Power Matters.™

Microsemi

Ensuring Robust Precision Time: Hardened GNSS, Multiband, and Atomic Clocks

Lee Cosart
lee.cosart@microsemi.com

WSTS 2018

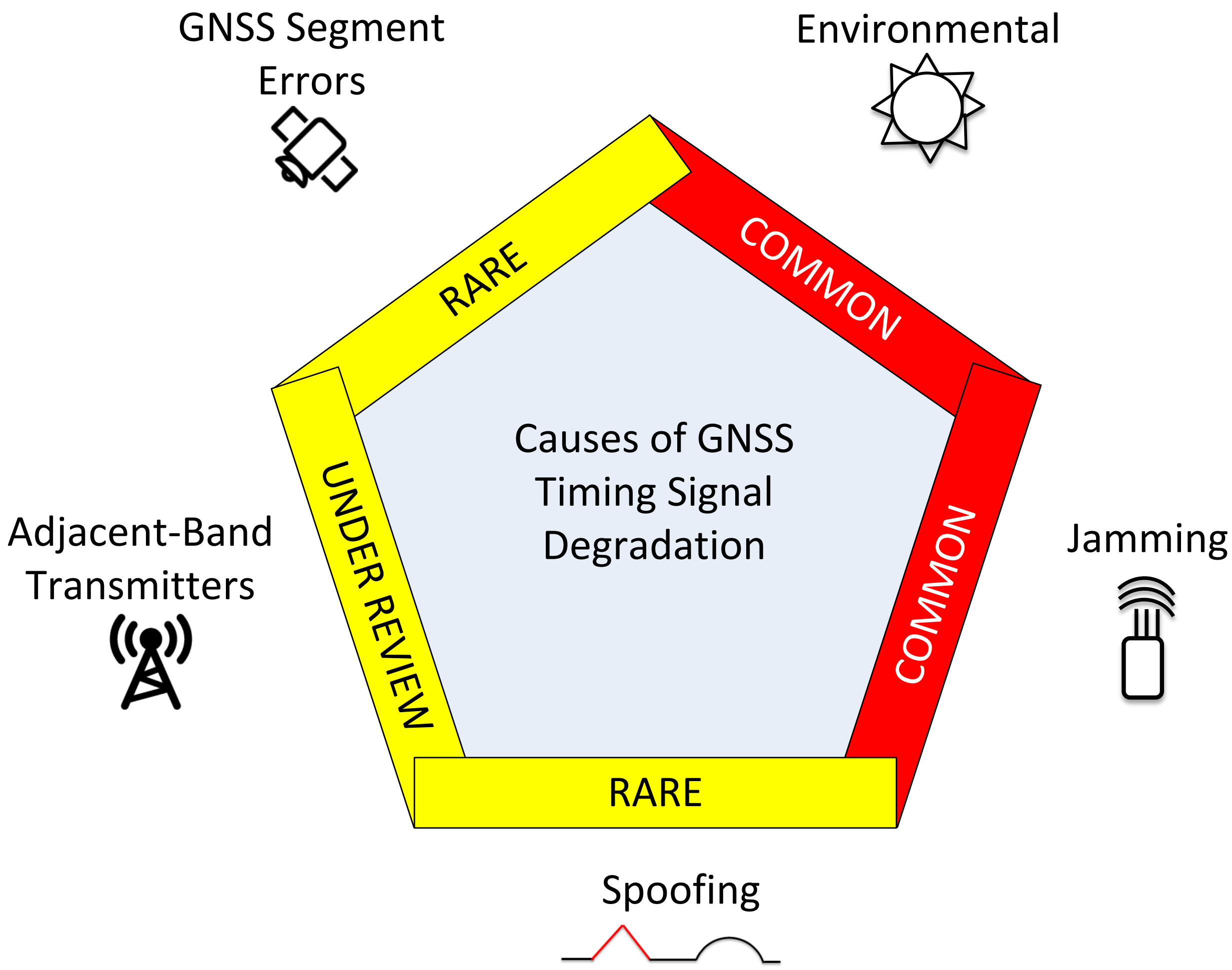
Outline

- Introduction
- The Challenge
  - Time requirements increasingly tighter
  - Signal environment increasingly more hostile
- The Solution
  - Hardened GNSS
  - Multiband (PRTC-B)
  - Atomic clocks (ePRTC)
- Summary

Telecom Timing Requirements

Application/ Technology	Accuracy	Specification
CDMA2000	3 µs	[b-3GPP2 C.S0002] section 1.3; [b-3GPP2 C.S0010] section 4.2.1.1
TD-SCDMA	3 µs	[b-3GPP TS 25.123] section 7.2
LTE-TDD (home-area)	3 µs	[b-3GPP TS 36.133] section 7.4.2; [b-3GPP TR 36.922] section 6.4.1.2
WCDMA-TDD	2.5 µs	[b-3GPP TS 25.402] sections 6.1.2 and 6.1.2.1
WiMAX (downlink)	1.428 µs	[b-IEEE 802.16] table 6-160, section 8.4.13.4
WiMAX (base station)	1 µs	[b-WMF T23-001], section 4.2.2
LTE MBSFN	1 µs	Under study
PRTC	100 ns	[ITU-T G.8272] (Primary Reference Time Clock)
ePRTC	30 ns	[ITU-T G.8272.1] (Enhanced Primary Reference Time Clock)

