How is Public Safety reliant on GNSS and is this a concern?

GNSS Solutions is a regular column featuring questions and answers about technical aspects of GNSS. Readers are invited to send their questions to the columnist, **Dr. Mark Petovello**, Department of Geomatics Engineering, University of Calgary, who will find experts to answer them. His e-mail address can be found with his biography below.

MARK PETOVELLO is a professor (on leave) at the University of Calgary. He has been actively involved in many aspects of positioning and navigation since 1997 and has led several research and development efforts involving Global Navigation Satellite Systems (GNSS), software receivers, inertial navigation systems (INS) and other multi-sensor systems.
E-mail: mark.petovello@gmail.com

Much like many industries and organizations, as the nature of Public Safety grows and evolves, its members have looked to leverage available technologies that help them achieve their goals. In this case, the goals are first and foremost Public Safety followed closely by Member Safety whether it be police, fire or others.

Hand in hand with the benefits of new technologies comes the dependency on said technology and the need to plan for the "what if" scenario should technology fail or let us down as it can on occasion.

One technology that is not new to Public Safety but is growing in its use is GNSS. The most obvious use of GNSS is to support location services for staff and assets — the tracking of team members and vehicles. However, with the latest advances in technology it has also become a necessity for precise timing to support basic radio/communications system operation. This aspect or use of GNSS/GPS is often overlooked.

This article provides some examples of how Public Safety can be threatened by over-reliance on GNSS and justifies why contingency plans have been put in place. Although the examples are specific to Public Safety services in the Greater Toronto Area (GTA), Canada, they can be expected to be similarly relevant in other jurisdictions in Canada, the United States, and abroad.

GNSS Timing in Public Safety

Public Safety users are still *very* dependent on reliable LMR (Land Mobile Radio) radio communications to provide a high level of public safety while ensuring their own safety.

Modern Public Safety LMR systems make use of two key elements that are very dependent on precise timing and both are used in the current APCO (Association of Public Safety Communications Officers) standard (APCO 25) that is often referred to as "P25 Phase II". APCO applies in Canada and the United States, and thus covers most of North America. Other jurisdictions (e.g., Europe, Asia, etc.) may use different standards, but it is expected that they all have similar reliance on GNSS, as described below.

The first of these key elements is the fact that P25 Phase II is a TDMA (Time Division Multiple Access) technology and uses a modulation scheme that time slices a 12 kilohertz radio channel to allow two conversations, or talk groups, to exist in the same spectrum. This is a way to increase the radio channel and system capacity allowing more users access to the system, higher availability and a higher grade of service.

To ensure that this time slicing of the spectrum is possible, the system must have a very precise time standard that is identical across the network and the same at all nodes or radios sites. In Canada, these networks can span cities, regions or provinces and have hundreds of sites. At each of these sites and nodes there are two GNSS receivers — a main and a standby — that are used to keep all radio transmissions in time.

Without this timing reference and without the accuracy and precision afforded by GNSS, the time slots and corresponding voice conversations that they contain would start to bump into each other and the users would have garbled, missed and/or lost radio transmissions. From a Public Safety perspective, any disruption to communications is of course concerning

and compromises the two prime goals listed in the opening paragraph.

The second use of precise timing is for the purpose of Simulcast. Simulcast is the process in modern Public Safety radio systems where radio signals on the same frequency or channel from two different sites intentionally overlap the same geographic area. This overlap is to ensure that Public Safety members have radio coverage at all times with no gaps. This approach is different than a cellular network when the handset "hops" from site to site rather than listening to multiple sites.

In order for the Public Safety portable radios to listen to multiple sites that are located random distances away and still properly decode the incoming transmissions, the timing of these overlapping signals must be stable, synchronized and well known. The GNSS receivers located at each site are also used to provide the required timing for this aspect of the radio system operation.

> "Considering the above, **the dependency of Public Safety on GNSS-derived time signals** is obviously very high — should the time standard drift or become unavailable for an extended period of time **the system would become unstable** and fall into a mode that shuts down sites and reduces coverage and capacity."

Considering the above, the dependency of Public Safety on GNSS-derived time signals is obviously very high — should the time standard drift or become unavailable for an extended period of time the system would become unstable and fall into a mode that shuts down sites and reduces coverage and capacity. This is often referred to as "fail-soft". When in this mode, it can seriously affect user communications and in turn the ability to maintain the key goals of Public and Member Safety.

To prevent fail-soft and degraded/limited service, the system has many built-in redundancies and contingencies.

