Dependency of Communications Systems on PNT Technology

Charles Curry, B.Eng, FIET
Chronos Technology Ltd
Stowfield House
Upper Stowfield
Lydbrook
Gloucestershire
GL17 9PD

charles.curry@chronos.co.uk

www.chronos.co.uk
www.gps-world.biz
www.syncwatch.com

White Paper originally created as a contribution to Royal Academy of Engineering Study on PNT Vulnerability

Revision	Date	Change
V1.0	Mar 25th 2010	Chronos White Paper for Release

Introduction

All communications technologies require time or timing with appropriate accuracy, stability and reliability to operate effectively or at all. Stability of radio communications transmission, constant digital traffic flow, time slot alignment and traditional services over next generation Ethernet based infrastructure are some of the features that good time and timing bring to communications networks. Timing is now often referred to as the 4th utility and indeed is the second component of a major network build to be implemented after the power infrastructure.

Aligning, synchronising or syntonising time and timing to a common 'clock' was made easier with the emergence of a reliable global source when the GPS system became fully operational. One of the first telecom networks to recognise and adopt GPS as a timing source was BT in the mid 90's. Since then, the cost of the timing technology that leverages the GPS signal has dropped dramatically and become considerably easier to implement. The explosion in growth of communications systems and hence applications needing precision timing during the first decade of the 21st century has meant that many systems will design in GPS as a commodity source of 'time', often, due mainly to aspects of economy, with little attention to issues of reliability or susceptibility to poor reception.

When considering the impact this utility called 'Time' has on Telecom networks and the applications that sit on Telecom networks, it is appropriate to split it into three clear and separate aspects. 1) Traffic Timing ('Frequency'), 2) Common epoch (usually UTC) time slot alignment ('Phase') and 3) Time of Day ('Time') - 'FPT'. It will be important to examine the impact of loss of timing that each of these very different aspects of Time has on different applications in communications networks. This effectively turns the challenge into a three dimensional problem. We can then bring technology evolution into the mix. Communications technology is evolving to a packet based process; timing transport is becoming more complex and less deterministic – pushing more edge applications to choose GPS timing – so the take-up of PNT timing at the edge is likely to increase over the next 10 years. We now have a four dimensional problem!

Standards and Symposia

Timing in telecoms is so important that two annual symposia – WSTS and ITSF, dedicate their direction to the technology. WSTS – Workshop in Synchronization for Telecommunications Systems is a 3 day papers driven event with industry expert speakers, held annually in Boulder, Colorado and hosted by NIST – National Institute of Standards and Technology[1]. ITSF – International Telecom Sync Forum is also a 3 day papers driven experts' forum held annually in a different European city[2].

Both symposia are run by steering groups significantly populated by members of the key Standards groups which govern the rules relating to time and timing in telecom networks. These are ITU, ETSI, ATIS, IEEE and IETF. The key set of benchmark Standards are set

[1] The author is on the WSTS steering group.

[2] The author founded ITSF in 2001 and chairs the steering group.

by ITU – International Telecommunications Union - Study Group 15 Question 13[3]. The ITU Standards have defined the requirements for synchronous transmission methods including Synchronous Digital Hierarchy (SDH) Standards and most recent Synchronous Ethernet (SyncE) Standards. They also tend to gather in and qualify the adaptation and adoption of the more specific technology Standards e.g. the new Packet Time Protocol (PTPv2) from the IEEE. Not much timing work has taken place in ETSI. SyncE and PTPv2 together provide the timing technology for next generation networks (i.e. Ethernet Networks). SyncE manages the timing or frequency of the packets through the network with traceability to the existing network Primary Reference Clock (PRC) and PTPv2 uses a protocol through the Ethernet network whereby a so-called 'Grandmaster' synchronises an active remote client in both frequency and time.

Positioning, Navigation & Timing (PNT) Technology

In order to comprehend how PNT – (practically only GPS for the present) technology is implemented for timing, the essential architecture of a PNT timing system must be understood. Fig 1 below depicts a simplified architecture.

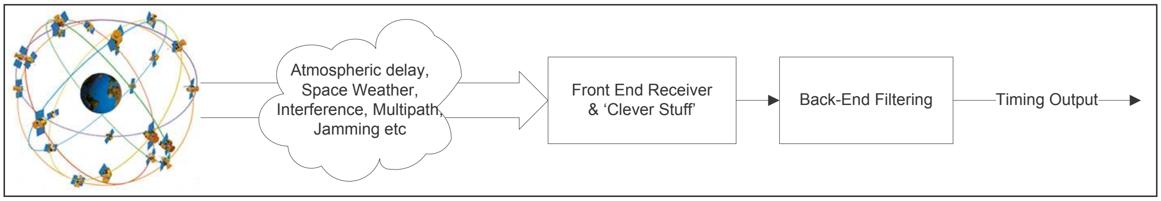
Atmospheric delay, Space Weather, Interference, Multipath, Jamming etc
Front End Receiver & 'Clever Stuff'
Back-End Filtering
Timing Output

Figure 1: Signal path from GPS Satellite Constellation to the Timing Output

A vulnerability and susceptibility analysis of the architecture can be focused into three main areas. Transmission medium, front-end 'clever stuff' and back-end 'filtering'. The transmission medium defines the path the PNT signal takes from the satellite (or transmitter if terrestrial e.g. eLoran) to the receiver. The front-end 'clever stuff' defines manufacturers' intellectual property that is bundled up with the GPS engine to limit vulnerabilities to (for example) multipath. Back-end 'filtering' is used specifically for cleaning up the timing output and may deliver a frequency (e.g. 2.048 MHz in Telecoms, 10 MHz in DVB) or a UTC aligned 1pps signal.