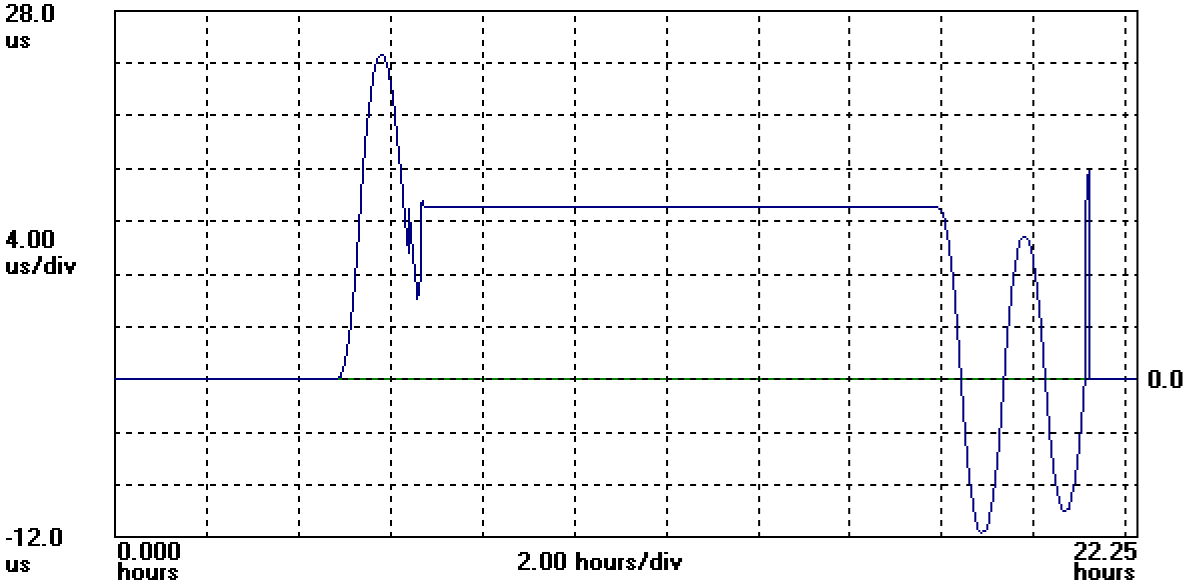
Known GNSS Vulnerabilities to Telecom



This, as well as solutions for mitigating these vulnerabilities, is discussed in the ATIS technical report on GPS vulnerability ATIS-0900005, which can be downloaded here: http://www.atis.org/01_resources/whitepapers.asp

Example: GNSS Segment Error

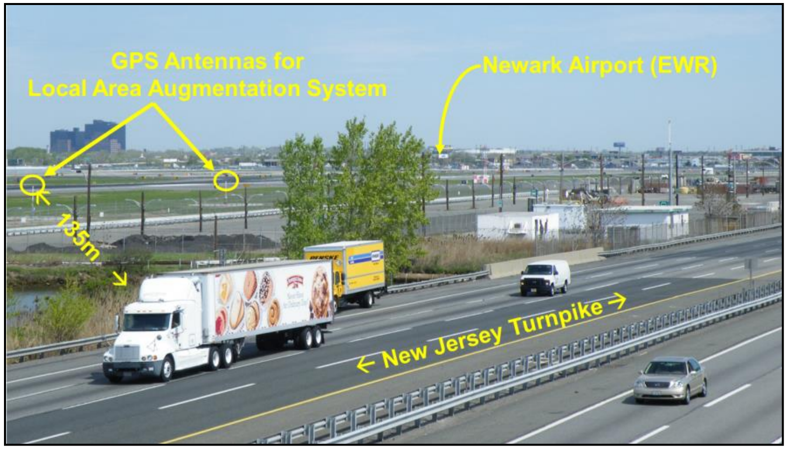
January 2016 GPS Segment Error:
13 µs UTC offset error



Plot showing how the anomaly event impacted one GPS timing receiver

Example: GNSS Jamming

- **GPS signals are vulnerable**
  - GPS signals are received at a very low power levels when they reach the Earth and are easy to disrupt
  - Many types of GPS jammers exist (CW, swept RF, matched spectrum, broadband, etc.) but they are all built with the purpose of preventing GPS signal reception
- **GPS jamming threats are rampant throughout the world**
  - Many publicized events involving GPS jammers disrupting critical infrastructure
  - GPS disruptions are the result of intentional and unintentional jamming
    - Local Area Augmentation System unintentionally jammed by passing vehicles using personal privacy devices
    - South Korea intentionally jammed using high power jamming devices deployed by adversaries



Intentional High-Power GPS Jamming

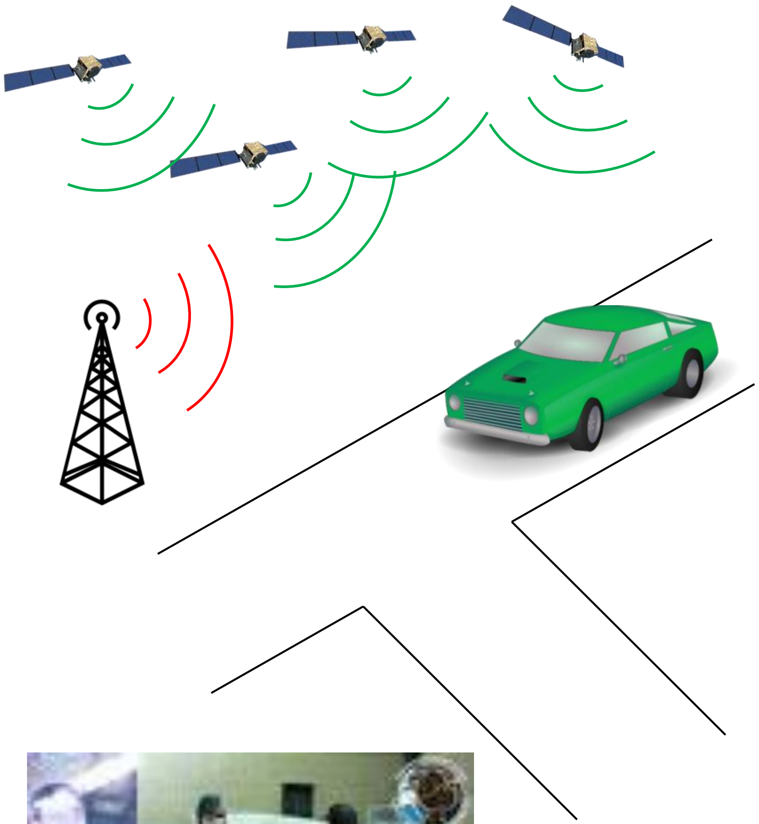
[The Central Radio Management Office, South Korea]

