergencies/space-weather

11 Curry C 'Dependency of Communications Systems on PNT Technology' Chronos Technology 2010. Available at http://www.chronos.co.uk/files/pdfs/wps/Dependency_of_Comms_on_PNT_Technology.pdf

12 Government Office for Science 'The quantum age: technological opportunities' 2016. Available at https://www.gov.uk/government/publications/quantum-technologies-blackett-review

13 Grejner-Brzezinska D and others 'Multisensor Navigation Systems: A Remedy for GNSS Vulnerabilities?' Proceedings of the IEEE 2016: volume 104 pages 1339-1353. Abstract available at http://ieeexplore.ieee.org/document/7441992/; Moore T and others 'The Potential Impact of GNSS/INS Integration on Maritime Navigation' Journal of Navigation 2008. Abstract available at https://www.cambridge.org/core/journals/journal-of-navigation/article/potential-impact-of-gnssins-integration-on-maritime-navigation/C51D4B30DB98DDE21FEF00DC555285A2

14 Fernandez-Prades C and others 'Robust GNSS Receivers by Array Signal Processing: Theory and Implementation' Proceedings of the IEEE 2016: volume 104 pages 1207-1220. Available at http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7444116

15 https://en.wikipedia.org/wiki/Receiver_autonomous_integrity_monitoring

16 Ofcom 'Statement on Authorisation regime for GNSS repeaters' 2012. Available at https://www.ofcom.org.uk/consultations-and-statements/category-3/gnss-repeaters/statement

17 http://ec.europa.eu/growth/sectors/electrical-engineering/red-directive_en

18 Curry C 'The Impact of the GPS UTC Anomaly Event of 26 January 2016 on the Global Timing Community' Proceedings of the 48th Annual Precise Time and Time Interval Systems and Applications Meeting, Monterey, California, January 2017: pages 164-170. Abstract available at https://www.ion.org/publications/abstract.cfm?articleID=14986

19 Tepper F 'The FAA gets a case study with a drone crash inside an MLB stadium' TechCrunch 2017. Available at https://techcrunch.com/2017/05/23/the-faa-gets-a-case-study-with-a-drone-crash-inside-an-mlb-stadium/

20 Spirent 'What is GPS Receiver testing?' https://www.spirent.com/go/What-is-GPS-Receiver-Testing

21 Chronos Technology 'GPS Antenna Installations Best Practice' http://www.chronos.co.uk/files/pdfs/cs-an/GPS-Installation-Best-Practice.pdf

22 Schuster W and Ochieng W 'Novel Integrity Concept for CAT III Precision Approaches and Taxiing: Extended GBAS (E-GBAS)' Journal of Navigation 2011: volume 64, pages 695–710.

23 Adjrad M and Groves P 'Enhancing Conventional GNSS Positioning with 3D Mapping Without Accurate Prior Knowledge' Proceedings of the 28th International Technical Meeting of The Satellite Division of the Institute of Navigation 2015: pages 2397-2409. Available at http://discovery.ucl.ac.uk/1472567/

Chapter 5: Standards and Testing

Fragmented standards

Standards can be a catalyst for economic growth. They enable innovation and boost productivity, and overall they even reduce the regulatory burden for businesses. In a 2015 report[1] by the Centre for Economics and Business Research, 36% of companies said that using standards increased their productivity, and 70% said that standards improved their supply chain by improving supplier products and services.

But for GNSS applications, the standards landscape is fragmented. Some types of GNSS device are not fully covered by standards. In other areas, new regulations have come into force to improve this situation, but businesses are often not yet aware or compliant. Of even more concern, existing standards are often ill-suited to critical national infrastructure.

Defining terms

Standard: refers to a terminology, principle, measure, test or level of quality that can be used for comparison.

Standardisation: refers to being designed, operated or manufactured in a standard manner. A set of equipment might be standardised and thus all be the same, yet not referenced to a formal standard.

Resilience: the ability to prepare for and adapt to changing conditions and recover from deliberate attacks, accidents, or naturally occurring threats.

Robustness: the ability to withstand threats without significant degradation or loss of performance.

