Answering the Call for a GNSS Back-up

The team behind the new report on the economic impact for the UK of a GNSS disruption says eLoran is an option, a good option, but not the only option to back up GNSS. Meanwhile, concerns about the potential ramifications of a widespread GNSS failure, long expressed by voices in the United States and UK, may now be taking hold in the European Union.

PETER GUTIERREZ, *Inside GNSS*'s European correspondent, is a senior reporter and editor based in Brussels, Belgium, who has written about Europe's GNSS programs for many years. He received his bachelor's degree from the University of Texas at Austin and a M.S. degree from the University of Massachusetts at Amherst.

A government report commissioned by Innovate UK, along with the UK Space Agency and the Royal Institute of Navigation, entitled "Economic impact to the UK of a disruption to GNSS", comes in the wake of troubling incidents for GNSS operators, both the United States and Europe.

Last year a problem with the GPS satellite timing signal triggered alarms and caused an unknown number of outages, and in Europe earlier this year the fledgling Galileo signal crashed due to unspecified ground facility issues.

"We wanted to know the economics behind a loss of GNSS, and if there are innovations in the GNSS market we should be investing in, perhaps addressing GNSS vulnerability or new technology integration," said Andy Proctor. "Understanding the economics of a GNSS worst-case situation has not been done in the UK before."

Proctor, who chairs the UK Government PNT Group, commissioned the UK GNSS vulnerability report for Innovate UK, an executive non-departmental public body sponsored by the Department for Business, Energy & Industrial Strategy.

"Innovate UK is a Government Agency," Proctor said, "a non-departmental body, which means we work in a cross-government way, talking to all departments regularly. We invest, mostly via grants, into UK businesses to stimulate economic growth, unlock R&D and market barriers and address market failures."

Of crucial concern to Proctor and Innovate UK is the fact that while GNSS is a widespread technology, the full extent and nature of its use, as well as the resilience of its users to disruption, has not yet been understood.

The lead researcher and writer of the report is Greg Sadlier, Divisional Director, Space, at London Economics.

"We do lots of GNSS work," Sadlier said. "We actually lead a consortium that does research for the European GNSS Agency (GSA) market analysis report. So, we do a lot behind the scenes in Europe space and also in the UK space policy environment.

"Given the substantial use of GNSS in the UK, the question was do we need to worry about resilience and, if so, to what extent."

What is Vulnerability?

Although the report is not strictly concerned with defining the possible causes of a major GNSS outage, who or what the possible culprits might be is pretty clear.

For example, there is space weather; when the solar winds are acting up, satellite signals propagating through the Earth's atmosphere can be profoundly affected. Indeed, the solar weather scenario was the basis for the chosen duration of the envisaged GNSS crash described in the report.

"For the study," Proctor explained, "I decided upon a five-day duration, as it links in with scenarios in the national risk register, the space weather impact reports such as that from the Royal Academy of Engineering, and also the UK Government Space Weather Preparedness Strategy."

But, he said, the GNSS signal could also be deliberately attacked. Terrorists can buy or build a jammer that is powerful enough to affect large areas of a major city from a publicly accessible location. Indeed, with a simple multi-frequency jammer, now easily available, any person can knock out all L1 to L5 bands, meaning GPS, Wide Area Augmentation System (WAAS), Galileo, EGNOS, and the rest. Finally, satellite components and/or ground-based systems can fail.

"It should be noted," Sadlier said, "that the overall impact of an outage of GNSS is not necessarily independent of the source of the disruption: e.g., a severe natural space weather event causing a loss of GNSS may also cause an outage of other (satellite) services, including communications, broadcasting, meteorological, earth observation, as well as power supply."

Stark Terms

The report finds that the UK could lose £1 billion per day (about $1.263 billion) if GNSS were to go down. And such a crash would cause more than just financial losses, as everyday essential activities would also be affected, including emergency care and mass transportation. A lack of GNSS would hit navigation hard, but would also affect multiple industries that need it for mapping, tracking and timing.

The report explains how GNSS is used, what part it plays in a variety of systems, as well as how resilient those systems are in the case of GNSS disruption across 10 application domains: road, rail, aviation, maritime, food, emergency and justice services, surveying, location-based services (LBS), other infrastructure, and other applications.

What was probably already clear to some and what will be alarming to many others is the finding that all critical national infrastructures in the UK rely on GNSS to some extent, with communications, emergency services, finance, and transport identified as particularly intensive users.