The first of these is having multiple GNSS receivers distributed across the network to provide geo-redundancy and help to reduce the impact of single unit failure or local interference.

The second is to have these receivers equipped with a rubidium standard that allows them to "free run" without a synchronizing signal for some days while still maintaining the required synchronization.

The third is to have the GNSS devices equipped with receivers that span multiple bands and constellations in case of a constellation failure or issue.

Examples of Over-Reliance

Despite these contingencies, GNSS outages and disruptions can and have occurred and caused local and even wide spread outages across the radio networks. Below are several examples where Public Safety services in the GTA experienced short-term problems that, thankfully, did not adversely affect Public Safety.

In one case, in January of 2016, an incorrect satellite code upload to the GPS constellation triggered an error in the time standard. For additional details, read "GPS Glitch Caused Outages, Fueled Arguments for Backup" at < http://www.insidegnss.com/node/4831>. GNSS receivers in many LMR systems saw this as a valid fault or error in the time standard and if they were pre-set in a particular way (the factory default) they would shut themselves down as a preventative measure.

The issue in this case for many systems was that *all* receivers in the system were programmed the same way and so *all* GNSS receivers in the system perceived the timing as a local anomaly and took themselves offline — assuming other GNSS receivers in the same system would take over. The operational impact of this and the short-term — I dare say — panic that ensued was very disconcerting, to say the least.

To avoid this from occurring in the future there have been changes made to the GNSS receiver programming and they have been configured to ignore short-term timing anomalies and marshal on for as long as possible relying on their internal rubidium standards to provide the required synchronization. This of course would be sufficient and work in the short term, but the system would eventually fall back to fail-soft if it persisted.

In another case that occurred over a 6-hour period on Good Friday 2017 (starting late-morning and ending mid-afternoon in the Eastern time zone), there were local disruptions to GNSS receiver availability due to local in-band radio interference. Fortunately, this was a short period of time and on a holiday like this the system traffic was low and the potential disruption and impact was nominal.

The concern over this particular event is that it occurred very close to a strategic node in the system that is key to the systems operation and affected a large number of GNSS receivers including the one that provides timing to the Public Safety services' internal IT network. Had it persisted and if the source could not be found there was a contingency plan in place to "fail over" to the redundant node — located some distance away — that would have been able to provide the timing required.

The cause of the interference was never found and it disappeared as suddenly as it appeared — 6 hours

later — and has not been seen since. It could have been as sinister as a "GPS jammer" that is known to exist or as simple as a rogue unlicensed wireless mic or cordless phone. We have polled the surrounding area to no avail.

A similar event to this some months ago that affected the main dispatch channels was traced to an older and inexpensive TV antenna amplifier that had been plugged in by the home owner after being out of service. The device was voluntarily removed by the home owner.

Summary and Outlook

In summary, the dependency of Public Safety users on GNSS constellations and the timing that they provide is growing and becoming more critical for basic operations and are no longer nice-to-have capabilities.

This dependency has made it necessary to be vigilant and monitor the health of these data streams and the systems that are dependent on them. It has also prompted the development of strategies to ensure that there are redundancies and fallback solutions should the GNSS data stream be disrupted for long periods of time.

Some of these strategies may include the use of multiple frequency GNSS receivers, GNSS receivers that can make use of multiple constellations or even alternative time signals from terrestrial based systems.

I would encourage the custodians of all Public Safety systems to investigate the potential vulnerability and conduct a risk assessment when it comes to GNSS and its use. IG

STEPHEN ORR is an accomplished Wireless Industry Specialist and has more than 30 years of Wireless and Telecommunications experience in the areas of Engineering, Sales, and Business Management.

Stephen graduated from the University of New Brunswick in 1985 with a B.Sc. in Electrical Engineering and in 2001 he went on to complete his MBA at Queens University in Kingston.

Stephen started with Motorola Canada in 1985 in the Radio Systems Engineering group designing Land Mobile Radio systems for a variety of Public Safety and Commercial users.

Since then, he has held numerous senior technical and business leadership roles including Vice President, Strategy and Business Development. He has a broad background in the area of wireless communications covering Digital Cellular networks (HSPA/LTE), Mobile Payments and P25 Digital Land Mobile Radio (LMR).

In May 2013 Stephen joined the Durham Regional Police Service (DRPS) and currently manages all aspects of the Region Wide P25 Trunked Radio (LMR) System. This system provides service to all user groups in the Region – Police/Fire/Other - and is supporting more than 3,000 users.