Society may already be dangerously over-reliant on satellite radio navigation systems like GPS, the Royal Academy of Engineering warned in a report published on 8th March. The range of applications using the technology is now so broad that, without adequate independent backup, signal failure or interference could potentially affect safety systems and other critical parts of the economy.

Global Navigation Space Systems: reliance and vulnerabilities, to give the full title, looks into the increasing use of global navigation satellite systems (GNSS) to gain accurate data for positioning, navigation and timing (PNT). The US-operated Global Positioning System (GPS) is best known as the first major implementation of this technology but other GNSS systems are being planned and built, including the Russian GLONASS and Europe’s Galileo.

The Academy’s report focuses on our increasing reliance on GNSS and the current limited use of GNSS-independent backups for PNT data. The vulnerabilities of GNSS to deliberate or accidental interference, both man-made (such as jamming) and natural (such as solar flares) are also highlighted.

GNSS dependency is now widespread across the UK. As well as the ubiquitous satnav, the signals are used by data networks, financial systems, shipping and air transport, agriculture, railways and emergency services. The European Commission, in its mid-term review of the European satellite radio navigation programmes (18th January 2011) estimated that an €800 billion chunk of the European economy is already dependent on GNSS.

All GNSS applications are vulnerable to failure, disruption and interference and the report looks at a range of possible consequences of these, from the inconvenient (such as passenger information system failures) to possible loss of life (such as interruptions to emergency services communications).

The severity of the errors may be so large as to give noticeably suspect results which can immediately be identified by the users, but the real threat lies in “dangerously misleading” results which may not seem obviously wrong – a ship directed slightly off course by faulty data could steer it into danger.
There is also a concern over the criminal use of jamming equipment to bypass GNSS systems – easily available technology can be used to block tracking of consignments of goods or to defraud systems that collect revenue using GNSS (such as toll-road charging).

Dr Martyn Thomas CBE FREng, Chairman of the Academy’s GNSS working group, said, “GPS and other GNSS are so useful and so cheap to build into equipment that we have become almost blindly reliant on the data they give us.

“A significant failure of GPS could cause lots of services to fail at the same time, including many that are thought to be completely independent of each other. The use of non-GNSS back ups is important across all critical uses of GNSS.”

The Academy’s report looks at security awareness and recommends that critical services include GNSS vulnerabilities in their risk register and that these are reviewed regularly and mitigated effectively. It says the provision of a widely available PNT service as an alternative to GNSS is an essential part of the national infrastructure – a terrestrial radio navigation system called eLORAN is already in development for this purpose.

The Academy also suggests policy responses including the closing of a legal loophole which allows the import, advertisement and possession of jamming devices. The UK government could trial the deliberate jamming of signals for a limited period to allow users to evaluate the impact of the loss of PNT data and the effectiveness of their back-up plans.

Finally, the Academy advises the creation of an R&D programme focused on antenna and receiver improvements that would enhance the resilience of GNSS dependent systems against natural and man-made threats.

Dr Thomas adds: “The deployment of Europe’s Galileo system will greatly improve the resilience of the combined GPS/Galileo system, but many of the vulnerabilities we have identified in this report will remain. No-one has a complete picture of the many ways in which we have become dependent on weak signals 12,000 miles above us.”

The Academy’s report, *Global Navigation Space Systems: reliance and vulnerabilities* is available online at [www.raeng.org/gnss](http://www.raeng.org/gnss)
Global Navigation Space Systems: reliance and vulnerabilities was prepared by a working group consisting of the following group of Academy Fellows and other experts, commenting in a personal capacity and not necessarily as representatives of their respective organisations:

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

Professor Jim Norton, Independent Director;

Alan Jones, Cotares Ltd;

Professor Andy Hopper FREng, University of Cambridge;

Nick Ward, General Lighthouse Authorities of the UK & Ireland;

Professor Paul Cannon FREng, Qinetiq;

Neil Ackroyd, Ordnance Survey;

Paul Cruddace, Ordnance Survey;

Martin Unwin, Surrey Satellite Technology Ltd

with contributions from:

Charles Curry, Chronos Technology Ltd;

Professor Washington Ochieng; Imperial College, London

Founded in 1976, The Royal Academy of Engineering promotes the engineering and technological welfare of the country. Its Fellowship – comprising the UK’s most eminent engineers – provides the leadership and expertise for the organisation’s activities, which focus on the relationships between engineering, technology, and the quality of life. The Academy provides independent and impartial advice to Government; works to secure the next generation of engineers; and provides a voice for Britain’s engineering community.