Microsemi

a MICROCHIP company

Securing GPS Systems Against Signal-in-Space Threats

Jeremy Warriner

- Director, Government Systems
- Office: (303) 539-4914
- Email: jeremy.warriner@microchip.com

Rich Foster

- Senior Manager, Business Development
- Office: (303) 539-4971
- Email: rich.foster@microchip.com

Randy Brudzinski

- Vice President, Frequency & Time Division
- Office: (408) 428-7986
- Email: randy.brudzinski@microchip.com

Overview

- Threats to GPS and Our Critical Infrastructure
- Actionable Solutions for Hardening our Infrastructure and Residual Gaps
- Summary

Global Positioning System

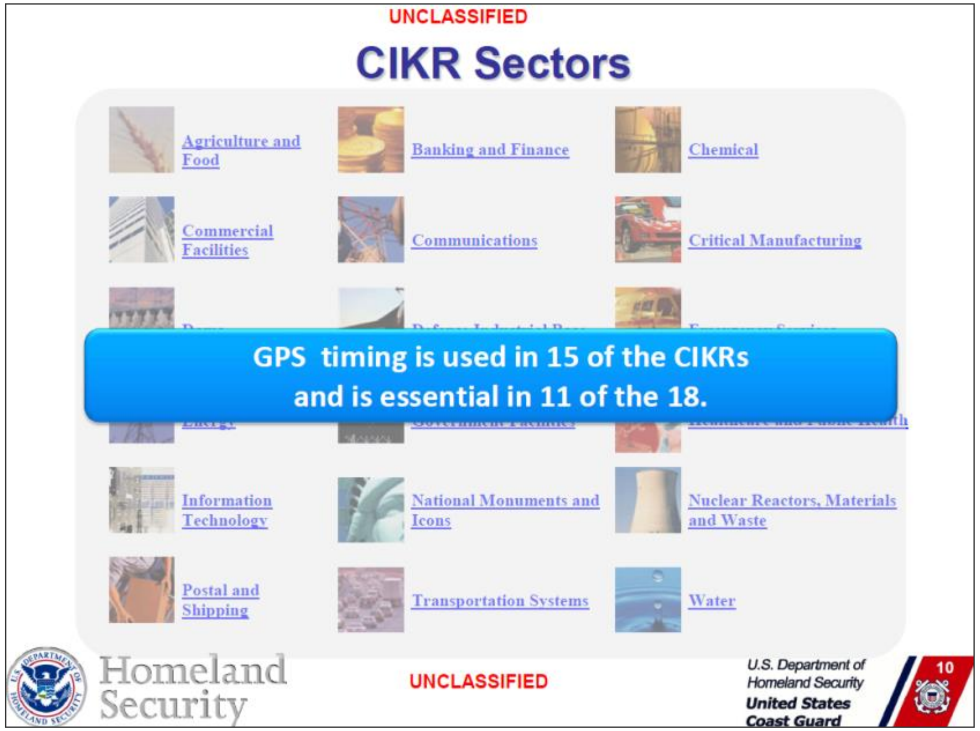
A Victim of its Own Success

The Biggest Insider Threat: GPS Receivers

- **Insider threats aren’t always people, they can be “things” as well**
  - Chelsea Manning (2010): Leaked ~750,000 documents to WikiLeaks
  - Edward Snowden (2013): Leaked information on global surveillance programs run by the NSA
  - Stuxnet (2010): Infected PLC devices were used in and ultimately destroyed Iranian centrifuges

- **GPS receivers have become trusted insiders**
  - The Positioning, Navigation, and Timing (PNT) solution provided by GPS is “blindly” trusted by many systems
  - GPS receivers are essential to 11 of the 18 Critical Infrastructure and Key Resource (CIKR) sectors

Industry must “open its eyes” to the potential impact of GPS attacks and actively participate in the defense of the services they provide



UNCLASSIFIED

CIKR Sectors

Agriculture and Food	Banking and Finance	Chemical
Commercial Facilities	Communications	Critical Manufacturing
Information Technology	National Monuments and Icons	Nuclear Reactors, Materials and Waste
Postal and Shipping	Transportation Systems	Water

GPS timing is used in 15 of the CIKRs and is essential in 11 of the 18.

