OR BETTER NOT?

Challenging GNSS Vulnerability?

The reasons for GPS vulnerability due to interference are explained and reasons behind the system being designed as it is today discussed. In addition, consideration is given to why some new developments in future satellite signal structures must meet certain constraints due to United States and NATO national security issues.

The impact of GPS on all maritime operations is immense; one would hardly know what to do were it ever to fail in what it generally does. But unlike in many fairy tales, real life may be a little harsher than ideal; a simple little box may deny our access to the marvellous GPS, surprising us in any place and at any time. No reason to panic, though; we need only recognise this potential risk and act accordingly. The little risk is called interference, either unintentional or intentional. The reader might wonder how this advanced satellite system could ever be vulnerable to interference. Is this due to a less optimal system design, or are our receivers just not good enough? None of this. The reasons have simply to do with physics, economics, politics and the military.

The satellite system has been designed to offer world-wide 3D position determination at any time of the day and year. This was possible with a 24 satellite constellation. A further requirement was that the userâ€™s antenna should be a simple device; one that was sensitive to signals coming from all directions above the horizon and not any sort of dish which needed to be pointed towards a satellite. The result was an accurate and versatile navigation system which has millions of users world-wide today. Its performance is so impressive that, up until some years ago, there was almost full consensus that all other radio navigation systems world-wide could be phased out, leading to large cost savings.

Unfortunately, however, this marvellous system also has some weaker points: it proved to be susbceptible to interference. In the early stages of satellite navigation this mechanism was widely ignored, except by the military. But as more and more users became aware of this phenomenon, a thorough investigation was initiated by a US Presidential Directive. This was carried out by the Department of Transportationâ€™s Volpe Center and the outcome, the so-called Volpe Report on the vulnerability of GPS made public on 10 September 2001, has attracted considerable international attention. So that apparently there is indeed a problem to be solved. But let us start with the question of why GPS and other current and future satellite navigation systems are often vulnerable to interference.

Signal Robustness Versus National Security

About 27 GPS satellites are currently in orbit and operational. From a height of approximately 20,200km, each satellite has a view of some 38 per cent of the entire earthâ€™s surface. The satellite transmitter, with an output power in the order of 100 Watts, illuminates this 38 per cent, equivalent to 200 million square kilometres, through a special beam-forming antenna. No wonder that we will receive a very weak signal at the userâ€™s position (Figure 1). Standard receiver antennas output the unimaginably low electric power of just -160 dBW, or one tenthousands of a millionth of a millionth of one Watt. Please note that it is not the distance of the satellite to the user but rather the area that must be illuminated that determines the received power at the antenna. The chosen modulation type of the satellite signals, known as spread spectrum, means that the receiver is still capable of accurately measuring the time of arrival of these extremely weak signals.

These measurements form the basic information from which the user position, actually the antenna position, is derived.

Although the GPS signal structure has some built-in interference rejection capability, interference signals that are about 10,000 times more powerful than the satellite signals cannot easily and effectively be rejected by simple technical means. So any interference received by the GPS antenna which is stronger than one millionth of a millionth of one Watt may harm the GPS C/A signals. This is quite alarming, as a small cellphone size jammer can easily output a signal of 2 Watts. According to the Volpe Report (http://www.navcen.uscg.gov) such units might prevent proper operation of a GPS receiver at distances of up to tens of kilometres. Just imagine what â€˜naughty boysâ€™ could do! Figure 2 shows a small research test jammer with an output of just 1 milliwatt. This little unit denies L1 C/A GPS operations within a range of 100 metres from the small box.

Is GPS Vulnerability Always Annoying?

The reader may wonder why satellites in fact have such low power transmitters and why the signal structure is not made more robust against interference. The power question is difficult to solve for the simple reason that all electric power used by a satellite must be generated by solar cells. Even if the solar cell generator and the transmitted power were both increased by a factor of ten, then the jamming signal would too need only to be stronger by the same ratio: increased from 1 to just 10 mW. The next question is whether it would be possible to design satellite signal structures that were much more robust against interference than the ones used right now. Yes, that could be done. However, another problem would then arise.

The US and NATO military forces consider GPS also as a potential risk. A small aeroplane filled with explosives and equipped with an autopilot and a GPS receiver could make a poor-manâ€™s cruise missile. This might be one good reason why the military are eager to have the capability of deny GPS to users in selected areas. So if GPS signals are to be far more robust than they are today, the military would need more powerful and advanced jammers to deny GPS if needed.

