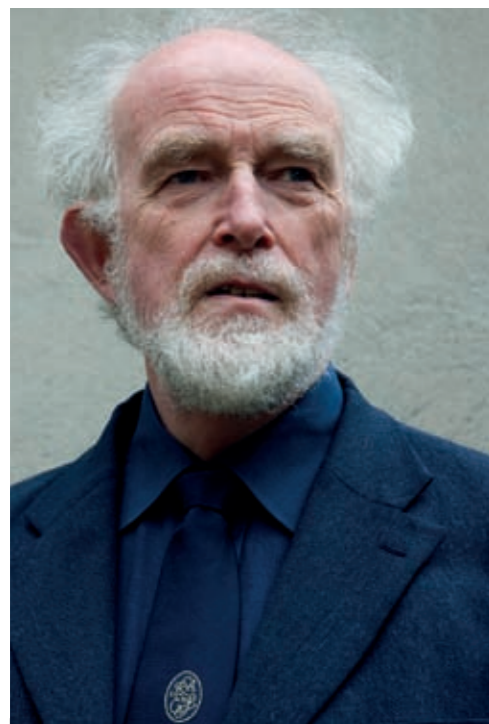


OPINION: GLOBAL NAVIGATION SATELLITE SYSTEMS

– ACCIDENTAL SYSTEMS AND UNINTENDED CONSEQUENCES



Dr Martyn Thomas CBE FREng

The free-to-use Global Positioning System and other satellite navigation services have resulted in applications so pervasive that there is now a real threat to global security if the systems should fail. Dr Martyn Thomas CBE FREng maintains that a radio-based system that could provide essential backup is now under threat from funding cuts.

Sometimes brilliant engineering leads to unexpected problems. GPS, the first and best known Global Navigation Satellite System (GNSS), has been so successful that more and more activities have come to depend on it for accurate data on position, navigation and timing (PNT).

Some of these activities are surprising and many have safety implications. Some are so important that if there is a significant risk that the satellite signal might fail, then there is an urgent need for a backup. There is a danger that eLORAN – a diverse source of PNT that could be widely available and used as a backup to GNSS – may be switched off just as the world wakes up to the fact that it is urgently needed. This must not happen.

GPS was conceived as a military system. However, when Korean airliner KAL 007 accidentally flew into Soviet airspace and was shot down, Ronald Reagan announced

that the USA would make GPS available for civilian use. Other types of GNSS – GLONASS (Russia), Galileo (Europe) and Compass (China) – have followed. The existence of these freely available and precise sources of PNT has triggered the development of a remarkable range of applications.

GNSS signals are used internationally by almost every industry: rail, road, aviation, space, maritime, agriculture, energy, surveying, construction, law enforcement and telecommunications. Some uses are important for safety, such as those that control the location, dispatch and navigation of ambulances, or help ships to enter harbour and dock safely, or support search and rescue operations.

Some uses of GNSS are important commercially, such as road user charging or time-stamping of financial trades. Some support national infrastructure such as power or telecommunications. Some are

important for protection of the environment, from landslide detection to the enforcement of fishing limits.

This dependence on GNSS connects many otherwise independent services into an 'accidental system' with a single point of failure: the satellite PNT signal. In an urban area, an erroneous GPS signal could cause road accidents while disrupting the dispatch and navigation of emergency vehicles and their communications. At sea – in fog or at night – jamming could cause collisions between ships or with obstructions and lead emergency beacons to broadcast false positions, delaying search and rescue.

No one has oversight of the increasing range of services that depend on GNSS or the increasingly complex ways in which they interact.

A satellite signal is a weak foundation for important services, and GPS signals are less than 10^{-16} Watts when received, even with a clear sky. A satellite signal can fail in dozens of ways. While some of these failures would disrupt the signal from only one satellite, others, such as incorrect data upload, could affect a whole constellation of satellites. Other failures, resulting from extreme solar activity, harmonics from legitimate broadcasts, or deliberate jamming, could affect the signal from all GNSS services.

GPS jammers are readily available. Circuits can be found on the internet, and commercially built jammers cost as little as US\$20. Some models jam all GNSS frequencies (and all mobile telephone frequencies as a bonus). The police have recovered jammers from car thieves and other criminals in the UK. Some lorry and company-car drivers use jammers so their employers cannot tell where they are. Every time GNSS signals are used for an unpopular

application, such as road user charging, the incentives to jam the signals become stronger and increase the risk that jamming will impact critical services.

Most of the commercially available jammers are short range, though at least one has a reported power of 25W, which could affect receivers across hundreds of square miles. Recent tests by the Ministry of Defence and Trinity House, the Lighthouse Authority, have demonstrated that the effects of jamming are unpredictable: even receivers specially built for use in critical applications may shut down, give absurd results or show plausible but incorrect information.

Although it is illegal to use jammers in the UK, there is no law against buying, importing or possessing them. It is to be hoped that the next Government will legislate to plug this hole. As made clear by a recent seminar organised by the Digital Systems Knowledge Transfer Network of the Technology Strategy Board and the Royal Institute of Navigation, GNSS jamming, deliberate or accidental, is a "clear and present danger".

The solution to a single point of failure of PNT is to have a second source that, if it fails, does so independently. This cannot be another satellite system because a jamming signal or solar storm that disrupted GPS could also disrupt Galileo and GLONASS.

Important applications should not, therefore, depend on GNSS signals as their only source of PNT but should have a diverse backup that uses local atomic clocks, terrestrial radio transmitters or another source whose stability is guaranteed to be wholly independent from GNSS.

Ideally, there should be a widely available source of PNT data that is highly likely to continue working if GNSS fails or satellite

signals are jammed. Enhanced LORAN (eLORAN) – a network of powerful terrestrial radio transmitters that broadcasts PNT data completely independently from GNSS – is a strong candidate.

Unfortunately, eLORAN is under threat because the modest funding needed to keep the service running in the UK is under review by the Department of Transport. In the USA, the older LORAN-C service was terminated earlier this year and the sites, towers and network that would be needed for eLORAN may be decommissioned. In view of the vulnerabilities of GNSS, the medium-term future of eLORAN needs to be guaranteed urgently. We cannot afford to wait for the disruption of GNSS to prove just how much we depend on these satellites to maintain essential services.

BIOGRAPHY – Dr Martyn Thomas CBE FREng

Dr Martyn Thomas founded the software engineering company *Praxis* in 1983 and was Chairman until 1996. He now acts as an independent expert witness where complex software engineering issues are involved. He was awarded a CBE in 2007 for services to software engineering.

Dr Martyn Thomas has been chairing an Academy study working group that has been looking at GNSS vulnerabilities and reliance. Their report is due to be published in late summer 2010.