This vast reliance on GNSS has developed over decades, based on widespread assumptions about availability and continuity. GNSS is also a primary input for transport, including road, air, maritime, and rail transport, as it is in agriculture, surveying, and for the legal professions.

The UK space industry derived an estimated turnover of £1.7 billion (about $2.15 billion) from PNT services in 2014-15, supporting 4,000 jobs, while sectors generating a total of £206 billion (about $260 billion) in gross value added (11.3% of UK GDP) are supported directly by GNSS. But the crucial role played by GNSS in national infrastructures means that an even wider range of economic activities is underpinned by GNSS indirectly. Proctor also noted that there were many areas where the impact of a GNSS disruption was difficult to monetize, so that the final estimates arrived at in the report are likely to be low.

"We always expected the transport sector to be heavily impacted," Proctor said, "but most surprising to me was the level of reliance of the maritime sector. I just didn't think it would be so great, and this is something that sector in particular should take a look at and consider."

Indeed, in the maritime navigation sector, GNSS is now widely treated as the sole necessary navigation solution. Virtually all traditional and even more recent back-up systems have simply disappeared, such that all other means of navigation have been replaced by GNSS.

The "Vulnerability Community"

The report will certainly be welcomed by the so-called "vulnerability community", a loosely connected band of determined individuals that includes the likes of Dana Goward of the Resilient Navigation and Timing Foundation, who has been trying to ram home the GNSS vulnerability message for years.

The "Vulnies" also include eminent personalities such as Professor David Last, Past-President of the Royal Institute of Navigation, and even the venerable Brad Parkinson, "Father of GPS". All of these and other figures have appeared at industry and policy events with messages not so much of doom and gloom, but of beware and prepare.

They believe it is perfectly right to point out the potential vulnerabilities of satellite-based navigation, so that the widening array of critical GNSS-supported operations can be appropriately safeguarded.

EU Heeds the Call

So far, no government seems to have moved very far towards answering the call for a GNSS back-up system. The European Union (EU) is no exception. Indeed, until very recently, anyone trying to get a serious answer from the European Commission (EC) on the question of GNSS vulnerability might have assumed the Commission hadn't given the issue much thought at all.

The EU's avoidance of questions about GNSS vulnerability is probably understandable, if nothing else on a human level. After more than 20 years of bleeding, sweating and crying tears on the road to an operational Galileo system, the last thing those folks will want to hear is "'Oh, by the way, Galileo is not resilient enough so we need to look for something else".

Attention is sometimes diverted by talk of the Galileo Public Regulated Service, the vaunted, military-like PRS. But it is generally expected that only a small proportion of Galileo users will have access to the PRS, and while it may be more robust, it will certainly not be immune to a wide-scale GNSS outage, either natural or man-made.

But the EU's reluctance to look GNSS vulnerability square in the face may be changing. Inside GNSS recently reported, as per unnamed sources, that the Commission is funding a study in support of a European radionavigation plan, and that the study discusses the need for resilient PNT and looks at using terrestrial systems as well as space-based signals. This again will be music to the ears of the vulnerability squad.

Meanwhile, the European Space Agency (ESA), it appears, is also taking a broader perspective in its new navigation endeavors, describing a PNT effort, not a GNSS one, with a strong emphasis on hybrid systems.

In a recent conversation, one highly placed source within ESA said the Agency is "very conscious" of the vulnerabilities of GNSS, including Galileo. "The more these systems are used the more vulnerable they are," our source told us. "I think we are still at an early stage in terms of market penetration. The number of users is still very low compared to what it will be in the future. There is a growing awareness, and we are at the correct stage to start implementing solutions to address vulnerability."

Proctor said he too senses an increasing understanding of the vulnerabilities of GNSS across the EU. "There is still a lot of awareness to raise I believe, as GNSS has become proliferate and often embedded in systems sometimes without risk managers being aware."

Back-up Options

Sadlier referred us to a full range of possible back-up systems considered in the report, from clocks and sextants to determine position at sea, or the use of old paper maps on the road, to more modern technologies such as radar systems.

"The aviation sector can make use of a number of existing back-up systems," he said, "but there is currently no 'universally applicable' alternative to GNSS for the case of positioning and navigation, and many of the traditional means of navigation might not be readily available or useable, depending on the individual application." True enough, my sextant went missing years ago.