Existing and new standards

Uses can be split into consumer, professional and safety-related areas, defined in Table 5.1:

Table 5.1
Three broad areas of GNSS use have different standards needs

	Used by	Typical device/area
Consumer	General public	Mobile phone or in-car satnav. Typical device cost £00s
Professional	GNSS specialists, surveyors, financial sector, telecommunications	Surveying, agriculture, high-value timing systems. Device cost £00s - £000s
Safety	Aviation, maritime, road, defence, rail	Safety-critical environments, highly regulated. Device cost £000s - £0,000s

Consumer

Until June 2017, consumer products that incorporate GNSS (such as in-car satnavs) only had to conform to standards associated with CE marking. These include the Radio & Telecommunications Terminal Equipment (R&TTE)[2], Low Voltage Directive (LVD)[3] and Electromagnetic Compliance (EMC)[4] directives from the EU. Standards under these directives do not address the specifics of GNSS (though the case of mobile phones is more complex – see box).

Now the Radio Equipment Directive (RED)[5] has come into force, covering all equipment that intentionally transmits or receives radio waves, including devices that receive GNSS signals.

RED will ensure that GNSS devices have a degree of resilience to any non-GNSS signals in nearby bands, and that they do not cause unintentional interference. Manufacturers need to prove the received GNSS signal will not degrade by more than one decibel when there is activity in adjacent frequency bands.

Products with the CE mark are safe and will work as designed, but there are no guarantees of robustness or resiliency to jamming, spoofing and cyber threats. For most consumer applications this is not a great concern, but future consumer devices that use GNSS within the Internet of Things and smart cities might be considered elements of critical infrastructure, where this needs to be addressed (see below).

Mobile telecoms

For mobile phones and other mobile telecom devices, the 3rd Generation Partnership Project (3GPP)[6] generates specifications that ensure interoperability of systems.

UK businesses play a leading role in 3GPP technical working groups, from device manufacturers to testing organisations and test equipment manufacturers. GNSS testing specifications in this context set out requirements for conformance to parameters such as:

- Accuracy and sensitivity
- Dynamic range
- Multipath and performance in moving conditions
- Operation under multiple network configuration and status

Manufacturers who demonstrate conformance to these specifications can sell their products to operators of mobile networks, and the consumer can be assured that the device meets a performance specification under any network conditions.

Professional

Professional grade GNSS receivers, used for example in precision farming and surveying, are those where the GNSS capability is the core component of the system. Unlike a phone or an in-car satnav, these devices may not work at all if GNSS fails. They may have multi-frequency capabilities, require accuracy of centimetres or less, require high-precision timing, and make differential corrections; and they often require some specialist knowledge to operate. They will generally have more capable electronics and vastly more capable antennas than those in the consumer domain.

Like consumer products, these are subject to RED, EMC, and LVD; but they are also subject to other standards to ensure that they can integrate into wider systems in a flexible way. For example, US National Marine Electronics Association standards[7] NMEA 0183 and 2000 define electrical and data communication specifications to enable connection of marine electronic devices such as echo sounders, sonars and GPS receivers. These standards are used in many GNSS devices as the standard output data format.

The main problem in this area is that there are no published performance standards that could be used directly to compare the resilience and robustness of one GNSS receiver or system against another. Instead, purchasers must rely on manufacturer specifications, or conduct their own comparative evaluation testing.

In the telecommunications sector, that problem has been addressed. The International Telecommunications Union develops the technical standards that ensure networks interconnect seamlessly. They include specifications for equipment output and performance, network clocks, and protocols that transport frequency and time around a network. Businesses must ensure they can demonstrate conformance to these interoperability standards, which form the basis of the current operation of global telecommunications and computer networks. These standards are very important in allowing network operators to build infrastructure that will support the fixed and mobile networks and the precise timing requirements of the future.

Financial standards

The new EU Directive on Markets in Financial Instruments II[8] empowers the European Securities and Markets Authority to develop regulatory technical standards and implement technical standards. These technical standards will come into force in January 2018, and specify for example that:

- The time reference used for synchronising business clocks used by operators of trading venues shall be Coordinated Universal Time (UTC).
- The maximum divergence from UTC can be either one millisecond or 100 microseconds based upon configurations. The granularity of the timestamps can be either 1 millisecond or 1 microsecond.
- Operators of trading venues must demonstrate traceability to UTC and deliver proof by documenting the system design and specs.

The source of UTC can be GNSS. Businesses must comply with the directive, assess their dependence on GNSS and engineer their systems for conformance to the standards. As conformance must also be demonstrated, there is now a need for more in-depth testing and validation.