Dates	Aug 23-26, 2010 (4 days)	Mar 4-14, 2011 (11 days)	Apr 28 – May 13, 2012 (16 days)
Jammer locations	Gaesong	Gaesong, Mt. Gumgang	Gaesong
Affected areas	Gimpo, Paju, etc.	Gimpo, Paju, Gangwon, etc.	Gimpo, Paju, etc.
GPS disruptions	181 cell towers, 15 airplanes, 1 battle ship	145 cell towers, 106 airplanes, 10 ships	1,016 airplanes, 254 ships

Prof.Jiwon Seo – Yonsei University, South Korea, Resilient PNT Forum

Example: GNSS Spoofing

- **GPS spoofing attacks transmit signals that appear to be from a GPS satellite**
  - Spoofer can transmit a single satellite signal or multiple signals to simulate an entire GPS constellation
  - GPS receivers use the spoofed signals but produce an incorrect position and time solution
  - Almost all spoofing attacks are precipitated by a jamming event in which the GPS receiver losses lock on the correct GPS signals and then they are replaced with the spoofed GPS signals

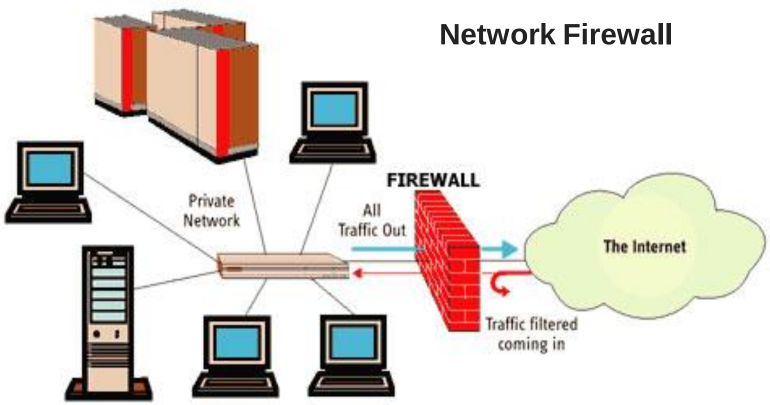


- **Spoofing attacks are more complicated, and while less prevalent than jamming attacks, are on the increase**
  - Iran claimed to have captured a RQ-170 using GPS spoofing techniques
  - Russia Black Sea spoofing attack
  - Academia has demonstrated the feasibility of spoofing GPS on many occasions