Transmission Medium

Natural and man-made phenomena in the signal path from a GPS satellite to the receiver define the susceptibility of a PNT timing system to non-deterministic events.

Natural phenomena include 'Space Weather'. Space Weather includes the disruption to the ionosphere caused by solar activity. Solar activity follows an 11 year cycle and currently is at a minimum. When output from a solar flare hits Earth's upper atmosphere it causes the formation of additional free electrons which can diffract the signal path or

[3] Chronos is an ITU member and attends the ITU SG15/Q13 meetings

slow down the signal. This is potentially more disruptive to location than timing since 1 nanosecond of delay equates approximately to 30 cm of position.

Man-made phenomena include jamming, meaconing and spoofing. Jamming is the most likely activity which will impact a conventional industrial use GPS timing system. Meaconing (delaying and rebroadcasting) and Spoofing (false signal) which effectively rebroadcasts erroneous satellite ephemeris are more likely to be encountered in battle theatre situations although accidental meaconing could be caused by the proximity of a GPS antenna with poor impedance matching. Jamming can be split into 4 broad areas: Accidental, Criminal, Red Team Deliberate and Blue Team Deliberate.

Accidental Jamming is most likely to be caused by harmonics from other RF signals which sit on the weak GPS signal-from-space. This will typically be localised and potentially manageable once identified. This may be mitigated by moving the GPS antenna to screen out the problem and is less likely to be an issue for a GPS timing system. One specific form of accidental jamming (meaconing) is from a (typically old) co-located GPS antenna rebroadcasting the signal on account of poor VSWR in the amplified signal path from the low noise amplifier; this would interfere with reception in an adjacent antenna. For this reason antennas should be mounted as far apart as possible and never closer that about 2m.

Criminal Jamming is caused by people who are looking to defeat GPS tracking systems. At present this is limited to car thieves, but could extend to road toll evasion, tracker evasion, commercial mileage limit avoidance etc. This will typically be indiscriminate and both moving and stationary. It may be fairly low power just to defeat the localised vehicle location system but the car thief is unlikely to be concerned with managing power levels to minimise impact on additional nearby GPS reception. This is unlikely to be a problem for a GPS timing receiver if the antenna is mounted on a building roof and the back-end filtering is sufficient to mitigate a short term jamming event.

Red Team Jamming (e.g. Terrorist) is deliberate and may be targeted at some specific aspect of critical infrastructure, not necessarily timing systems. It will be indiscriminate, more likely to be high power and may occur at a number of locations simultaneously. This is more likely to be a problem for a GPS timing system and the impact will be dependent on the back-end filtering.

Blue Team Jamming is deliberate – generally to defeat a perceived threat of covert tracking. It will probably be low power and have a similar impact to criminal jamming. However their use profile should be investigated and there would be an impact if they parked for long periods near critical infrastructure which used GPS timing e.g. a TETRA base station

Front-end ‘Clever Stuff’

Front end ‘clever stuff’ is the intellectual property that GPS silicon or equipment designers develop to enhance the ability of the receiver to use the GPS signal. This will normally impact aspects like speed to first fix, operation in locations with poor satellite visibility, low signal strength, multipath issues, resilience to interference etc. This report will not address this area in any particular detail as it generally impacts location and positioning more than timing.

It is however worth observing that GPS systems optimised for location and positioning accuracy generally do not perform sufficiently well for timing applications.

In the future however – Assisted GPS – 'A-GPS' will enable the GPS signal to be useable for timing applications deeper inside a building. Applications leveraging A-GPS for timing have not emerged yet; the essential technology whilst available is still in the research phase. These are likely to be more susceptible to jamming as the signal is naturally weaker inside a building.

Back-end 'Filtering'

Back-end filtering is a critical aspect of a GPS timing receiver which will define susceptibility to jamming and interference. To simplify this element – consider four types of oscillator which are effectively used as flywheels – Temperature Compensated Crystal Oscillators, (TCXO), Oven Controlled Crystal Oscillators (OCXO), Rubidium (Rb) atomic clocks and chip scale atomic clocks (CSAC)

TCXO[4] – Temperature Compensated Crystal Oscillator is a low cost (cents/pence) component. The TCXO forms part of a phase locked loop or the basis for a numerically controlled oscillator to offset or compensate for inherent aging and offset. The TCXO will track the GPS off-air signal but will have no ability to 'hold-over' in the event of loss of GPS signal. Recent developments in back end signal processing means that very low cost GPS timing systems fit for purpose in terms of instantaneous stability are available as super-components for a few pounds.

OCXO[5] – Oven Controlled Crystal Oscillator is a more expensive oscillator (£10s-£100s) with various levels of hold-over stability – usually more stability is more expensive. Like the TCXO the OCXO forms part of a phase locked loop or the basis for a numerically controlled oscillator to offset or compensate for inherent aging and offset but considerably less than the TCXO. The OCXO will track the GPS off-air signal and will have reasonable hold-over performance (of the order of hours depending on stability specification) in the event of loss of GPS signal.

Rb Atomic – Rubidium Atomic Oscillator is a much more expensive oscillator (£1000+) and forms the heart of major telecom network timing infrastructure. Rb brings

[4] Quartz varies in frequency with temperature. This variation is typically linear at ambient temperatures and a TCXO make use of this property to compensate for accuracy based on knowing the temperature.