Homeland Security

UNCLASSIFIED

U.S. Department of Homeland Security
United States Coast Guard

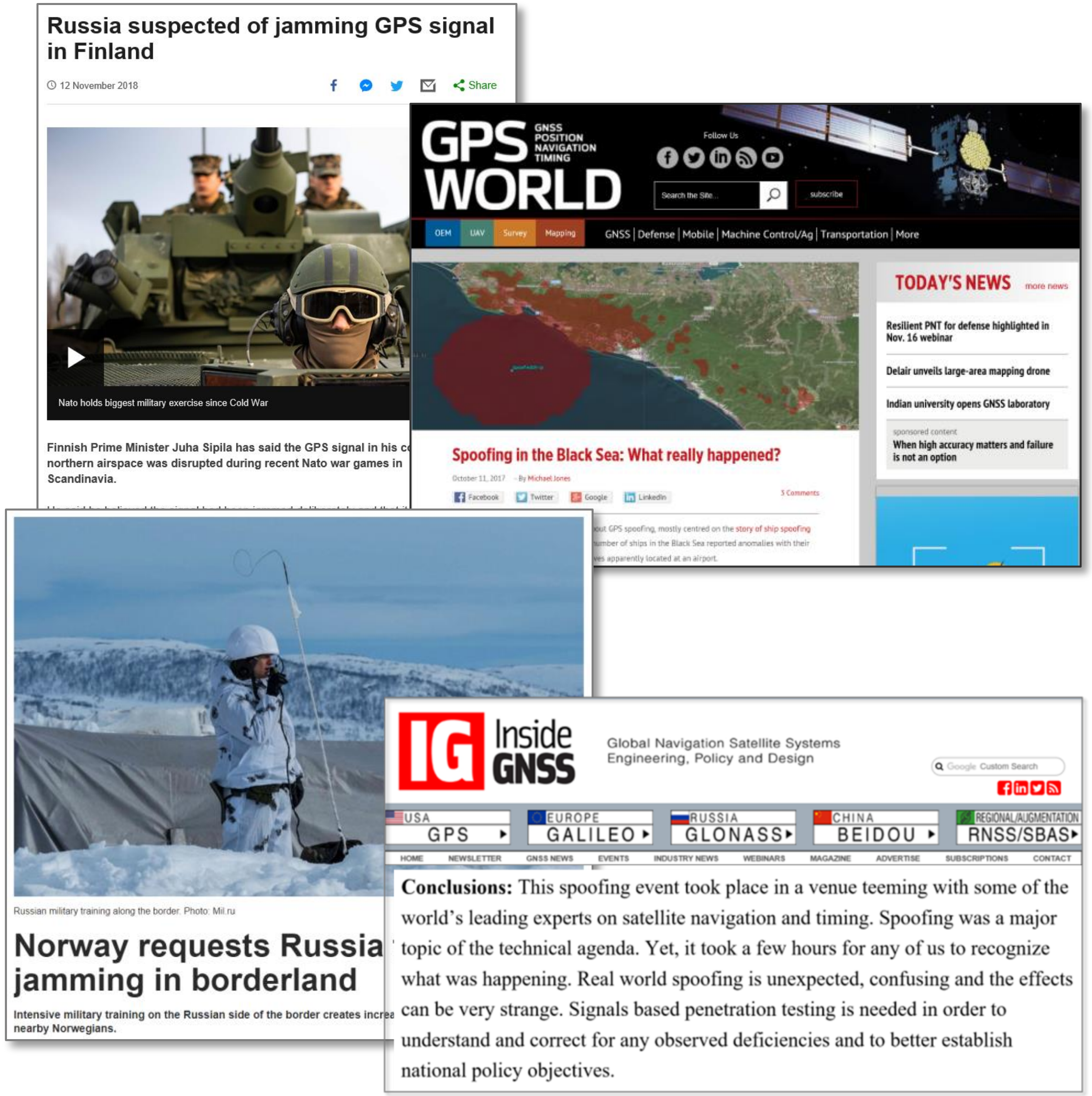
10

GPS Enables our Critical Infrastructure

- **Positioning, Navigation, and Timing (PNT) is not identified as a Critical Infrastructure and Key Resource (CIKR) sector but a majority of CIKR sectors depend upon it**
  - There is no obligation for continued availability or performance of the GPS system
  - The occurrences of PNT disruption are increasingly frequent and occur overseas and in the U.S.

- **Continued availability of PNT service is in the economic and strategic interests of the U.S.A.**
  - Enables other services to be provided at a lower cost point to our citizens (good use of taxpayer dollars)

Government must accept its role in providing assured PNT service or enabling industry to provide assured PNT services



Russia suspected of jamming GPS signal in Finland

12 November 2018

Share

Nato holds biggest military exercise since Cold War

Finnish Prime Minister Juha Sipila has said the GPS signal in his c
northern airspace was disrupted during recent Nato war games in Scandinavia.

GPS WORLD GNSS POSITION NAVIGATION TIMING

Follow Us

Search the Site...

subscribe

OEM | UAV | Survey | Mapping | GNSS | Defense | Mobile | Machine Control/Ag | Transportation | More

Spoofing in the Black Sea: What really happened?

October 11, 2017 · By Michael Jones

Facebook Twitter Google LinkedIn

3 Comments

out GPS spoofing, mostly centred on the story of ship spoofing
umber of ships in the Black Sea reported anomalies with their
ves apparently located at an airport.

TODAY'S NEWS more news

Resilient PNT for defense highlighted in Nov. 16 webinar

Delair unveils large-area mapping drone

Indian university opens GNSS laboratory

sponsored content

When high accuracy matters and failure is not an option

Russian military training along the border. Photo: Mil.ru

Norway requests Russia
jamming in borderland

Intensive military training on the Russian side of the border creates increa
nearby Norwegians.