Safety

Standards in the safety domain are different from other areas. With consumer and professional standards, policing and accreditation are light – reflecting the need to keep matters simple, otherwise the standards are self-defeating. Such a light regulatory environment is not appropriate when lives are at stake, so safety standards and critical standards take a more rigid, process-oriented approach. As a gauge of how serious the failure of a given system might be, standard IEC61508 describes how to calculate safety integrity levels: a scale that goes from 0 (no consequence) to 4 (catastrophic; loss of multiple lives).

Aviation, maritime and rail each have a structured, formalised safety culture and regulatory environment. This is defined by the International Civil Aviation Organisation (ICAO) and the International Maritime Organisation (IMO), and in the UK by the Rail Standards and Safety Board (RSSB). Standards set by the IMO and ICAO address systems approved for use, data processing techniques, safety of life at sea and navigation requirements. Their standards cover equipment specifications, operational procedures and international GNSS harmonisation.

For the UK rail sector, the RSSB has produced a guidance document[9] on the use of satellite positioning technology for location-dependent applications. It addresses applications such as:

- Automatic train protection
- Train integrity
- Trackside personnel protection
- Tilting trains
- Track discrimination and driver advisory systems
- Door operation and warning systems
- Passenger information systems

Although this guidance document is of high quality, it does not set out mandatory requirements or standards for the rail sector to adopt. The Department for Transport, Network Rail and RSSB should determine whether the guidance can be formalised into a mandatory standard. This would result in cost savings, due to more effective and common-practice use of location information across the rail network.

eCall and e112

An EU initiative known as eCall will bring rapid assistance to motorists involved in a collision anywhere in the European Union, by installing a device in all vehicles that will automatically dial 112 in the event of a serious accident, and send airbag deployment and impact sensor information, and position coordinates (primarily determined using Galileo), to local emergency agencies. This will be mandatory in all new cars sold within the EU after April 2018.

Standards are still being developed for eCall, as many manufacturers have produced proprietary solutions to be early to market. PNT is crucial to eCall, and as GNSS will not always be available, other solutions need to be found.

In Russia, a fully interoperable system called ERA-GLONASS is being deployed, with the aim to require an eCall terminal and a GPS/GLONASS receiver in future new vehicles.

Similar to the eCall initiative, e112 is a proposed enhancement to the 112 emergency number system across the EU. Today, when an emergency call is made, the telecoms operator transmits location information to the emergency centre — but the accuracy, using mobile cell or sector ID, ranges from 100 metres to 40 kilometres; emergency services

want 5 to 10 metres. So the EU is now considering a regulation to ensure devices such as tablets and mobile phones are equipped with Galileo and EGNOS chipsets, and so able to automatically send more accurate location data. It is not necessary to use Galileo and EGNOS to achieve e112, but the EU will use this initiative to drive market uptake of those systems. In the US, an equivalent concept for all calls to the 911 emergency number is already in place: e911.

Regulation and the associated standards are yet to be developed but are likely to follow the consumer route of RED, with accuracy performance criteria against which conformance can be demonstrated by testing.

The need for a unified approach

GNSS applications in critical services are not served well by the fragmented standards environment. Patchy coverage, an inconsistent approach and the multitude of international organisations all mean that for a system to exhibit and demonstrate resilience and robustness to the loss of GNSS, a great deal of effort must be expended to determine if any existing standards are suitable and relevant. What is more, critical applications need levels of resilience and robustness that are not addressed in any existing standards.

We need a single set of metrics to help designers and purchasers of critical-services systems assess robustness and resilience, including systems-of-systems vulnerabilities. In theory, one standard could cover all critical applications, defining performance metrics that encapsulate realistic targets – for example being able to operate for five days without GNSS. Equipment manufacturers and integrators could demonstrate conformance with new testing methodologies.

This approach of having one overarching standard is also recommended in the early results of the EU project STRIKE3[10], which is monitoring and analysing current best practice. The project is likely to propose receiver testing and threat reporting standards for the EU.

Testing

Standards alone are not enough. Customers need assurance that a product actually meets a standard. A certified testing organisation can provide this assurance by testing the product against a specification of compliance. Possible parameters are outlined in Table 5.2.