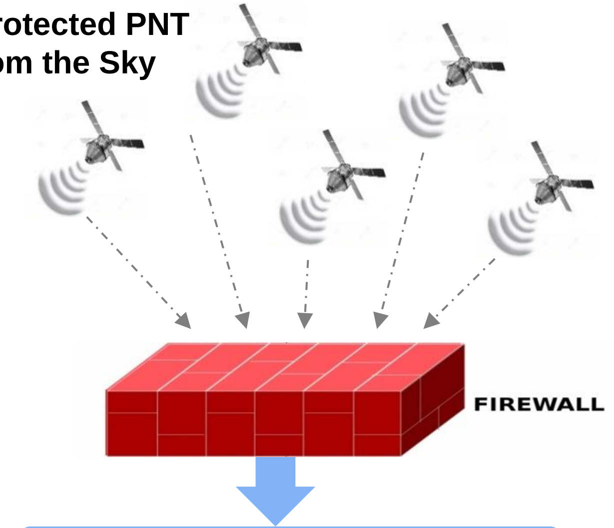
GNSS Firewall

Physical Firewall at Electrical Substation

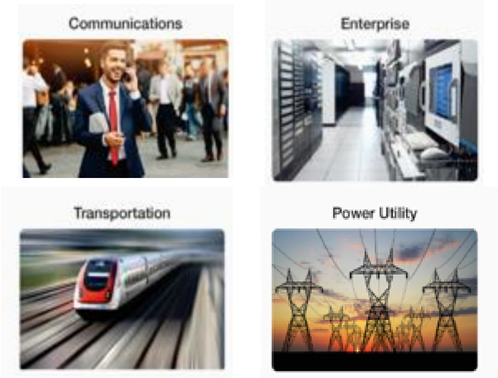
Network Firewall



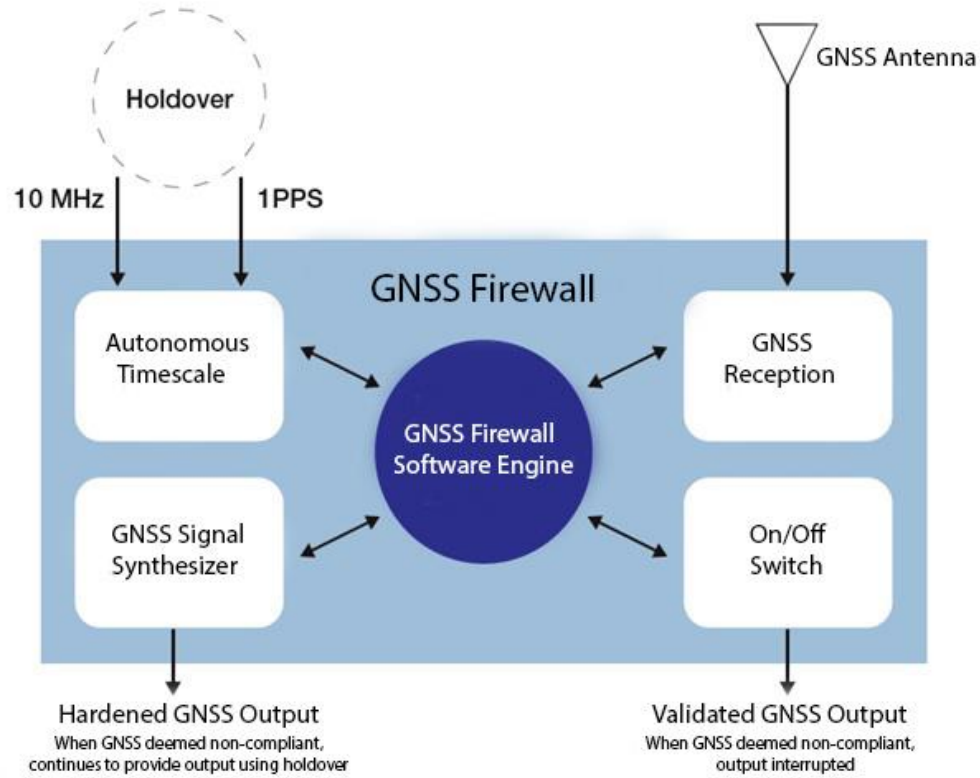
Unprotected PNT from the Sky



Secure PNT for Critical Infrastructure



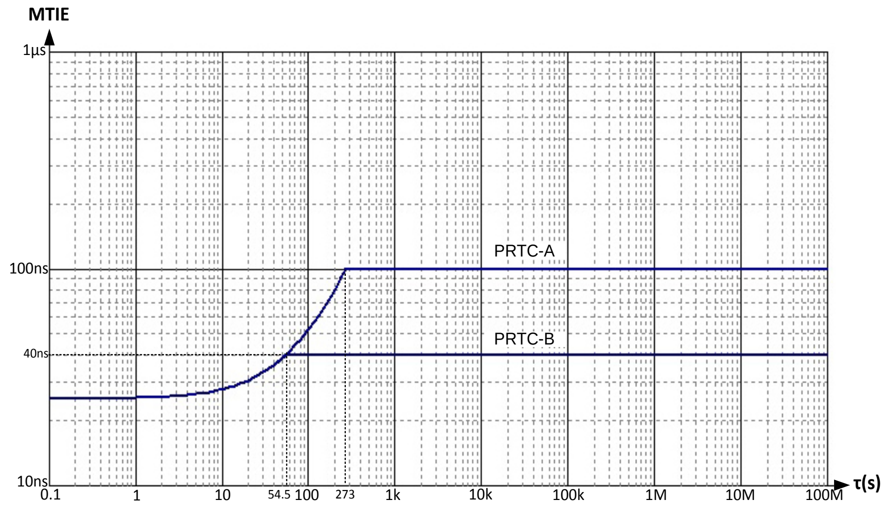
GNSS Firewall

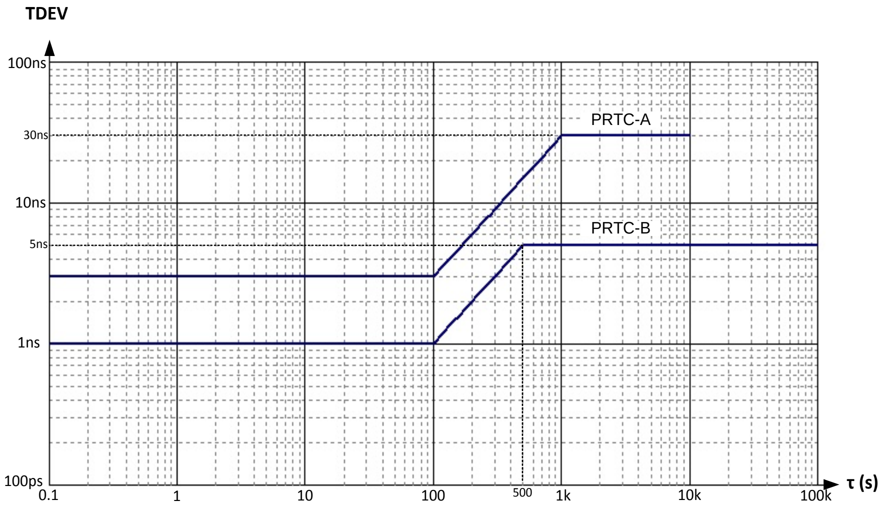


- Identifies spoofing and jamming and protects GNSS systems using autonomous timescale and analysis of incoming GNSS signal power
- 1PPS and 10 MHz timing reference inputs can be used for extended holdover and enhanced detection capabilities
- In the event of anomalous conditions, validated GNSS output turned off but hardened GNSS output can be used
- Hardened GNSS output is the most secure by providing a synthesized, fixed position, GNSS signal isolated from the live-sky environment