IG Inside GNSS

Global Navigation Satellite Systems Engineering, Policy and Design

Google Custom Search

USA GPS | EUROPE GALILEO | RUSSIA GLONASS | CHINA BEIDOU | REGIONAL/AUGMENTATION RNSS/SBAS

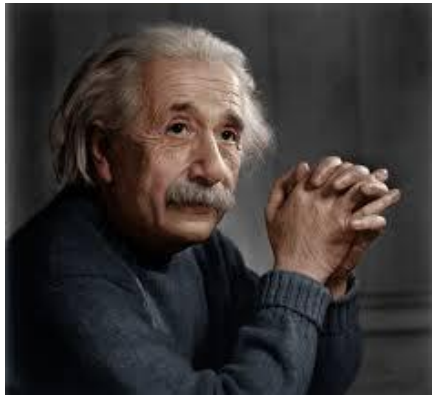
HOME | NEWSLETTER | GNSS NEWS | EVENTS | INDUSTRY NEWS | WEBINARS | MAGAZINE | ADVERTISE | SUBSCRIPTIONS | CONTACT

Conclusions: This spoofing event took place in a venue teeming with some of the world's leading experts on satellite navigation and timing. Spoofing was a major topic of the technical agenda. Yet, it took a few hours for any of us to recognize what was happening. Real world spoofing is unexpected, confusing and the effects can be very strange. Signals based penetration testing is needed in order to understand and correct for any observed deficiencies and to better establish national policy objectives.

Signal-in-Space Threat

- **Signal in space threats are generally categorized based on the failure mode they induce in a GPS receiver**
  - **Jamming**: Partial or complete loss of ability to receive GPS signals
  - **Spoofing**: Tricking a GPS receiver into receiving illegitimate signals
- **Many GNSS systems are available for use but they provide minimal protection against signal-in-space threats**
  - Other constellations are useful in detecting errors in the space and ground segments of GPS but these errors are few and far between
  - GNSS constellations are relatively close in frequency so jamming events often impact all the constellations
  - It is only slightly less trivial to spoof multiple GNSS systems than it is to spoof GPS alone

System	GPS	GLONASS	BeiDou	Galileo	IRNSS
Owner	United States	Russian Federation	China	European Union	India
Coding	CDMA	FDMA	CDMA	CDMA	CDMA
Number of satellites	31 (at least 24 by design)[8]	28 (at least 24 by design) including:[9] 24 operational 2 under check by the satellite prime contractor 2 in flight tests phase	5 geostationary orbit (GEO) satellites, 30 medium Earth orbit (MEO) satellites	8 test bed satellites in orbit, 22 operational satellites budgeted	3 geostationary orbit (GEO) satellites, 4 geosynchronous orbit satellites
Frequency	1.57542 GHz (L1 signal) 1.2276 GHz (L2 signal)	Around 1.602 GHz (SP) Around 1.246 GHz (SP)	1.561098 GHz (B1) 1.589742 GHz (B1-2) 1.20714 GHz (B2) 1.26852 GHz (B3)	1.164–1.215 GHz (E5a and E5b) 1.260–1.300 GHz (E6) 1.559–1.592 GHz (E2-L1-E11)	1.17645 GHz (L5) 2.492028 GHz (S1)
Status	Operational	Operational	15 satellites operational, 20 additional satellites planned	In preparation	4 satellites launched, 3 additional satellites planned to be launched by Early 2016



We cannot solve our problems with the same thinking that we used when we created them.