With GNSS applications, many companies either do minimal testing or fail to use proper methods. While some countries are providing guidance on this, the UK is not – even though GNSS testing is a UK strength. Two of the world's leading GNSS test equipment manufacturers[11] are based in the UK.

What, why and how

Tests examine the operation of receiver antennas, electronics and algorithms; they ensure that the receiver can operate in a larger system to accomplish its intended role; and they assess the ability of that system to withstand threats.

Any link in the supply chain from manufacturers to users may need to test a product to find out whether it is suitable for the job, and how robust it is to threats. Many applications require that conformance to standards or specifications is demonstrated, and the only repeatable way to do this is through testing. With 3GPP for example, only specialist GNSS testing capabilities can demonstrate conformity with specifications for interoperability.

A live test in a normal environment can be useful, but because the environment is constantly changing it is not repeatable. That is why many companies use specialist GNSS test equipment that can record and replay authentic GNSS signals or simulate signals. This way, devices can be tested under different conditions, or different devices can be compared under the same conditions.

However, there is no uniformity of approach across industrial sectors regarding the manner of testing. This has led to different products responding in different ways when GNSS is compromised.

Guidance needed for CNI

The US Department of Homeland Security has produced guidance[12] for installing and maintaining time and frequency sources in fixed locations, including the use of GNSS. It has also issued specific guidance[13] on developing and operating GPS equipment used by US critical infrastructure. This addresses issues such as mitigating systems against jamming and spoofing, common themes and recommended algorithms.

No such guidance is available for UK critical infrastructure. This means that contractors and government departments are operating in isolation and to different protection levels. To provide a minimum protection level of critical services in the UK, we should create a test methodology, guidance or test parameters for GNSS receivers, or ideally for the PNT capability within a system. This guidance could be based around the parameters of integrity, availability, continuity and accuracy (Table 5.2).

Table 5.2
Guidance for testing could focus on four parameters

Parameter	Detail
Availability	Time to first fix Re-acquisition time Operation in non-GNSS conditions, including timing outputs Long-term operation
Integrity	Operation in poor RF environments Operation under conditions of GNSS data/system errors Ability to flag when subject to interference
Continuity	Ability to switch between PNT sources, as necessary Continuous output, regardless of environmental conditions
Accuracy	Position and time accuracy within required parameters Accuracy specifications in harsh conditions

Critical services can show resilience and robustness by encouraging or mandating that equipment demonstrate conformity to a technical standard or guidance. For each service it should be possible to set minimum performance metrics for accuracy, integrity, availability and continuity of PNT. This will provide national authorities with assurance of the ability of those critical services to deliver assured PNT data in all expected environmental conditions. The EU STRIKE3 project, which includes UK industry as a partner, has started to propose testing standards and methods to assess performance of GNSS receivers under a range of interference threats. But the STRIKE3 project will not complete until 2019, and action should be taken before then.

Testing systems of systems

There seems to be a gap in UK capability in testing PNT at the systems-of-systems level. For example, how can we fully test a system where inputs from multiple sensors, GNSS, WiFi, Bluetooth, accelerometers and gyros are all blended together? Or how all the components of a car, fire engine or aircraft work together in all conditions and locations? On a sunny day in Oxfordshire, how do you conduct worst-case testing of the navigation and communications systems used by emergency services?

Some solutions exist but they can be complex and expensive. Live testing of these systems is difficult and can be dangerous. Imagine trying to test failure modes of new equipment in an aircraft – you would need to make the aircraft fail to do so. Organisations should invest more time and effort into these higher-level testing scenarios.

UK facilities

The UK has some world-class testing facilities: some at government or government linked locations such as the National Physical Laboratory, Satellite Applications Catapult and Dstl/ Ministry of Defence; others in the private sector such as MIRA, Raytheon and Spirent.

However, there is no central register or database of UK facilities for PNT testing, making it difficult for an organisation to obtain information on where it can carry out work or whether testing is possible. Creating such a database will greatly improve awareness for all organisations, and lower the barriers to access for small to medium sized businesses.

Conclusion

Many sectors have developed criteria and standards for specific GNSS applications, but these are often not related to critical services. We need a set of metrics that apply across critical services, focusing on robustness and resilience to GNSS and PNT issues. Conformance to these metrics can be demonstrated by developing an appropriate test framework and methodology, and carrying out the tests and analyses in UK facilities.