[5] At higher temperatures e.g. ~80°C the variation with temperature flattens off. Putting the quartz resonator into a single or double oven minimises the impact that external temperature changes have on the frequency stability.

considerable improvement in holdover - moving the ability of the infrastructure to withstand GPS outage from days to months.

CSAC - Chip Scale Atomic Clocks are just emerging from the R&D labs with first commercial deliveries anticipated by mid 2010. These will offer stabilities better than Rb along with power consumption less than a tenth and in a package footprint smaller than the current miniature Rb oscillators. A clear paradigm shift in technological innovation and a technology to watch for its mitigation capabilities.

In terms of mitigation – one can also consider the use of two oscillators in a 1:1 resilient architecture (usually OCXO and Rb) and then managing the mean time to repair (MTTR) to under 24 hours in the event of failure to ensure that system failures are extremely unlikely.[6]

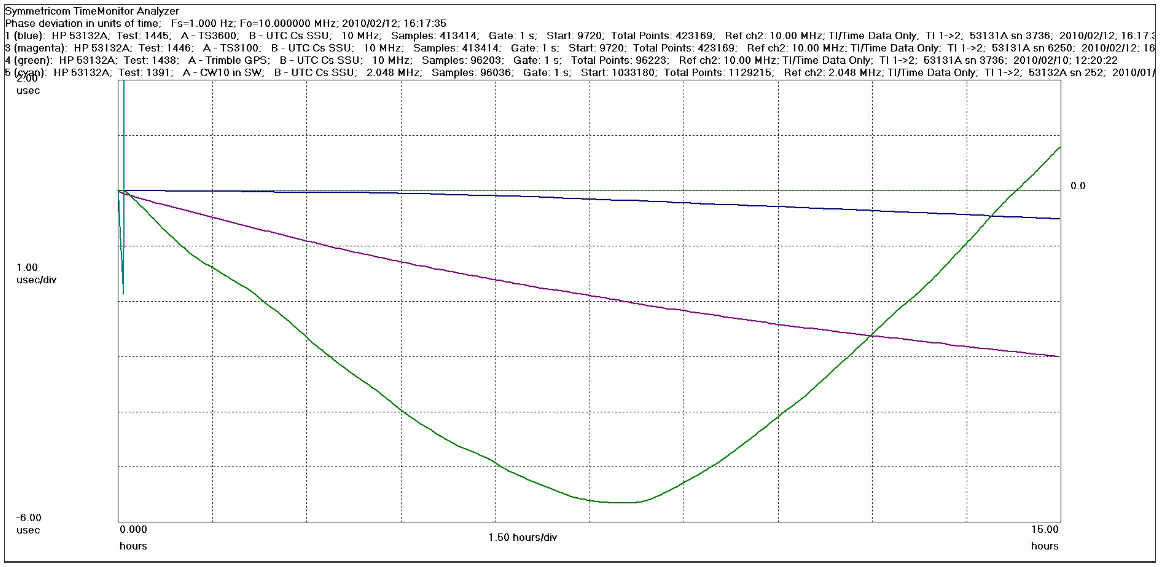

Figure 2 - Comparison of time error in holdover between TCXO (cyan), Low Stability OCXO (Green), High Stability OCXO (Magenta) and Rb (Blue) based GPS timing receivers.

National or Core Telecom Network Traffic Timing

In order to understand the vulnerability of telecom network infrastructure to loss of GPS timing we need to examine how the network uses ‘time’ to manage traffic flow and also how that ‘time’ is implemented into the network.

Digital bits & bytes are assembled into containers or packets and these flow round telecom networks at a constant rate. The actual speed is determined by the transport layer and can be as fast as ~40 Gbit/s in the highest speed optical transport networks although 100 GbE is under development. All timing has to be traceable to a common clock within

[6] With MTTR of 24 hours, MTBF – Mean time between failures at the system level approach 100s if not 1000’s of years. Given 1000+ elements in network (not unusual with mobile base stations) – the likelihood of a network affecting failure could be quite high even with this apparently extraordinarily high MTBF.

any one network. Then traffic handed over from one country's network to another – e.g. between UK and Germany although not be traceable to the same clock, the error between the two must not be greater than that allowed within each network. This is known as a plesiochronous boundary.

A telecom network is like a road system consisting of side roads, main roads, junctions and of course motorways. Junctions clock the traffic in and out and ensure that (a) The rate is appropriate for the road type and (b) The rate is constant i.e. no speeding up and slowing down (known as wander). In telecom networks – junctions are switches which are based in towns and cities – city switches equate to motorway junctions. Town switches are more like aggregators, assembling traffic onto a higher speed link and sending it to the city switch.

The types of timing error that must be managed are constant traffic speed errors and varying traffic speed errors (wander). Constant speed errors result in traffic arriving at the exit junction faster or slower than it is being clocked in. This should be taken care of in an elastic buffer process, but if the error is 'too large for too long', the buffer will have to be emptied (known as a buffer slip) to make way for traffic behind (telecom traffic cannot stop like road traffic). This results in loss of data and potentially application failure. Wander is a variation in traffic speed (usually around a mean) – so may cancel out if not 'too large for too long'. However wander sometimes gets amplified as it passes from none network element to another – eventually becoming 'too large for too long' and resulting again in traffic loss as a buffer empties.