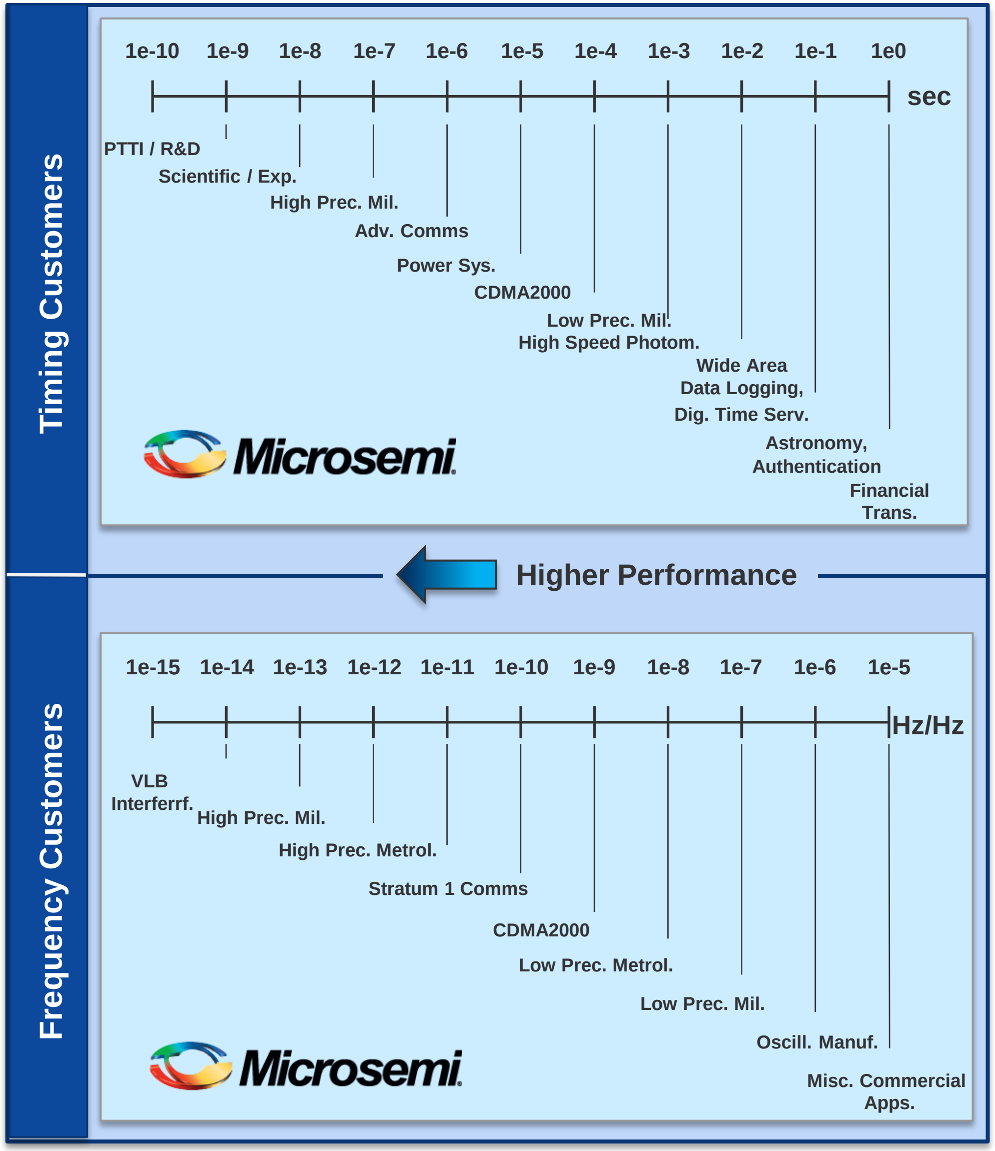
- Albert Einstein

The Sky is Not Falling

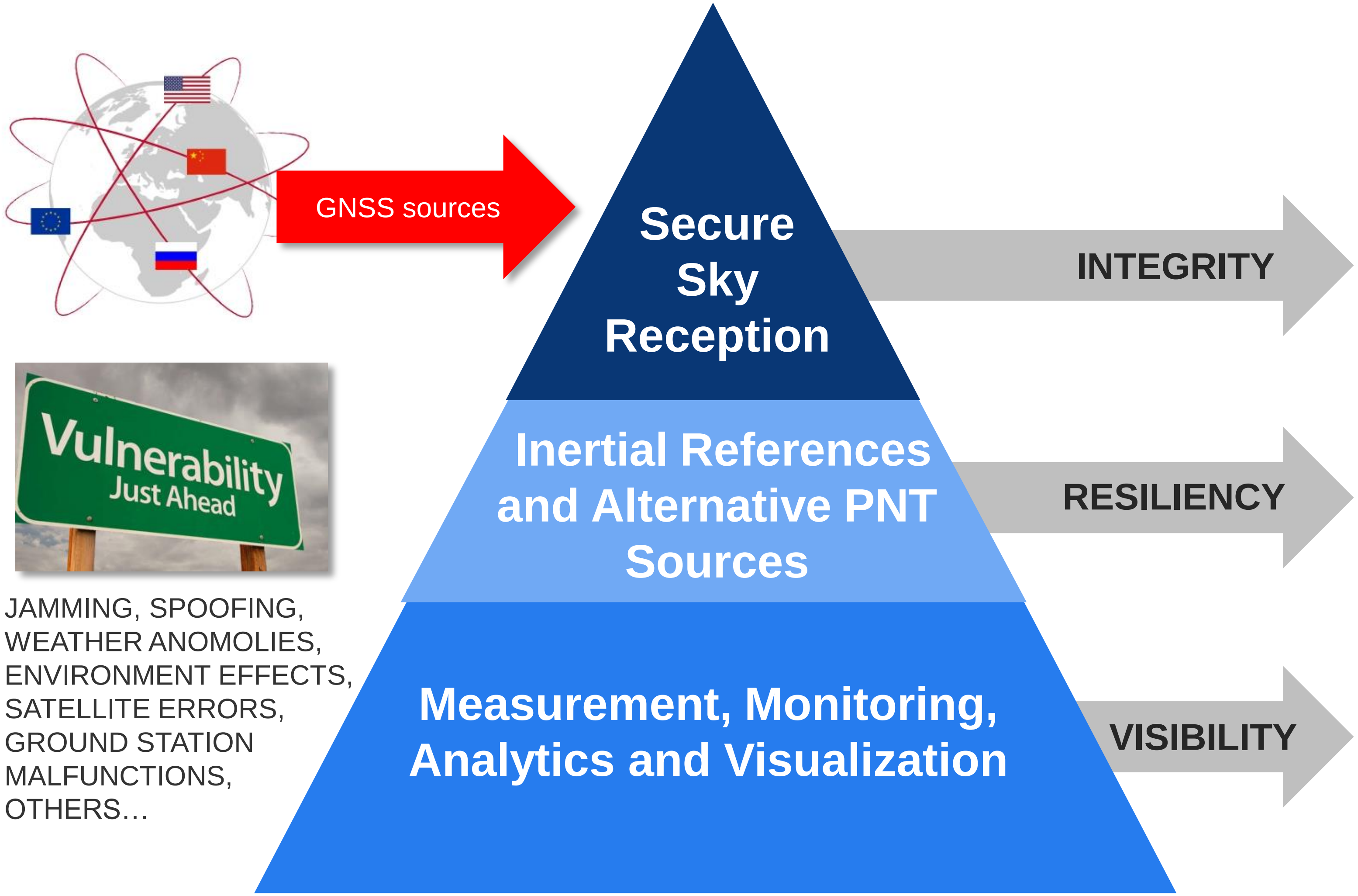
Real-world efforts to protect, toughen, and augment PNT infrastructure

