GNSS Reliance and Vulnerabilities

In March this year, the Royal Academy of Engineering made headline news when it published a report on the UK's reliance on global navigation satellite systems (GNSS), and its consequent vulnerability to loss of such systems' availability.

The Academy's report makes ten recommendations to mitigate that vulnerability: three address awareness and impact, five propose policy responses, and two recommend ways of improving resilience. The leader of the study, Martyn Thomas, takes us on a whirlwind tour through the recommendations.

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.

It is quite common that managers who are responsible for important activities are unaware that the disruption of GNSS position, navigation or timing (PNT) signals would create problems for them. We recommend a thorough investigation of dependencies so that the risk registers are complete and effective mitigation strategies can be put in place.

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

Disruption of GNSS signals has the potential to create an emergency (perhaps as a result of a shipping accident) while simultaneously reducing the effectiveness of emergency response teams such as search-and-rescue.

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

Equipment and services may use GNSS indirectly, by relying on communications or timing signals that themselves depend directly or indirectly on GNSS. Tracing these indirect dependencies is important and it would be made much easier if all services clearly documented the extent of their reliance on GNSS.

No signal, satellite being jammed...

Policy Responses

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

The police are already recovering jammers that they suspect are being used illegally. It should be made harder to obtain jammers and easier to prosecute those who possess them without a legitimate need.

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.

GAARDIAN and SENTINEL provide the building blocks for networks of sensors that can detect problems with GNSS, alert users, and facilitate appropriate responses.

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.

It is very difficult for service providers or users to exercise their contingency plans while GNSS is working properly because they often do not know which of the equipment and services on which they depend will fail, or the nature of these failures when GNSS is jammed at low power and the interfering signal is gradually increased.

If it is considered too dangerous to jam GNSS *over a wide, urban area, then it must be urgent that a separate and diverse source of PNT data is made available.*

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.

If a new system such as Road User Charging is introduced and if jamming the GNSS signals will allow road users to escape the charges, it creates a strong incentive to jam, and the consequences for other users of GNSS could be serious. Such perverse incentives can often be avoided with careful system design.

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

A typical jammer, now available.

A single Government agency should have overall responsibility for ensuring the continued availability of PNT data. Otherwise it will fall into the gaps between Departments and inadequate attention will be paid to strategic risks and opportunities.

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 blindspots. We are encouraged by progress with eLoran in this context.

If a diverse source of PNT signals is made available, with a commitment to maintain the service for many years, then the new system will gradually be built into new equipment. This will greatly reduce the costs for users to provide their own backup systems and will eliminate many of the vulnerabilities that currently exist.

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 TSB should stimulate the wider use of the existing best practice technologies. We believe that further research could lead to additional improvements in effectiveness, cost or practicality of technologies for improved PNT resilience.

Read The Whole Report

This whistle-stop tour gives only the highlights and recommendations of the RAEng report in a handy form. For more depth, the full report is highly recommended, and available to download free online. Go to www.raeng.org.uk/news/publications/list/mostrecent.htm