Slips which result in loss of data at an equipment or network boundary can have a significant and very detrimental impact on traffic and the impact is becoming more significant as we move towards an increasingly all digital telecom infrastructure. Contrast analogue voice traffic with VoIP (Voice over Internet Protocol). An analogue voice circuit would output a click; a VoIP call would begin to exhibit the 'Norman Collier'[7] effect. Encrypted data traffic can also be badly affected if the whole or part of the message has to be resent.

A Slip is defined as 'Frequency Error' x 'Observation Time' x 'Data Rate' divided by the 'Buffer Length'. Once a GPS conditioning signal is lost, the frequency error is determined by the local oscillator in 'holdover'. If we consider an 'E1' (2 Mbit/s) traffic highway with a buffer length of 256 bits the approximate quantity of slips is indicated in Table 1 below

[7] Norman Collier was a comedian whose stage performance consisted of pretending that the microphone was cutting out so the audience only heard occasional syllables from his speech.

Table 1: (Very) Approximate Number of 'Slips' with Different Oscillators in Holdover

Oscillator	3 mins	3 hrs	3 days	3 wks	3 mths
TCXO	0	1	600	30k	500k
Low Spec OCXO	0	0	200	9000	50k
High Spec OCXO	0	0	5	150	3000
Low Spec Rb	0	0	0	15	300
High Spec Rb	0	0	0	3	50

The 'too-large-for-too-long' issue is quantified by continuously measuring the relative time error between two clocking elements or networks – known as Time Interval Error (TIE) with nanosecond granularity, then observing the maximum TIE (MTIE) over different observation periods e.g. 100/1000/10,000 seconds etc. MTIE has become the bedrock metric for telecom timing measurement and ITU[8] and ETSI[9] Standards for the last 20 years. The timing required by each critical part of a telecom network is defined by an MTIE 'Mask' – effectively a line in the sand which defines the maximum time error in nanoseconds which is allowed for any given observation period. Fig 3 below shows some MTIE masks and a typical measured performance metric.

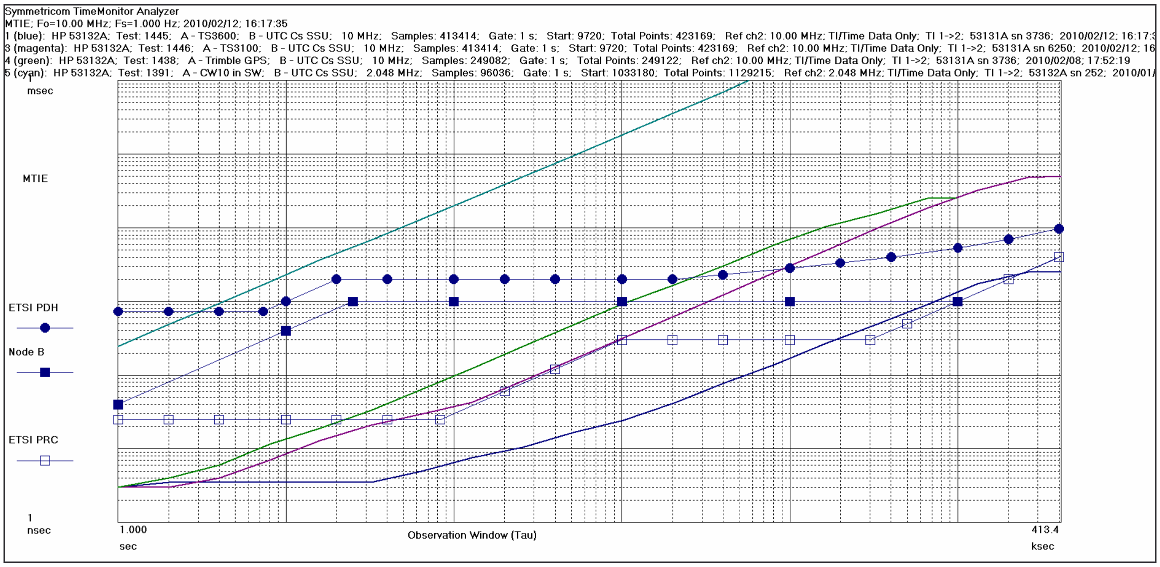

Figure 3: MTIE Metrics. Comparison of time error in holdover between TCXO (cyan), Low Stability OCXO (Green), High Stability OCXO (Magenta) and Rb (Blue) based GPS timing receivers

Failure of the process of regenerating the timing within the requisite MTIE at each switch node will result in timing errors. GPS is now often used to derive timing both at the core

[8] ITU G.810 – Transmission Systems And Media; Digital transmission systems – Digital networks – Design objectives for digital networks; Definitions And Terminology For Synchronization Networks

[9] ETSI EN 462-1-1 Transmission and Multiplexing (TM); Generic requirements for synchronization networks; Part 1-1: Definitions and terminology for synchronization networks

and edge of telecom networks. The short term errors in raw GPS timing are too large for satisfactory use in telecom infrastructure even when considering the 'clever stuff' wrapped up in the GPS silicon. Back-end filtering plays the key role in the vulnerability of telecom traffic to GPS outage and corresponding timing errors and a summary analysis is shown below in Table 3.

The key to the Summary Vulnerability tables is shown below in Table 2 below. It should be noted that each system and individual manufactures' equipment will behave differently. The classifications are indicative only and full testing is recommended to determine individual equipment, system and network vulnerabilities.