User Requirements Vary Widely

- **A GPS problem does not necessitate a GPS solution**
  - Unwavering trust in GPS is the fundamental reason systems are vulnerable in the first place
  - A singular focus on “fixing” GPS vulnerabilities does not establish a secure system
- **There is no silver bullet that makes all GPS-based systems secure by design**
  - Timing applications have a wide array of users and performance requirements that don’t necessarily require GPS performance
  - Many technologies exist that can establish diversity in a system design so that GPS isn’t treated as the only solution



Protect, Toughen, and Augment PNT



JAMMING, SPOOFING, WEATHER ANOMOLIES, ENVIRONMENT EFFECTS, SATELLITE ERRORS, GROUND STATION MALFUNCTIONS, OTHERS…

Secure Sky Reception

INTEGRITY

Inertial References and Alternative PNT Sources

RESILIENCY

Measurement, Monitoring, Analytics and Visualization

VISIBILITY

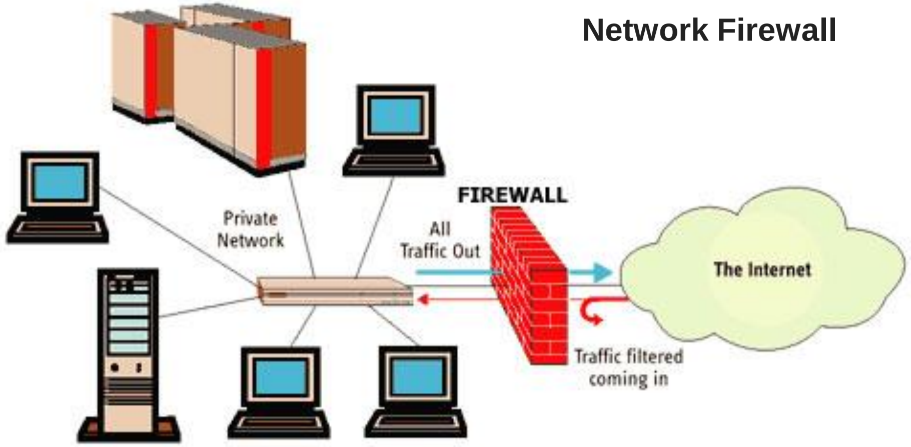
Secure PNT Objectives

- **Defend and protect PNT from threats**
- **Significantly mitigate GNSS disruptions through adoption of best practices and/or use of independent PNT sources**
- **Quickly identify and recover from PNT disruptions**

