GETTING OUT OF A JAM

DEVICES TO JAM GPS SIGNALS ALREADY EXIST AND GPS 'SPOOFING' HAS BEEN SHOWN TO WORK IN PRACTICE. BUT HOW BIG ARE THE THREATS AND WHAT CAN YOU DO TO MITIGATE PROBLEMS? GUY BUESNEL LOOKS AT HOW YOU CAN ASSESS THE RISKS

A lot has been written about the vulnerabilities of GNSS to signal disruption through jamming, spoofing or the effects of solar weather. Reading much of the material on this, one can be left with the feeling that GNSS is too vulnerable, that the low strength of its signals means that it is inherently unsuitable as the world's primary source of precision position, navigation and timing.

We know a great deal about the mechanisms that have the potential to disrupt GNSS signals but an often neglected point is how likely is it that a system will encounter disruption in normal use and what is the impact on the system if it does? This really deserves a good answer. If typical users will rarely encounter GNSS disruption and if they do, that disruption in terms of degraded availability or performance is minimal, then very little or no mitigation is likely to be required. On the other hand, if typical users can expect to regularly encounter GNSS disruptions that significantly affect availability and performance, then there is a good case for improving system resilience.

It's becoming progressively easier to get hold of jammers that can produce disruptive interference. Many websites sell unobtrusive 'personal privacy devices' (PPDs) that plug into a vehicle's cigarette lighter. These devices emit radio waves on common satellite frequencies, preventing equipment – such as SatNav or telematics systems – from receiving and processing satellite signals. The system is unable to calculate or report its own position or provide precise timing information while the jammer is on.

Jamming could be a threat to all businesses and industries that rely on GNSS for their operations. This includes the construction industry, where GNSS is used for surveying and where precise position and timing information from GNSS is used to track heavy vehicles and machinery. For instance, in the US, many concrete trucks are equipped with GNSS for tracking as it is important to deliver a correct mix to the customer in a very timely manner. Jamming has the potential for causing significant disruption to these kind of operations.

laboratory conditions. Today, it is possible to simulate a variety of GNSS jamming scenarios with real-world PPD-like interference waveforms or to simulate crude or more sophisticated varieties of spoofing attack, with key system parameters being continuously monitored. In this way any unexpected or unwanted system behaviour can be identified and characterised and the potential impact to operations assessed. This is really a vulnerability audit of the system.

Once all this information has been collected, collated and analysed, it becomes much easier for an informed decision to be made on the most cost-effective mitigation techniques, which depending on the scale of the identified problems, can range from the introduction of simple operational guidelines to the inclusion of a complementary (or back-up) system, such as eLORAN, which is a ground based 2-D fixing system. eLORAN signals are far less susceptible to interference than GNSS, given the much higher power level of the signals.

Father says

Bradford Parkinson is widely recognised as being the father of GPS. In 1973 he became manager of the Navstar GPS development programme, and he is a key member of the US National Space-Based Positioning, Navigation, and Timing (PNT) Advisory Board, which provides independent advice to the US government on GPS-related policy, planning, programme management, and funding profiles in relation to the current state of satellite navigation services. He says we must learn to 'protect, toughen and augment' GNSS to ensure that it meets users' needs. Protection is about taking pre-actions such as legislation, and re-acting when interference or spoofing occurs. Toughening is about making' equipment more resilient to GPS/GNSS threats. Augmenting is about using substitute PNT sources such as eLORAN or inertial sensors as a complement to existing GNSS.

Effective risk assessment fits in with this framework. Knowing the impact of GNSS threats on the operation of your business may give you tools that will help you lobby politicians and industry bodies for improved legislation or standards, whilst practically, this knowledge will also likely provide 'quick win' methods for improving the overall resilience of your system. It is also clear that a deep understanding of GNSS threat evolution in the real world is required to keep up to date with the development of technologies that are being used to attack PNT systems..

WE MUST LEARN TO 'PROTECT, TOUGHEN AND AUGMENT' GNSS TO ENSURE THAT IT MEETS USERS' NEEDS

Guy Buesnel is product manager GNSS vulnerabilities at Spirent (www.spirent.com)

A broadcast tower that uses GPS for precise timing

Container ship using GPS for navigation