Table 2: Key to Vulnerability Summary Tables

✘	Failure of GPS would cause subsequent failure within indicated time period
✓	Failure of GPS may cause degradation of service within indicated time period
✔	Failure of GPS would not impact service within indicated time period

Table 3: Application: Telecom Network Traffic Timing - Vulnerability to Loss of GPS

Telecom Network Traffic Timing	3 mins	3 hrs	3 days	3 wks	3 mths	3 yrs	>3 yrs
TCXO	✘	✘	✘	✘	✘	✘	✘
Low Spec OCXO	✔	✓	✘	✘	✘	✘	✘
High Spec OCXO	✔	✔	✓	✘	✘	✘	✘
Low Spec Rb	✔	✔	✔	✓	✘	✘	✘
High Spec Rb	✔	✔	✔	✔	✓	✘	✘
1:1 System OCXO & Rb[10]	✔	✔	✔	✔	✓	✘	✘
1:1 System + Backup Timing[11]	✔	✔	✔	✔	✔	✓	✓
1:1 System + 24x365 Support[12]	✔	✔	✔	✔	✔	✔	✔
1:1 System + Backup + Support	✔	✔	✔	✔	✔	✔	✔

National infrastructure networks are typically designed with 1:1 Rb/OCXO resilient timing equipment known as SSUs (Synchronisation Source Utility[13]) at every major city switch and are supported with a next day critical element replacement service. Backup timing is enabled using physical timing links in the transport layer of the SDH network (and in the future in the transport layer of the Ethernet NGN network now standardised through ITU as Synchronous Ethernet or SyncE). When back-up is enabled - traceability becomes a key issue. Traceability to another GPS based timing reference is not allowed as GPS reception could be lost at that node as well. Best practice requires traceability going from switch to switch via SSUs eventually reaching more than three Caesium

[10] Assumes the Rb does not fail first after loss of GPS

[11] Backup Timing will be delivered through the telecom network infrastructure as SDH clock or SyncE clock traceable back to Cs atomic standards

[12] A 24x365 Support Service would typically deliver a replacement critical path element to site within 24 hours ensuring that the timing equipment never suffers a complete and catastrophic failure.

[13] SSUs are known as BITS clocks in the USA – Building Integrated Timing Source

atomic clock Primary Reference Sources in at least two separate locations[14]. Table 3 above illustrates how the different oscillator options impact the vulnerability of a network to loss of GPS. True resilience to GNSS interference or jamming can realistically only be obtained by using some kind of technologically independent backup system, e.g. Cs or eLoran and a managed support process guaranteeing a timely fault clearance process.

The mobile operators also have aggregation nodes where traffic from a number of local base stations is brought together and switched to a higher speed link before onward transmission to their core networks. Typically timing elements (if deployed at these nodes) adopt a local single string (i.e. not resilient 1:1) architecture using GPS with high grade Rb or OCXO usually because there is no access to network delivered timing.

There are many other smaller organisations or localised international organisations which carry telecom traffic. They may have just one switch in the UK or rationalised switches.

Having ascertained the vulnerability of core telecom network infrastructure to loss of GPS, this report will now consider mobile networks.

Mobile Networks

All mobile networks use their own national switching and transmission systems to manage traffic at the core. But mobile networks have other challenges associated with timing. These include base station timing for radio frequency stability and call hand-over management, migration to 4G/LTE services Ethernet backhaul, use of 3rd party backhaul and call time stamping.

Traffic is backhauled by the mobile operator from their base stations both through their own and 3rd party national infrastructure. There is also a new approach emerging called 'RAN' share – Radio Access Network where two or more mobile operators are outsourcing the responsibility for backhauling their traffic to another 3rd party.

Depending on the commercial wholesale contract, a national carrier may or may not be required to guarantee timing. Currently, timing is often conveniently delivered (for free) over the SDH E1 traffic signal and recovered by the base station. With the migration to NGN services partly brought about by the need to get more bandwidth availability at the edge of the network, access layer timing technology is by necessity evolving to SyncE or PTPv2. Both are experiencing significant deployment challenges at the moment which may well encourage take up of local base station 'economy' GPS timing as already used by the CDMA networks in the USA[15].

[14] The 'Rule of 3' concept enables absolute certainty as to which unit is faulty in a self test process. With only two Cs clocks, a relative timing comparison cannot declare which unit has gone unstable. Using two different locations also ensures that a building fire does not compromise the overall network timing.

[15] The well known 'San Diego incident' US DoD own-goal illustrates how localised GPS jamming can bring down a mobile telecom network.

There are two key aspects of timing required at a base station – RF stability and time slot alignment or Phase. RF stability (5 x 10^{-8} or 50 ppb) is derived by phase locking the base station local oscillator to the incoming traffic signal and is necessary for both FDD (Frequency Division Duplex) and TDD (Time Division Duplex) systems. Time slot alignment or phase – a prerequisite for TDD transmission systems and future LTE/4G systems in the UK requires base stations to be synchronised to within 1 microsecond of a common epoch (usually UTC) – is derived either from local GPS receiver or in the future visa the Ethernet packet time protocol PTPv2. This is much harder to achieve than the FDD synchronisation.

Likely impact of loss of GPS to the base station performance will include radio frequency drift, call hand-over failure and traffic speed reduction in the TDD transmission process.