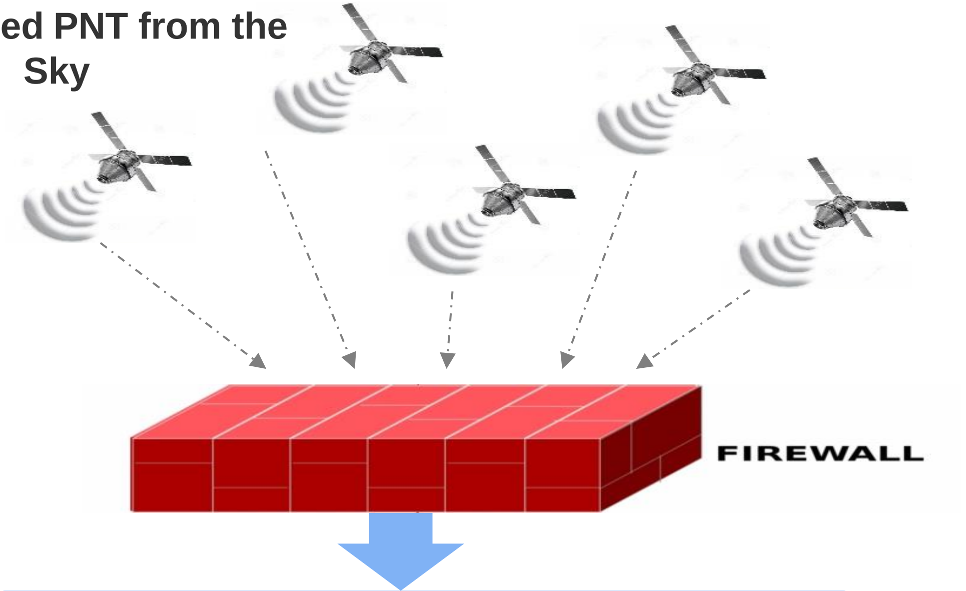
Signal-in-Space Integrity & the Firewall CONOP

