

Today few people drive with a map as a backup to their navigation system, and if they happen to have a map or street guide it is seldom an updated version. *Global Navigation Satellite Systems* have provided a cheap user-friendly solution with such great success that it has taken the market by force, causing older technologies to become obsolete within a very short time frame.



*Global Navigation Satellite Systems (GNSS) supplying Point, Navigation and Timing (PNT)* have infiltrated many professions and many applications have moved beyond the boundaries of supplying navigation data only. Some of the applications include:

- Surveying, cartography, GIS & photogrammetry
- Engineering, scientific and environmental studies
- Emergency vehicles, emergency dispatch calls, emergency beacons, safety monitoring, search and rescue missions
- Agriculture
- Nature conservation & animal tracking
- Navigation of road, rail, maritime & air transportation, taxi services
- Real time tracking of public transport
- Safety & security, law enforcement, house arrest
- Military applications, missiles & warfare
- Fishing and dredging
- Secure tracking of valuable or hazardous cargo
- Unmanned aerial vehicles (UAVs)

What might come as a surprise is that the following applications also utilize *GNSS* due to the *accurate timing* produced:

- Data networks
- Financial systems (for timed transactions)
- Electrical power grids
- Communication systems (mobile networks, digital radio broadcasts)
- Weather forecasting and earthquake monitoring

The systems have become so connected and interdependent in such a short time that there is no complete overview of the increasing range of



services that depend on GNSS and the complex way in which these systems interact. The interdependency and integral connectivity has raised concerns on our dependence on GNSS and the implications of system failure.

The first concerns were raised in May 2009 when the USA reported that they would have difficulty in maintaining their American *Global Positioning System* (GPS) and in launching new satellites to schedule and cost. The effect on world economies could be disastrous when taken into account

how many professions and applications are dependent on the PNT data supplied exclusively by the American GPS.

GNSS signals are particularly weak and vulnerable to (intentional or unintentional) interference. The signal can be swamped by radio noise caused by solar storms, unintended man-made radio interference and intentional interference (jamming or spoofing). Regardless of the cause, the implications of losing GPS information can be dramatic and potentially severe.

In the eighteenth *James Bond* movie *Tomorrow Never Dies*, the film opens with a scene at a terrorist arms bazaar where a terrorist purchases an *American GPS* decoder. The decoder is later used by a media mogul in an attempt to start a war between the People's Republic of China and the United Kingdom by creating a counterfeit GPS signal to steer a UK warship into South Chinese seas. This is a doomsday scenario of intentional interference and a potential security risk to governments around the world. Although no significant occurrences of deliberate interference have been documented, real spoofing devices have been developed in a laboratory to identify possible security measurements.



Dedicated jamming devices are readily available on the internet and several countries have made it illegal to own, use or sell such devices. With the increased revenue streams (such as a GPS-based toll road system) there is a financial incentive for organized crime syndicates to invest in exploiting the vulnerabilities of the system. This includes the jamming devices for hi-jacking of cars or trucks transporting valuable cargo or aircraft hi-jacking. Jamming technology exists today and is easily accessible. What does not exist is the ability to pinpoint the location of interference (intentional or unintentional).

Intentional and unintentional interference is normally localized. Unintentional interference has been experienced from poorly controlled signals from television towers, laptops, MP3 players, video recorders and mobile satellite services in a radius of up to 2km.

GNSS applications have become so broad that without adequate independent backup systems, signal failure or interference could potentially have disastrous effects. PNT data has become a matter of national security. Having the data jammed, corrupted or completely lost can have a severe impact on national security and could lead to major loss in economic assets.

Terrestrial land-based backup systems as accurate as GPS, based on completely different technology, exist in a few developed countries and a call has been made for other countries to adopt the system before disaster strikes.

**Esna Swart**  
[eswart@kartosurveys.co.za](mailto:eswart@kartosurveys.co.za)  
 Mobile: +27 (0)71 011 8044



## GLOBAL NAVIGATIONAL SATELLITE SYSTEMS

 <b>GPS</b> USA	Fully deployed US military satellite constellation and associated ground segments. Although originally conceived for military use, position, navigation and timing signals are fundamental to many civilian applications.
 <b>GLONASS</b> Russia	Russia's global navigation system which is nearing full deployment.
 <b>GALILEO</b> European Union	A global navigation satellite system being developed by the European Union to be a supplement (or alternative) to the American military GPS to be operational by 2014. The system is non-military and can provide assured services.
 <b>COMPASS</b> China	China's developing global navigation satellite system, planned to be operational by 2020.