Table 4 shows the vulnerability of various base station local oscillators to loss of GPS for FDD systems

Table 4: Mobile Base Station Timing – Vulnerability to Loss of GPS – FDD Systems

Mobile Base Station Timing	3 mins	3 hrs	3 days	3 wks	3 mths	3 yrs	>3 yrs
TCXO	✗	✗	✗	✗	✗	✗	✗
Low Spec OCXO	✓	✓	✗	✗	✗	✗	✗
High Spec OCXO	✓	✓	✓	✗	✗	✗	✗
Low Spec Rb	✓	✓	✓	✓	✗	✗	✗
High Spec Rb	✓	✓	✓	✓	✓	✗	✗

Table 5 shows the vulnerability of various base station local oscillators to loss of GPS for TDD systems. Whilst a secondary backup of a PTPv2 feed should continue the UTC alignment, it is not clear yet to the industry how vulnerable PTPv2 will be to network reconfigurations and packet delay variation since at the time or writing deployment of this technology is still experimental. One solution could be low grade OCXO with PTP back-up deriving timing off the network feed – this will not use GPS locally at the base station – but would reference GPS in the vicinity e.g. <50 miles. This option is not included in Table 4 which just examines the vulnerability of a local GPS at the base station. If GPS were also to be comprised at the location serving PTP packets to the base station then the table entries referring to PTP back-up should be ignored

Table 5: Mobile Base Station Timing – Vulnerability to Loss of GPS – TDD Systems

Mobile Base Station Timing	3 mins	3 hrs	3 days	3 wks	3 mths	3 yrs	>3 yrs
TCXO	✗	✗	✗	✗	✗	✗	✗
Low Spec OCXO	✓	✗	✗	✗	✗	✗	✗
High Spec OCXO	✓	✓	✗	✗	✗	✗	✗
Low Spec Rb	✓	✓	✗	✗	✗	✗	✗
High Spec Rb	✓	✓	✗	✗	✗	✗	✗
Lo Spec OCXO with PTP Backup	✓	✓	✓	✓	✓	✓	✓
Hi Spec OCXO with PTP Backup	✓	✓	✓	✓	✓	✓	✓

Low Spec Rb with PTP Backup	✓	✓	✓	✓	✓	✓	✓
High Spec Rb with PTP Backup	✓	✓	✓	✓	✓	✓	✓

Time of Day Applications

Many computer systems now require traceable and accurate time-of-day to timestamp financial transactions, call time & duration or time stamping of alarm events amongst others. Whilst NTP (Network Time Protocol) servers exist on the Internet – this is not secure enough for mission or commercially critical applications. So NTP servers are implemented within certain organisations' networks e.g. the financial community, mobile operators, government networks etc.

The effectiveness of an NTP transaction is dependent on the variation in timing as the PC based soft client communicates with the server. It is generally good enough for accuracies of a few 10s of msec as packet delay variation (PDV) on an Ethernet link is probably of the same order. To achieve better performance, PTP must be used with an active client designed into the application and the server or 'grandmaster' located reasonably close to the client.

These locally deployed NTP servers and PTP Grandmasters will usually use GPS as the source of UTC traceability and back this up with generally a high grade OCXO or Rb. Loss of GPS would result in the master clock losing time accuracy and so the vulnerability is application dependent.

The classical time error formula is $\mathbf{\Delta T = aS + 0.5bS^2 + c}$ where

a = Frequency offset due to temperature.
b = Average Frequency Drift (after 60 days normal operation).
c = Initial frequency offset due to transition from normal to holdover.
S = time in seconds.

We may assume in a reasonably temperature stable environment of an IT equipment room that 'a' is negligible. 'c' should be negligible in a well designed NTP server or PTP Grandmaster.

We can therefore identify vulnerabilities according to the following tables examining applications that are required to maintain accuracies within 1 sec, 1msec and 1µsec.

Table 6 illustrates a typical mobile billing system with time-stamping for legal evidence.

Table 6: Holdover Oscillator required to maintain <1sec relative to UTC – Vulnerability to loss of GPS

Oscillator Maintaining <1sec	3 mins	3 hrs	3 days	3 wks	3 mths	3 yrs	>3 yrs
TCXO	✓	✓	✓	✗	✗	✗	✗
Low Spec OCXO	✓	✓	✓	✓	✗	✗	✗
High Spec OCXO	✓	✓	✓	✓	✗	✗	✗
Low Spec Rb	✓	✓	✓	✓	✓	✗	✗
High Spec Rb	✓	✓	✓	✓	✓	✓	✗

Table 7 illustrates a typical financial transaction time-stamping system, however – we are seeing evidence of time stamping in financial transactions being required to much better than 1ms driven by the requirements of needing to track and correlate automated computer trading systems.

Table 7: Holdover Oscillator required to maintain < 1msec relative to UTC – Vulnerability to loss of GPS

Oscillator Maintaining <1msec	3 mins	3 hrs	3 days	3 wks	3 mths	3 yrs	>3 yrs
TCXO	✓	✓	✗	✗	✗	✗	✗
Low Spec OCXO	✓	✓	✓	✗	✗	✗	✗
High Spec OCXO	✓	✓	✓	✗	✗	✗	✗
Low Spec Rb	✓	✓	✓	✓	✗	✗	✗
High Spec Rb	✓	✓	✓	✓	✗	✗	✗

Table 8 illustrates the kind of accuracy required a TDD LTE/4G mobile network, TETRA, ‘Smart Grid’, DVB, DAB, automated computer financial trading systems.