PRTC-B: Multiband for Improved Performance & Robustness

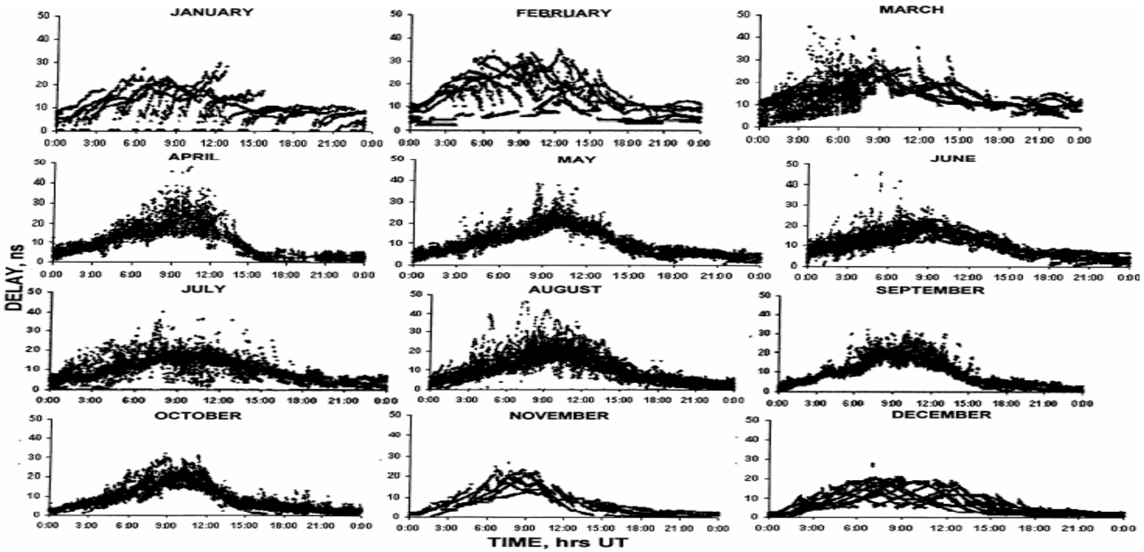
- A new class of PRTC is being worked on at the ITU-T, the PRTC-B
- The original PRTC will be called PRTC-A
- Proposed accuracy is 40 ns (vs. 100 ns for PRTC-A)
- Proposed MTIE/TDEV stability:





PRTC-B: Multiband for Improved Performance & Robustness

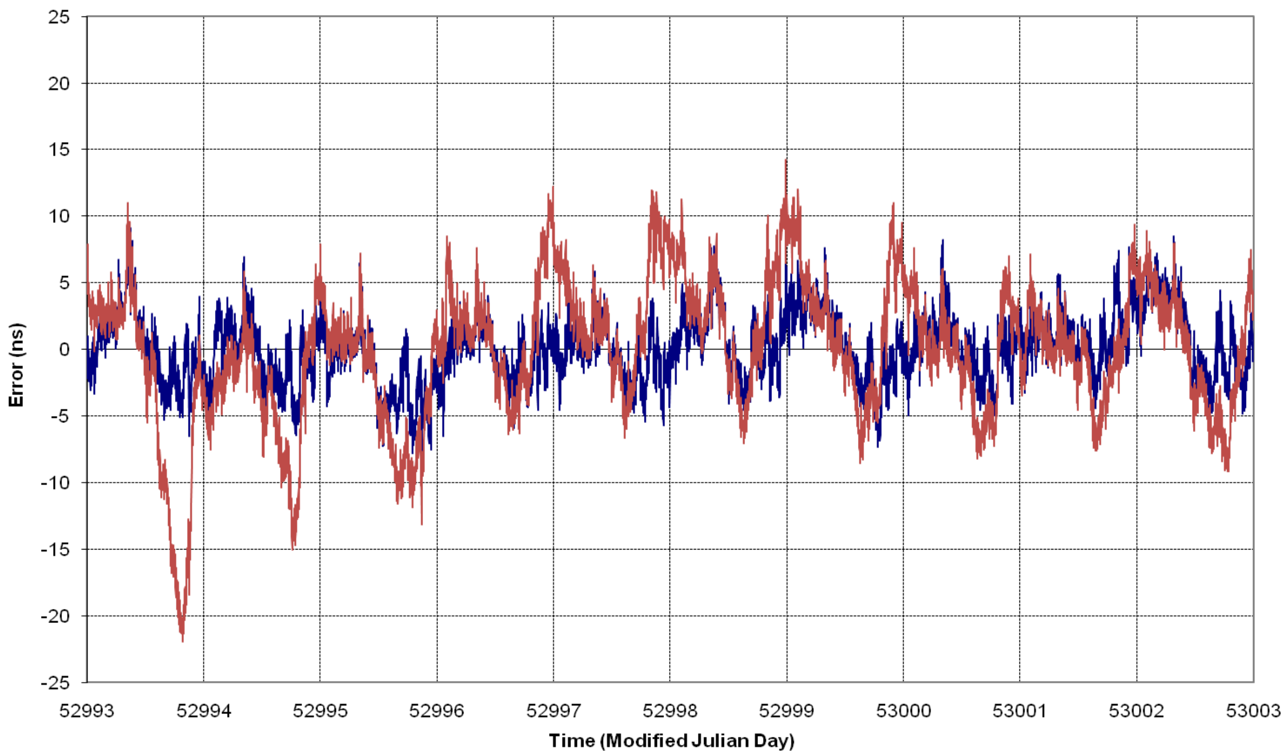
- Ionospheric delay varies diurnally with that variation changing through the year
- Ionospheric diural pattern changes throughout the year
- Space weather can also affect ionosphere