A GNSS consists of 3 segments as shown in Fig 1:

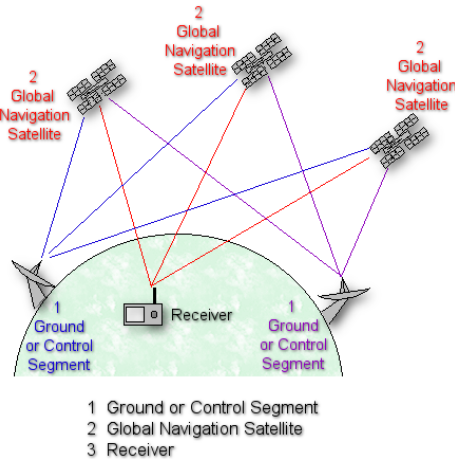


Fig 1 3 Segments of GNSS

1. A *Satellite segment* with a minimum of 24 satellites in 6 orbital planes forming a full constellation.
2. A *Ground or Control segment* is used to upload data to satellites, synchronize time across the constellation and to track the satellites to enable orbit and clock determination.
3. A *User segment* that consists of the receivers and associated antennas used to receive and decode the signal to provide PNT information.

## GNSS Vulnerabilities

Here are just a few possibilities of what can, and what has gone wrong:

### Too few satellites

All GNSS have a long-term dependence on stable financing and good management.

The US government identified a long term risk of a shortage of GPS satellites due to potential simultaneous failure of old spacecraft and late delivery of next generation satellites in March 2009.

During 1999 the Russian governmental commitment became unsustainable and lead to the temporary decline of GLONASS – this has since largely recovered.

### Operational mistakes

Pages of navigation data are uploaded to GPS satellites in advance of applicability. If bad data is uploaded to a satellite the clock and position knowledge may suddenly be in error.

Corrupt navigation data uploads occurred in March 1993, March 2000 and June 2002 – fortunately without serious consequences.

### Jump or drift of the clock on the satellite

The on-board atomic clocks can behave unpredictably and produce errors that grow slowly – before the operators can identify and mark them as unhealthy.

Failures such as those that occurred in July 2001 and 1<sup>st</sup> January 2004 caused location errors of up to 320 km.

### Bad signal shapes

If there is a fault in the signal modulation or generation process on a satellite it can cause unpredictable behaviour in receivers – potentially causing dangerous errors.

Two cases of such occurrence happened in 1993 causing errors of up to 8 metres and in March 2009.

### Satellite interference or destruction by solar flares or meteors

GPS satellites are vulnerable to being destroyed by meteors that would easily damage a satellite completely. Natural occurrences such as solar flares and ionosphere scintillation can also interfere, impede, or destroy the effectiveness of the GPS satellites in orbit.

### Terrorist threats to ground based GPS infrastructure

The GPS ground segment is designed to withstand a military attack, but could still be vulnerable to terrorist or cyber attacks.

### System Upgrades and Receivers

In April 2007 a 32<sup>nd</sup> GPS satellite was added to the constellation which caused problems in some receivers designed to handle only 31 satellites. In January 2010 an upgrade to the GPS ground segment software caused problems with military and timing receivers.

### Unintentional interference

Harmonic emissions from commercial high power transmitters, ultra wideband radar, television, VHF, mobile satellite services and personal electronic devices can interfere with the GNSS signals.

During 2002 a poorly installed CCTV camera in Douglas, Isle of Man, caused GPS signals within a kilometre to be blocked.

### Intentional interference

Receivers can be interfered with, not simply blinded by a strong, noisy signal known as jamming, but can also be fooled into thinking their location or the time is different due to a fraudulent GPS signals known as meaconing or spoofing.

Jamming is the most likely to happen as jamming devices are easily accessible via the internet. Meaconing (delaying and rebroadcasting) and spoofing (false signal) are currently less common.

Satellites could be intentionally destroyed during a terrorist attack. GPS technology is critical to the military of the U.S. and its allies. Missiles sent to destroy satellites from countries such as North Korea pose a valid threat.

View the March 2011 report published by The Royal Academy of Engineering;  
*Global Navigation Space Systems: Reliance and Vulnerabilities*

is available online at [www.raena.org.uk/gnss](http://www.raena.org.uk/gnss)