Table 8: Holdover Oscillator required to maintain < 1µsec relative to UTC – Vulnerability to loss of GPS

Oscillator Maintaining <1µsec	3 mins	3 hrs	3 days	3 wks	3 mths	3 yrs	>3 yrs
TCXO	✓	✗	✗	✗	✗	✗	✗
Low Spec OCXO	✓	✗	✗	✗	✗	✗	✗
High Spec OCXO	✓	✓	✗	✗	✗	✗	✗
Low Spec Rb	✓	✓	✗	✗	✗	✗	✗
High Spec Rb	✓	✓	✗	✗	✗	✗	✗

Examples of GPS Related Faults

The following examples are GPS attributed faults experienced by clients of Chronos and reported by the Chronos Support Team.

Leap Second Misinterpretation

This was a firmware issue. The GPS referenced NTP server received the message from the GPS constellation that a leap second should be inserted, but due to a known software bug (fixed but not implemented by the operator) the leap second was interpreted as a Leap Year! The impact on the client – a national UK mobile operator was that the time on their billing computer (which by law must always be within 1 second of UTC) went forward one year.

Satellite 24

The Cesium atomic oscillator on satellite PRN24 developed a fault at 6:30 am on Jan 1st 2006. One known impact of this fault was that a large proportion of at least two large national carriers' receivers – which were feeding GPS timing into the SSUs – set themselves as unusable. The SSUs then fell back to network clock traceable to their own Cesium primary reference clocks.

Missing Leap Second

This was another firmware issue which was known about, but in this instance not yet implemented in a formal release of software. The GPS receiver was set up to look for a leap second, but when one did not appear, it disengaged the GPS steering on the local oscillator (back-end) filtering. The problem took approximately 2 weeks for the frequency offset to be large enough to impact service. In this case the operator was a national broadcaster and DVB transmitters started to fail.

Risk Assessment for Future Vulnerability to GPS Outage

Whilst jamming has not caused notable outages, there are a few anecdotal incidents to date. It is perceived as an increasingly likely threat.

Two notable incidents traceable to GPS jamming are the failure of the Swedish national TV network in 2008 and the TETRA network in Athens during the 2008 Olympics. It's not clear whether the source of the problems were identified.

The ease with which jammers are available over the Internet[16] and the increasing use for criminal activity means that we will begin to see more jamming events. The most powerful jammer currently identified has a 25W power which could impact applications upto 200 miles away.

[16] Google search for the exact phrase 'GPS Jammers' found over 13,000 hits

The now well documented ‘San Diego’[17] incident illustrates how quickly and dramatically, a GPS jamming event can render a communications network inoperable. In the case of the San Diego CDMA network – low/medium stability OCXOs were used as backup.

A Short Review of Alternative UTC Traceable Systems

Any system proposed as an alternative to GPS must offer traceability to UTC via a route that does not include GPS and must use a technology that is not susceptible to the same jamming and interference as GPS. This precludes the use of Galileo (when available) and Glonass.

UTC traceability must include 3 independent Caesium atomic clocks cross comparing with each other to detect a faulty unit. Traceability to a known good reference should then be used e.g. GPS with the knowledge that it is not being jammed and that a local national standards organisation i.e. National Physical Laboratory (NPL) in the UK is monitoring it and has not announced a fault

DVB and DAB signals have been proposed as a suitable source of timing as has an emerging technology called ‘Rosum’ which leverages DVB signals. However digital broadcast transmitters use GPS/Rb timing sources and would therefore exhibit be vulnerabilities as defined above. Rosum could offer building penetration capability as an augmentation to direct GPS – but it is still experimental.

In the USA, the GPS stabilised CDMA signal has been used as an alternative to direct GPS because of its building penetration capability. As was illustrated above with the ‘San Diego’ incident this was no defence against GPS jamming.

Local LF transmissions e.g. the 60 KHz Anthorn signal or DCF77 at Mainflingen in Germany can offer independent UTC traceability with triple Cs back-up. However they represent a single point of failure as low cost LF receivers built into equipment are generally optimised for their own country reception. They are not a truly transnational solution.

Loran-C or the modernised version eLoran signal does represent a potentially resilient transnational non-GPS solution. Each Loran station has triple Cs atomic standards. Each transmission is traceable to UTC and monitored by a local national standards organisation. A Loran receiver by design will monitor multiple signals from different countries. Loran also has excellent building penetration capability as it uses a 100 KHz signal.[18]

[17] http://forums.groundspeak.com/GC/index.php?showtopic=160821

[18] The GAARDIAN project will research the capability of eLoran as an alternative to GPS

How to Recognise Vulnerability to PNT Jamming and Interference

By its very nature PNT jamming and interference is not something that can be created in a real world every day situation to see if it is a problem. Two approaches are proposed which can be adopted to recognise vulnerability to PNT jamming and interference. These are:

1. Detailed questioning regarding technology resilience.
2. Laboratory Testing of susceptibility to loss of PNT signal

1. Detailed questioning regarding technology resilience.

Questions regarding an application or product's timing resilience to PNT jamming and interference should focus on what frequency stability is required and over what period. Also what time of day accuracy or phase accuracy is necessary for the application?

Questions should then focus on

- Type of Oscillator used as a filter or for holdover
- Need for UTC traceability
- Redundancy within the equipment or network architecture
- MTBF and MTTR
- Backup to non GPS traceable timing[19]

2. Laboratory Testing

Testing is more complex, there are no recognised tests (like CE mark EMC and safety testing where susceptibility testing is the norm). There are no generic standards for holdover other than those published by the ITU. 3GPP which manages wireless communications is fairly minimalist on timing. Time of Day is dependent on standards published by individual industry bodies or companies' SLA requirements. The Standards for NTP are managed by the IETF. The Standards for PTPv2 are managed by the IEEE.