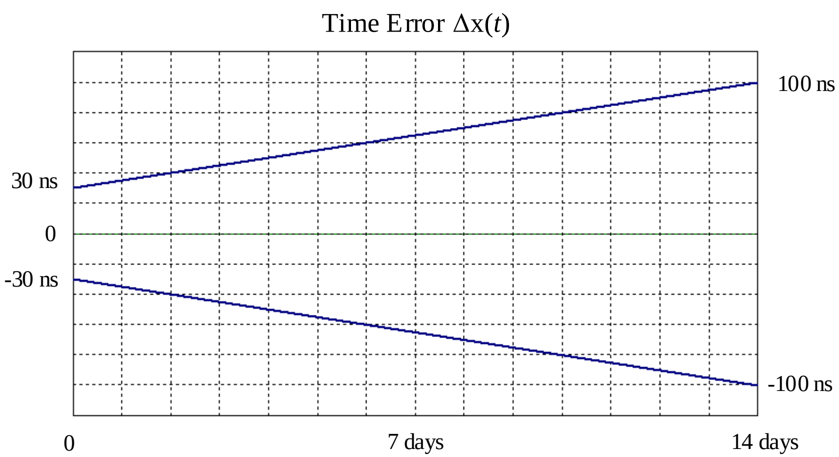
- Multiband receivers can accurately estimate ionospheric delay by using signals at different frequencies

PRTC-B: Multiband for Improved Performance & Robustness

- L1-only (single-band) receiver in red vs. L1/L2 (multiband) receiver in blue, with its ability to accurately estimate ionospheric delay dynamically, shows the performance advantage for multiband



ePRTC: GNSS + Atomic Clock



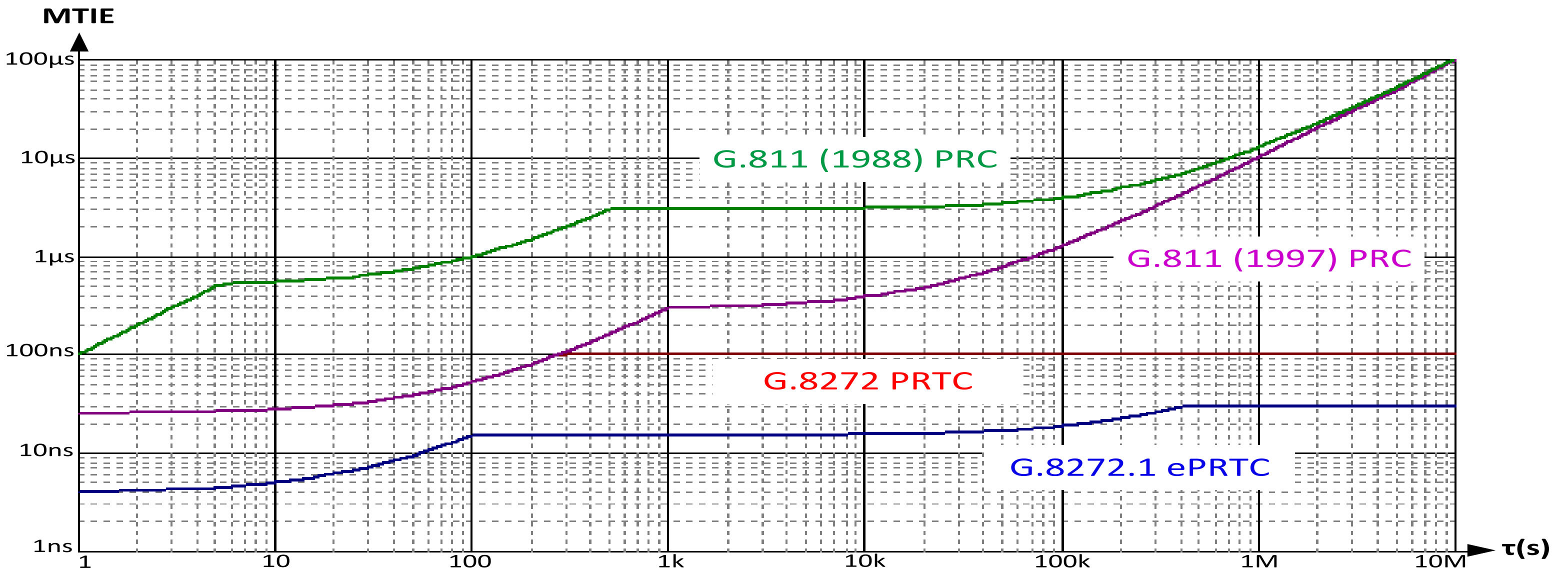
ePRTC: "enhanced primary reference time clock"

- Holds better that 100ns for 14 days of holdover "Class A"
- With better atomic clock, longer holdover ("Class B" 100ns for 80 days under discussion)
- Defined in ITU-T G.8272.1 (consented Sept 2016, published Feb 2017)
- GNSS (time reference) and autonomous primary reference clock as required inputs

- ePRTC attributes
  - Reliability: Immune from local jamming or outages
  - Autonomy: Atomic clock sustains timescale with & without GNSS connection
  - Coherency: 30ns coordination assures overall PRTC budget
  - Holdover: 14-day time holdover <= 100 ns

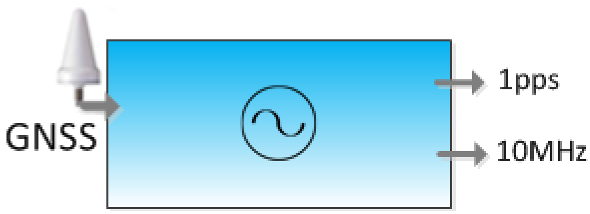
Primary Reference Clock Performance History

- G.811 (1988) *Timing requirements at the outputs of primary reference clocks suitable for plesiochronous operation of international digital links*
  MTIE (1000s)= 3µs
- G.811 (1997) *Timing characteristics of primary reference clocks*
  MTIE (1000s)= 300ns
- G.8272 (2012) *Timing characteristics of primary reference time clocks*
  MTIE (1000s)= 100ns
- G.8272.1 (2016) *Timing characteristics of enhanced primary reference time clocks*
  MTIE (1000s)= 15ns