Physical Firewall at Electrical Substation

Network Firewall



Unprotected PNT from the Sky



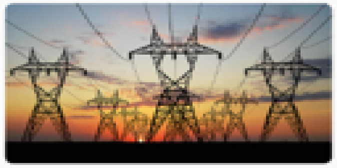
Secure PNT for Critical Infrastructure

Communications

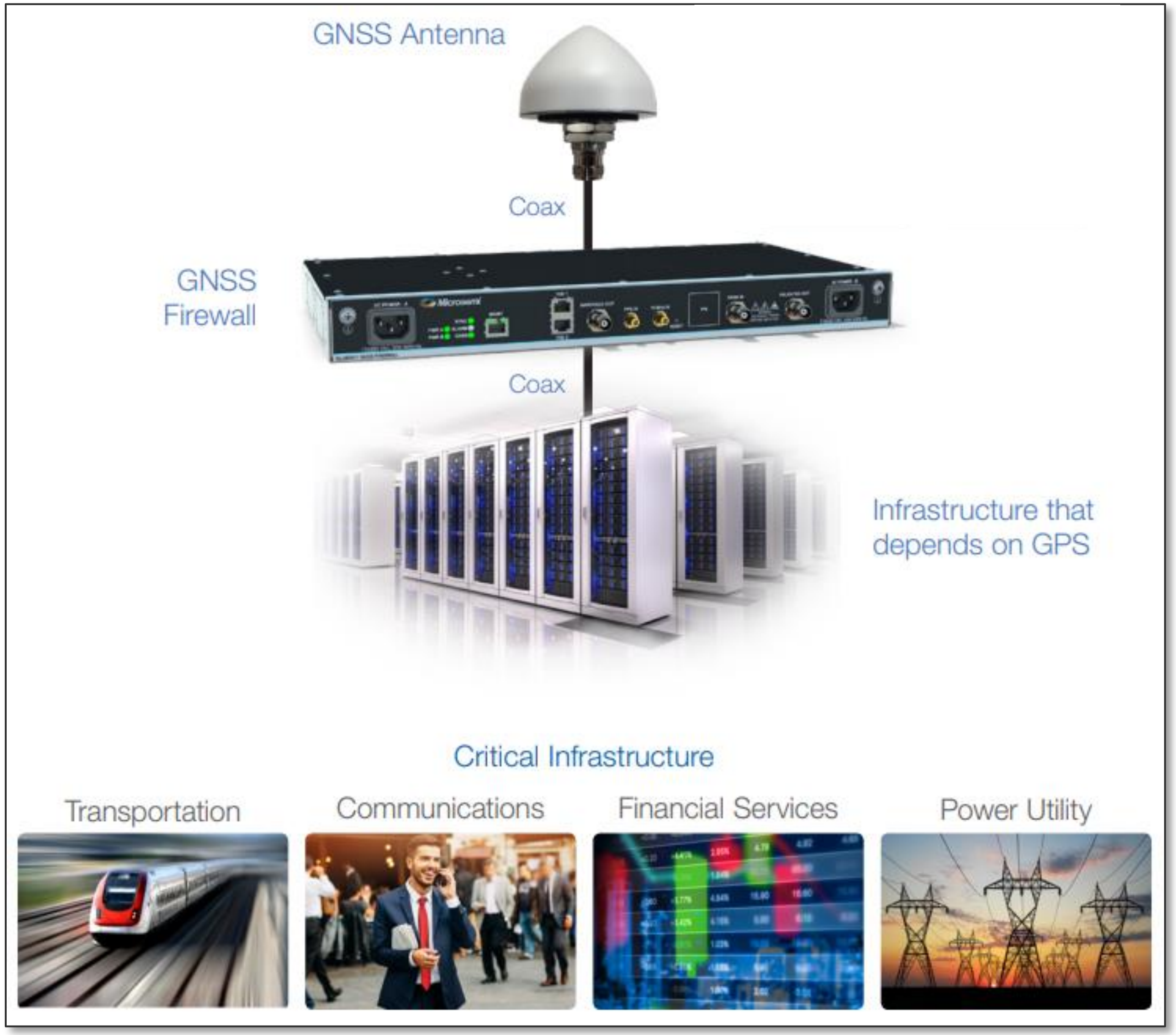
Enterprise

Transportation

Power Utility



GPS Firewall: Verifying the Integrity of GPS Signals



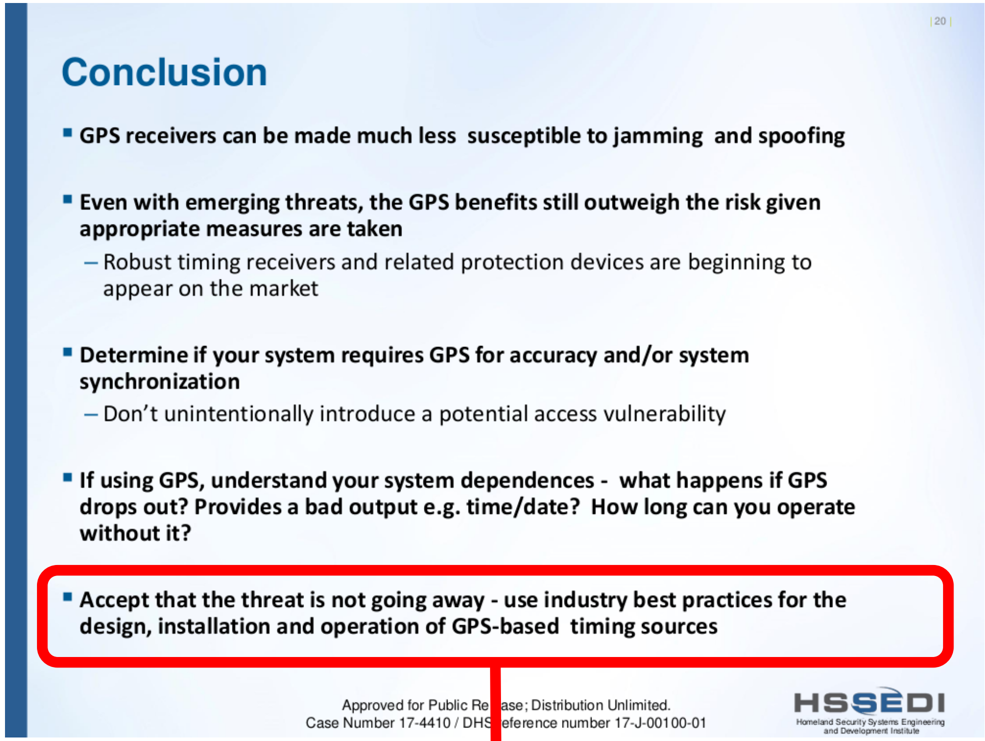
- **There are large deployments of GPS receivers within our critical infrastructure that do little to verify the integrity of GPS signals**
- **GPS firewall protects GPS receivers that would otherwise be vulnerable**
  - Uses multiple detectors to identify waveform, data, and solution anomalies in the GPS signal
  - Synthesizes a hardened GPS signal for downstream receivers to use
- **GPS firewall assumes that threats will evolve over time**
  - Detector algorithms are updated analogously to virus scanning software

Competent Receiver Testing

- **Responsibility for deploying competent GPS receivers or GPS systems is and should remain in the hands of system integrators**
  - System integrators can make the best decisions based on the specifics of their system
  - No need for a “one size fits all” standard that GPS receivers would be tested against

- **GPS threats are evolving similar to the way in which IT network threats evolve**
  - Having a “one size fits all” standard only addresses currently known threats, a better compliance model is NIST 800-53 where guidance is given but implementation is left to the system integrator
  - New GPS threat vectors need to be publicized so that industry can rapidly address them similar to the way it addresses IT threats
    - There is some assumption that Industry has the capability to rapidly update systems to address new threats

Excerpt from “Responsible Use of GPS for Critical Infrastructure” Briefing – Kevin Skey, 06 Dec 2017



| 20 |

Conclusion

- **GPS receivers can be made much less susceptible to jamming and spoofing**
- **Even with emerging threats, the GPS benefits still outweigh the risk given appropriate measures are taken**
  - Robust timing receivers and related protection devices are beginning to appear on the market
- **Determine if your system requires GPS for accuracy and/or system synchronization**
  - Don’t unintentionally introduce a potential access vulnerability
- **If using GPS, understand your system dependences - what happens if GPS drops out? Provides a bad output e.g. time/date? How long can you operate without it?**
- **Accept that the threat is not going away - use industry best practices for the design, installation and operation of GPS-based timing sources**