References

1 Centre for Economics and Business Research 'The economic contribution of standards to the UK economy' 2015. Available at https://www.bsigroup.com/LocalFiles/en-GB/standards/BSI-The-Economic-Contribution-of-Standards-to-the-UK-Economy-UK-EN.pdf

2 Directive 1999/5/EC of the European Parliament. Available at https://publications.europa.eu/en/publication-detail/-/publication/d84140b2-ec95-49fa-b88c-de819336ec4c/language-en

3 Low Voltage Directive (LVD) 2014/35/EU of the European Parliament. Avilable at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.096.01.0357.01.ENG

4 Directive 2014/30/EU of the European Parliament. Available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0030

5 Radio Equipment Directive (RED) 2014/53/EU of the European Parliament. Available at http://eur-lex.europa.eu/legal-content/GA/ALL/?uri=CELEX:32014L0053

6 http://www.3gpp.org/about-3gpp/about-3gpp

7 https://www.nmea.org/content/nmea_standards/nmea_standards.asp

8 Markets in Financial Instruments II Directive 2014/65/EU of the European Parliament. Available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0065

9 Rail Safety and Standards Board 'Guidance on the Use of On-Train Satellite Positioning Technology Based Locator for Railway Applications' 2015. Available at https://www.rssb.co.uk/rgs/standards/GEGN8578%20Iss%203.pdf

10 European Global Navigation Satellite Systems Agency 'Standardisation of GNSS Threat reporting and Receiver testing through International Knowledge Exchange, Experimentation and Exploitation' 2016. Available at https://www.gsa.europa.eu/standardisation-gnss-threat-reporting-and-receiver-testing-through-international-knowledge-exchange

11 Spirent Communications (Paignton, Devon) and Racelogic (Buckingham, Bucks)

12 US Department of Homeland Security 'Best Practices for Improved Robustness of Time and Frequency Sources in Fixed Locations' 2015. Available at https://www.dhs.gov/publication/best-practices-improved-robustness-time-and-frequency-sources-fixed-locations

13 US Department of Homeland Security 'Improving the Operation and Development of Global Positioning System (GPS) Equipment Used by Critical Infrastructure' . Available at https://ics-cert.us-cert.gov/Improving-Operation-and-Development-Global-Positioning-System-GPS-Equipment-Used-Critical

Acknowledgments

We are indebted to the expert panel for drafting the main body of this report and for their advice, which has shaped the recommendations set out in the executive summary. We also gratefully acknowledge the contributions of other individuals and organisations during the conduct of this review.

Chris Whitty, Mark Walport

Expert panel
Peter Briggs, Dstl
Prof Paul Cannon, University of Birmingham
Dr Paul Cruddace, Ordnance Survey
Prof Charles Curry, Chronos Technology
Mike Gilson, BT
Neil Horlock, Credit Suisse
Prof Sir Peter Knight, Imperial College London
Prof David Last, University of Bangor
Dr Leon Lobo, NPL
Roger McKinlay, Royal Institute of Navigation
Stuart Mann, National Grid
Dr Bob Mason, Terrafix
Prof Terry Moore, University of Nottingham
Prof Washington Ochieng, Imperial College London
Andy Proctor, Innovate UK
Prof Marek Ziebart, University College London

Contributors
Martin Bransby, General Lighthouse Authorities of the UK and Ireland
Guy Buesnel, Spirent Communications
Data Design Studios
Dr Mark Dumville, Nottingham Scientific
Prof Hugh Durrant-Whyte, Ministry of Defence
Paul Febvre, Satellite Applications Catapult
Dana Goward, Resilient PNT Foundation
Derwen Hinds, National Cyber Security Centre
Prof Todd Humphreys, University of Texas at Austin
Billy Marshall, Chronos Technology
Simon Mason, Arqiva
NPL
Royal Academy of Engineering
Trinity House

Review team
Dr Andrew Kaye
Dr Claudia Lally
Nicholas Williams

Editor
Dr Stephen Battersby

© Crown copyright 2018

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3 or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gsi.gov.uk.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication available from www.gov.uk/go-science

Contact us if you have any enquiries about this publication, including requests for alternative formats, at:

Government Office for Science
1 Victoria Street
London SW1H 0ET
Tel: 020 7215 5000
Email: contact@go-science.gsi.gov.uk