A holdover testing regime or programme for individual product elements could be established, both on the bench and connected to any back-up source of timing – where that should be tested as well.

The testing process would need to be clearly defined to avoid ambiguous results. The three way rule is important to uphold.[20]

[19] This is a critical question. We have heard people suggest that the CDMA signal could be used as a backup to GPS, but as CDMA uses GPS - this is a dangerous misconception. CDMA has got building penetration features

[20] Given 3 timing sources A, B & C. Testing AvB does not determine if A or B is at fault. Testing AvB, BvC & CvA ensures that the faulty timing source is recognised.

Conclusion

Given the increased threat from some form of GPS jamming and the increased likelihood of atmospheric interference as the sun moves into a more active period, the message from the summaries in Tables 6 & 9 is that modern or next generation fixed and mobile communications systems and applications are becoming more susceptible to the loss of the GPS reference. Even high spec Rb cannot hold up requirements for very long. With the drive to less expensive hardware solutions and the commoditisation of GPS technology, the situation is unlikely to improve.

The telecom transmission technology evolution from TDM networks to Ethernet means that the timing transport layer is becoming compromised. Whilst new timing technologies i.e. SyncE and PTPv2 are emerging, a move to low cost GPS timing 'engines' may seem less complex and more cost effective, but depending on the application, may have serious consequences if GPS was lost.

Lessons should be learned from the inherent reliability built into national fixed wire telecom carriers who not only use the highest spec Rb, they also build in 1:1 resiliency, network backup to an independent reference and support contracts to ensure that the risk of two failures at the same time in a critical path are minimised

Finally, whilst a high degree of independence can be obtained by referencing to independent Cs atomic standards, this is relatively expensive and difficult to connect to unless the organisation owns the network. The only true off-air transnational UTC traceable PNT reference with timing accuracy and stability to match GPS timing is eLoran. However eLoran is still an emerging technology but with the added promise that the in-building performance has potential to complement GPS timing. Much research still needs to be done to study the timing performance of eLoran over the seasons and in different and difficult built environment situations.

Charles Curry, B.Eng, FIET
Managing Director
Chronos Technology Ltd
charles.curry@chronos.co.uk
www.chronos.co.uk

Charles Curry is founder & Managing Director of Chronos Technology Ltd. Charles graduated in Electronics from Liverpool University in 1973, and started his career in semiconductor research at GEC Hirst Research Centre, progressing to Racal Instruments where he was responsible for sales of test equipment including specialist frequency and time products including supplying BT with their first Cesium atomic freq standard for timing their digital network.. In 1983 Charles supplied some of the first civil GPS receivers to the oil exploration industry whilst MD of GSE Rentals. He founded Chronos, a leading system integrator for synchronisation and timing products in the UK telecom industry, in 1986.

Charles founded the International Telecom Sync Forum (ITSF) in 2001 and chairs the ITSF Steering Group. He is also a member of the Workshop for Sync in Telecommunications Systems (WSTS) Steering

Group which meets annually in Boulder, Colorado. Charles is on the Steering Group for the UK governmental department - Business Innovation and Skills – Technology Strategy Board - Knowledge Transfer Network (KTN) for Digital Systems (previously Location and Timing) and is a Fellow of the Institution of Engineering and Technology (IET). Charles is also a member of the Industry Advisory Boards to Universities of Bath and Liverpool, Electrical and Electronics Faculties.

Acronyms

Acronym	Meaning
3GPP	Third Generation Partnership Project
A-GPS	Assisted GPS
ATIS	Alliance for Telecommunications Industry Solutions
BITS	Building Integrated Timing Source
CDMA	Code Division Multiple Access
CE	Conformité Européenne
Cs	Caesium (Atomic Frequency Standard)
CSAC	Chip Scale Atomic Clock
DAB	Digital Audio Broadcast
DVB	Digital Video Broadcast
eLoran	Enhanced Long Range Navigation
EMC	Electromagnetic Compatibility
ETSI	European Telecommunications Standards Institute
FDD	Frequency Division Duplex
FPT	Frequency, Phase and Time
GPS	Global Positioning System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ITSF	International Telecom Sync Forum
ITU	International Telecommunications Union
LTE	Long Term Evolution
MTBF	Mean Time Between Failures
MTTR	Mean Time to Repair
NGN	Next Generation (Telecom) Networks
NTP	Network Time Protocol
OCXO	Oven Controlled Crystal Oscillator
PDV	Packet Delay Variation
PNT	Positioning, Navigation & Timing
PRC	Primary Reference Clock
PTPv2	Precision Time Protocol v2 (IEEE-1588-2008)
Rb	Rubidium (Atomic Clock)
SDH	Synchronous Digital Hierarchy
SSU	Synchronisation Source Utility
SyncE	Synchronous Ethernet
TCXO	Temperature Compensated Crystal Oscillator
TDD	Time Division Duplex
TDM	Time Division Multiplex
TETRA	Terrestrial European Trunked Radio Access
UTC	Universal Coordinated Time (Universal Temps Coordinate)
VoIP	Voice over Internet Protocol
VSWR	Voltage Standing Wave Ratio
WSTS	Workshop in Synchronization for Telecommunications Systems