PRTC vs. ePRTC Time Accuracy and Stability

PRTC



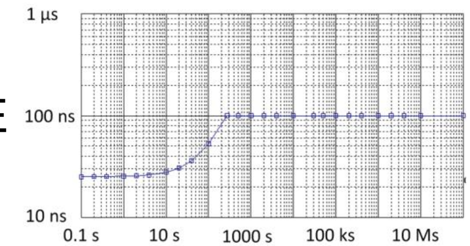
G.8272

Time Accuracy

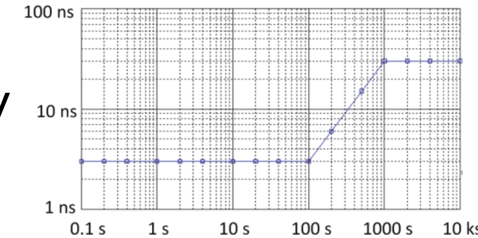
Time Error: <=100ns

Time Stability

MTIE

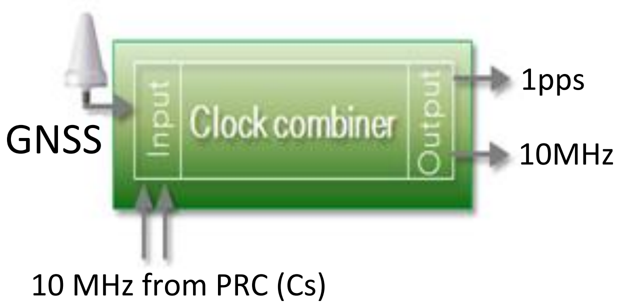


TDEV



MTIE is G.811 with 100 ns maximum
TDEV is G.811 exactly

ePRTC



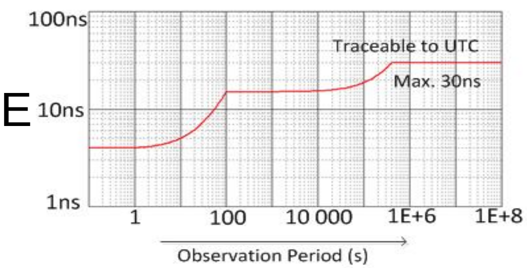
G.8272.1

Time Accuracy

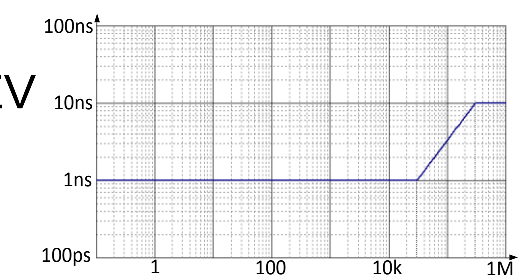
Time Error: <=30ns

Time Stability

MTIE

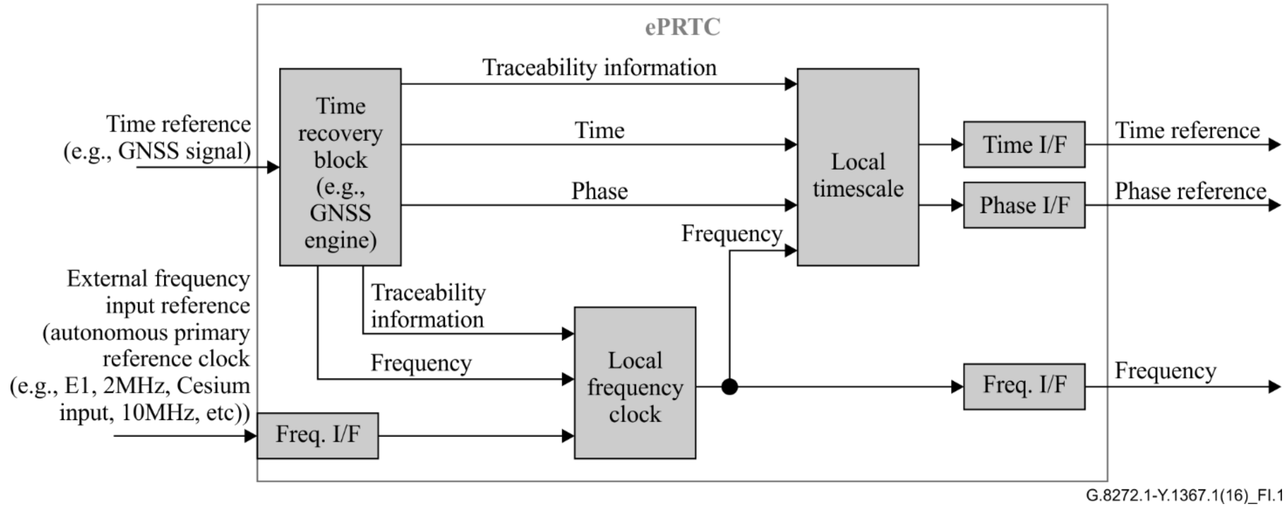


TDEV



MTIE below G.8272 with 30 ns maximum
TDEV below G.8272 and tau extended

ePRTC Functional Model

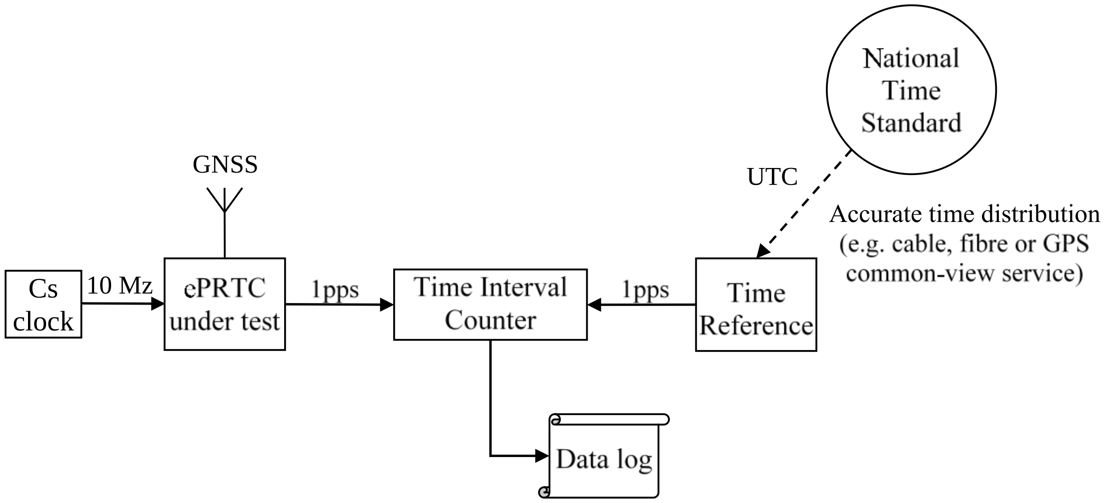


"Autonomous primary reference clock" is a key component of the ePRTC

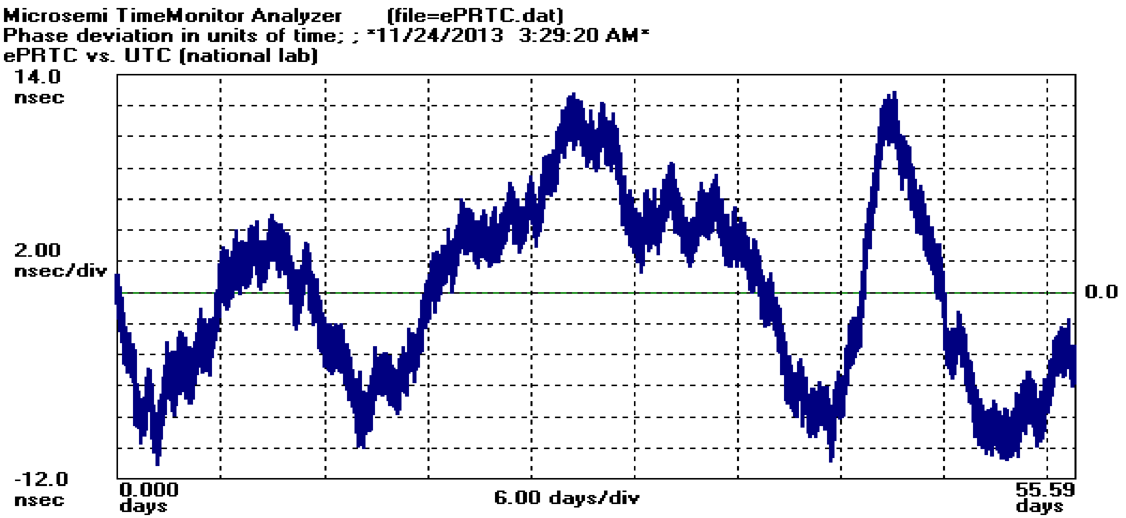
- Provides for highly accurate time of better than 30ns to UTC in combination with time reference
- Provides robust atomic-clock based time even during extended GNSS outages
- Long time constants can address diurnal effects such as those arising from variation in ionospheric delay of signals from GNSS satellites

Time Accuracy: ±30 ns vs. UTC

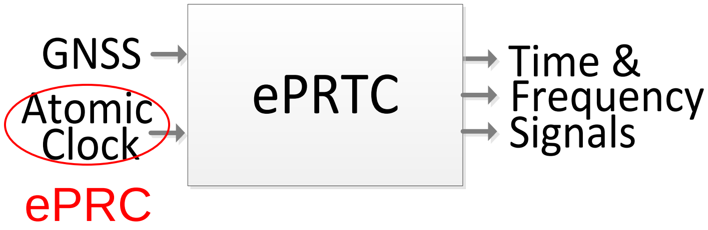
Setup for testing ePRTC against UTC:



Example measurement of ePRTC vs. UTC measured at a national lab:



ePRTC Time Holdover: Security



