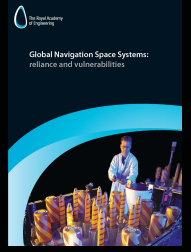
The Royal Academy
of Engineering

The Royal Academy of Engineering

Global Navigation SatelliteSystems
reliance and vulnerabilities

Martyn Thomas CBE FREng
3 August 2011

The Royal Academy of Engineering



The Study

Initiated in 2009 following a GAO report warning that GPS service levels might not be maintained

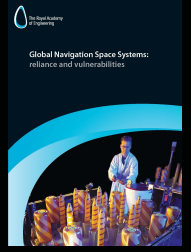
The RAEng had concerns that the degree of dependence on GNSS was not well understood

Our report was published in March 2011.

The Royal Academy of Engineering

Global Navigation Space Systems: reliance and vulnerabilities

The Royal Academy of Engineering



Report Contents

GNSS overview

The range of applications

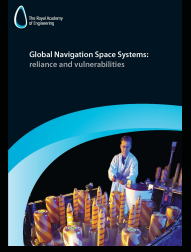
Vulnerabilities of GNSS services

Resilience to disruption of GNSS services

Conclusions and recommendations

Appendix: the General Lighthouse Authority Jamming Trials

The Royal Academy of Engineering



Intended audience for our report

Staff responsible for technical policy

- To help them to select appropriate PNT technology
- To inform risk analysis and risk management

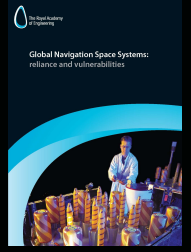
Industry regulators

- To help them to decide whether to introduce standards for PNT architectures in regulated applications

CPNI, Cabinet Office and Ofcom

- To help them to assess the CNI vulnerabilities
- To inform policy decisions

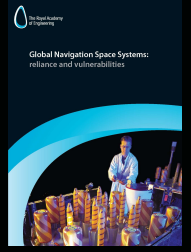
The Royal Academy of Engineering



The range of civil applications

- Rail
- Road
- Aviation
- Maritime
- Agriculture and Fisheries
- Energy
- Law Enforcement, Humanitarian
- Elderly and Disabled, Communications
- Financial & Banking, Surveying
- Scientific & Environmental
- Emergency Services
- Dredging

The Royal Academy of Engineering



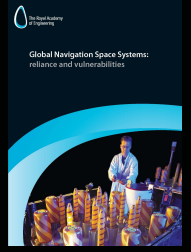
Vulnerabilities

Failure of the PNT service would cause common-cause failures of many applications that are otherwise independent and may be interrelated

For example, loss of PNT could lead to accidents, disruption to the emergency services, and loss of telecommunications

GNSS jammers are cheap, widely available and widely used: the JLOC detection network in the USA detects thousands of incidents each day

The Royal Academy of Engineering



Resilience: building high-integrity systems

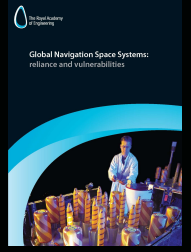
Protection: limited, high cost, some techniques are not available to civil users

Detection: limited (especially spoofing), fairly expensive

Backups are therefore essential

- Absence of common causes of failure
- This requires diversity - all GNSS systems share failure modes
- Manual systems are unlikely to provide effective backups unless they are frequently exercised

The Royal Academy of Engineering



Summary

Reliance on GNSS for PNT is high and increasing

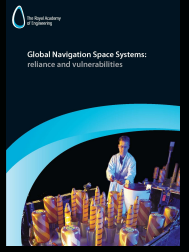
Risk from out-of-cycle solar events is unquantifiable

Risk from jamming is growing

Risk from spoofing is emerging and serious

GPS, Galileo and GLONASS have the same vulnerabilities

The Royal Academy of Engineering



Conclusions

The UK (like other developed countries) is already dangerously dependent on GPS as a source of PNT.

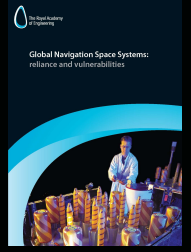
Backup systems are often inadequate or untested.

Jammers are too easily available and the risks are increasing.

No-one has a full picture of the dependencies and consequent vulnerabilities.

These risks could be mitigated cost-effectively.

The Royal Academy of Engineering



Recommendations

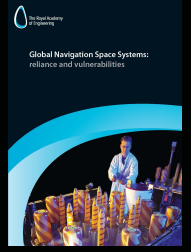
a) Raising awareness and analysing impact

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

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

3. Services that depend on GNSS for PNT, directly or indirectly, should document this as part of their service descriptions, and explain their contingency plans for GNSS outages of various durations.

The Royal Academy of Engineering

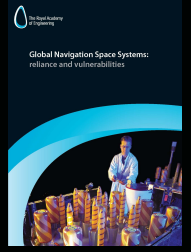


Recommendations

b) Policy responses

4. It is illegal to place GNSS jamming equipment on the market in the EU. The use of jammers is also a serious offence under the UK Wireless Telegraphy Act 2006. Ofcom has the ability to close remaining loopholes by putting in place a banning order under the 2006 Act which would prohibit import, advertisement and possession of jammers. We recommend that Ofcom should introduce such a banning order, ideally in co-operation with other European legislators.

The Royal Academy of Engineering



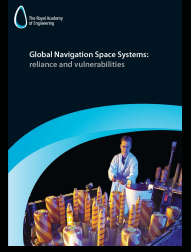
Recommendations

b) Policy responses

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

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

The Royal Academy of Engineering

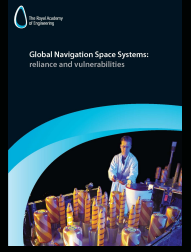


Recommendations

b) Policy responses

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

The Royal Academy of Engineering



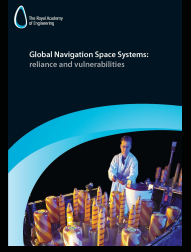
Recommendations

b) Policy responses

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

Greater cross-government coordination of S&T issues related to national security should explicitly recognise the importance of PNT treating it as an integral part of the operation of national infrastructure.

The Royal Academy of Engineering



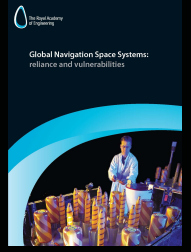
Recommendations

c) Increasing resilience

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

We are encouraged by progress with eLORAN in this context.

The Royal Academy of Engineering

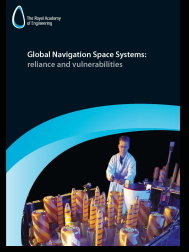


Recommendations

c) Increasing resilience

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

The Royal Academy of Engineering



To get free copies of the report

Contact Richard Ploszek, Senior Policy Advisor

The Royal Academy of Engineering

3 Carlton House Terrace, London SW1Y 5DG

richard.ploszek@raeng.org.uk

Or download from http://www.raeng.org.uk/gnss