For timing applications, Sadlier said, loss of GNSS can be mitigated by using adequate oscillators in the GNSS timing receiver that can hold time for a certain holdover period, ranging from a few minutes to many months. However, higher quality equipment with longer holdover periods is more expensive. Hence, loss of the GNSS signal will still affect sectors relying on its timing capabilities.

Of Course, eLoran

It seems any talk of GNSS vulnerability inevitably leads to the topic of eLoran. The two seem permanently linked. So much so that some have wondered whether the vulnerability "scare" isn't just a pretense for the "eLoran folks" to get their pet technology funded.

On the other hand, it is just as possible that eLoran is constantly being put forward because it is in fact the best single back-up option. As reports of movement towards establishing eLoran as a potential back-up system continue to circulate in the United States, a glance in Europe's direction also reveals a number of old Loran C navigation sites that could support an eLoran service as a back-up for GPS and Galileo.

Proctor said he was careful not to try to tip the scales when commissioning the report. "Yes, it's true, a lot of people seem to have been talking about eLoran lately. But when we commissioned the report we didn't lead Greg [Sadlier] in any way in terms of which potential back-up systems should be favored. As I have consistently said, I do not see eLoran as a cure-all for every case."

And STL?

Another technology currently making waves is called Satellite Time and Location (STL). The Satelles company is using existing low-earth-orbit Iridium satellites, normally used for communications, to deliver a powerful signal for accurate and resilient positioning, navigation and timing that works anywhere, including indoors.

The STL signal is about 1000 times more powerful than GNSS signals, and it has some built-in cryptography elements, making STL easier to "hear" in difficult locations and harder to jam or spoof, compared to GNSS.

However, as with all other options, STL has its limitations. As Satelles' Senior Radio Frequency Hardware Systems Engineer Stewart Cobb explained to us last December in Noordwijk, "STL works a lot like the old transit system where you watch a satellite go overhead and you take a series of fixes and between them you figure out your position. With GPS you need four satellites to get a fix, but generally you can see 10 or 12 so you can get a fix almost instantaneously. Basically, with STL it's going to take longer to get a precise fix."

Looking at the array of solutions examined in the report, Sadlier said, "The most applicable mitigation strategies for the largest number of applications are eLoran and STL. These high-availability services could mitigate many of the detriments in the maritime sector, and while the accuracy is insufficient for container stacking and autonomous cranes, the ability to schedule port operations and reduce downtime would help keep ports open."

The cost of resurrecting eLoran to a usable level, he said, would be on the order of £50m over 15 years (or about $65.1 million). The cost of STL is still unclear at this early stage in its development.

Proctor also suggested the best solution is likely to involve a combination of technologies. "The combination of eLoran and STL likely would give the broadest coverage in the event of an extended GNSS outage," he said.

The report identified Omnisense SP500 and Locata as possible preferred solutions for localized applications that require high levels of accuracy.

"Timing applications have been found to be resilient to a five-day outage of GNSS," Sadlier said, "but one could implement eLoran, STL, Locata or freely-available Network Time Protocol (NTP) servers as a source of timing for low accuracy applications. If higher accuracy is required, Precision Time Protocols (PTP) or time-over fiber networks, like NPL Time, are two alternatives."

Obstacles of the Political Kind

Proctor said there are three key target audiences for the report. First is the GNSS community itself. "This is a real evidence-based report," he said. "As such it is a resource for the industry in question. There is new factual information here, real figures about the real world."

Second, he said, is the infrastructure operators, the users. "It's for all of those people and organizations whose equipment needs GNSS to function. This applies all the way down in the supply chain to the general public, people who are already dependent on GNSS and may not even know it."

Finally, there are the policy makers, who need to understand and who may be in a position to say yes or no to funding initiatives.

"Personally, I believe there can always be more awareness of the benefits of GNSS and also the vulnerabilities associated with using it," Proctor said. "Perhaps the blockages are where GNSS has become cheap to procure and implement, so assessing the costs of using an additional technology to back it up, when it rarely fails, is a difficult sell."

The UK GNSS Vulnerability report is one of two PNT-focused studies recently commissioned in the UK, the other being a high-level Blackett Review, both of which will provide a well-rounded picture of the PNT-related economic and technical challenges faced by the UK, including critical infrastructure dependencies. IG