But jamming of GPS on the part of the military must not render the same system useless to themselves. Thus future GPS satellites (IIR-M,

IIF and GPS-III) will broadcast special encrypted M-code signals. These signals use frequency bands just outside the GPS C/A code L1 and L2 bands. In this way, civil user signals may be jammed without simultaneously destroying military signals. The M-code is encrypted to deny its navigation service to unauthorised persons. As some â€˜unfriendlyâ€™ persons wishing to jam M-code signals to increase their â€˜life expectancyâ€™, they will face a much bigger problem for the simple reason that M-code signals are far more robust than C/A codes. The launch of these M-code satellites is planned to start in 2004.
A very interesting point is the development of the European counterpart of GPS, Galileo, due to become operational in 2008. The interoperability of both systems offers many benefits to the civil user with respect to availability and integrity in areas with signal shadowing. The Europeans planned to include in Galileo a highly secure signal for Public Regulated Services (PRS). This signal is also encrypted and quite resistant to interference. Interestingly, the Europeans have for this special service the same frequency bands in mind as do the US for their M-code signals. As the US want to be able to deny all navigation signals to non-authorised users, they would like to keep control over denial of the Galileo signals too. However, the overlaying of the signals makes Galileo-PRS jamming by NATO more difficult if M-code signals are not too to be endangered. This delicate overlay discussion between the â€˜oldâ€™ and the â€˜newâ€™ continent was not yet solved at the time of writing this article.

Solutions?

The original designers of GPS may not have foreseen the enormous impact of their work at that time, more than two decades ago. The military originators of GPS must have experienced periods of euphoria but also of worry when they realised how its high accuracy could also backfire. This lead to the introduction of the intentional degradation of the GPS signals, known as Selective Availability (SA). The quickly developing civil market for GPS counteracted SA by a number of free-of-charge Differential GPS (DGPS) services, like IALA radio beacons along the coasts of many countries, Nation-wide DGPS (NDGPS) in the US, Eurofix in Europe (Figures 3, 4 and 5) and many others. To improve integrity and to make DGPS widely available the US-Wide Area Augmentation System (WAAS), the European Geostationary Navigation Overlay Service (EGNOS) and the Japanese MSAS will soon become operational. So that SA became ineffective and therefore has been set to zero in May 2000. But we got advanced jamming technologies in return. An oscillating scenario may clearly be observed in which pushing and slowing-down activities will hopefully eventually lead to a balance between the user advantages and national security risks of precise navigation systems.
The question remains of what the risk of interference means to the civilian user. Realising that a civil GPS receiver can be jammed may cause interruptions in the navigation process of vessels, and may even lead to dangerous situations. There are at least two basic solutions to this. The most straightforward one is to counteract interference by more advanced GPS receivers. Although there are quite a few technical possibilities for the rejection of interference, those that deliberately aim to jam are applying techniques of continually increasing sophistication. So this solution is not entirely waterproof.
The other solution is to ensure that the user is not fully dependent on GPS by having a hot backup system always available. Aviation has already taken this step; the US at the 1998 ICAO Meeting in Rio de Janeiro stated that â€˜Sole-means GPS is no longer considered an optionâ€™. Unfortunately, in the maritime world it is apparently more and more common practice to rely almost entirely on GPS. Officially, backup systems are installed. But it is questionable whether these systems are always really used and adequately maintained.
An often heard remark is that there are no alternatives for GPS. This is true - up to a certain level. The only widely available alternatives today are radar and Loran-C, the latter in the northern hemisphere only. These systems are not as accurate as GPS and therefore not useful for survey. However, for safety critical shipping operations the less accurate alternatives are still far better than having no system at all. So it is good news that much progress is noticeable in the US as well as in Europe in the development of high-performance Loran-C receivers. The availability of advanced and small-size equipment demonstrates a rebirth of this low-frequency terrestrial system. The US is upgrading its Loran-C system in respect of timing accuracy and reliability of the transmitter stations. Even more important is the fact that the user is not forced to select either GPS or Loran-C. Modern receivers integrate the two systems. This is one of the reasons for improvement in the timing of the high-power (200-1,200kW) Loran-C; so that the Loran-C timing becomes more accurately synchronised with GPS time. Precise time means critical information for many telecommunications, energy transportation and other processes in todayâ€™s society.
The introduction of Galileo is an important economic and political step in improving the overall performance of satellite navigation. However, as there are many similarities between the two satellite systems, it does not mean that the interference vulnerability issue is losing its significance.

Conclusion

GPS is a formidable system with an unprecedented impact on the navigation community. To minimise possible outages due to interference, users should have backup systems like Loran-C up and running and preferably integrated with GPS. This reduces the effects of interference in the navigation process and reduces also the challenges for potential hackers to jam satellite signals. If there is no effect, there is no fun either. This approach may help to protect safety-critical operations.