The “autonomous ePRC” with its ability to provide extended time holdover in the event of loss of GNSS provides security for the ePRTC system.

ePRTC “Autonomous PRC” requires G.811.1 ePRC

- G.811 clock requirements do not meet G.8272.1 “autonomous primary reference” requirements
- This led to the necessity of defining a TDEV requirement in G.8272.1 Annex A which then became the ePRC G.811.1 TDEV
- Essentially a new ITU-T “enhanced primary reference clock” had been defined, the “ePRC”
- Longer holdover (“Class B” ePRTC) would require more: The longer the holdover, the better the “autonomous primary reference” required.

Summary

- Timing requirements are becoming increasingly tight, with sources of time needing to deliver tens of nanoseconds or better to UTC.

- GNSS is the principal source of precision time, delivering time to critical infrastructure including communication, power infrastructure, and the financial industry.

- The ensuing performance and security requirements can be addressed by hardening GNSS, by using multiband, and by using GNSS in combination with standalone, autonomous atomic clocks.

- The solution for improving performance and security:
  - Hardened GNSS (GNSS Firewall)
  - Multiband (PRTC-B)
  - Atomic clocks (ePRTC)

Thank You

Lee Cosart

Senior Technologist

Lee.Cosart@microsemi.com

Phone: +1-408-428-7833