Approved for Public Release; Distribution Unlimited.
Case Number 17-4410 / DHS Reference number 17-J-00100-01

HSSEDI
Homeland Security Systems Engineering and Development Institute

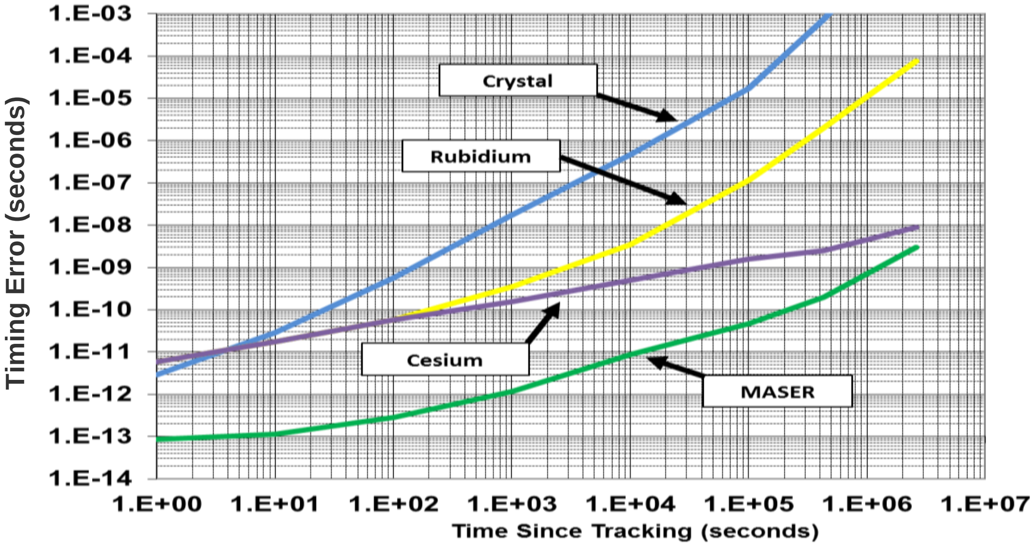
GPS Threats are Not Going Away and Will Continue to Evolve

Resiliency: Inertial References

- **Inertial references (e.g. inertial measurement units, frequency references) provide continuity of PNT service during GPS outages**
  - Highly complementary to GPS because they aren’t susceptible to the GPS threat vectors
  - Selection of an oscillator or IMU depends on the application requirements for operating duration without GPS

- **Inertial references also play a substantial role in validating the integrity of GPS signals**
  - The independent solution from oscillators or IMUs provide an incontrovertible reference that can be used to evaluate the integrity of the GPS solution
  - Higher stability frequency references and IMUs improve the ability of a system to detect GPS spoofing events

Atomic Clocks

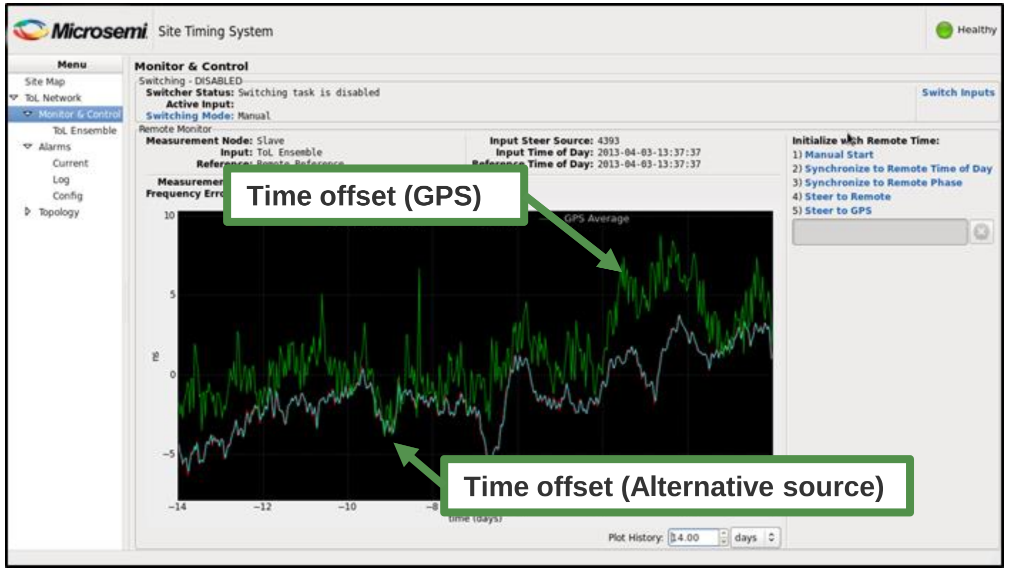


Oscillator Type Determines How Long A System Can Operate Without GPS

Resiliency: Alternative PNT Sources

- **Alternative sources of Positioning, Navigation, and Timing (PNT) distribution provide a high level of system resiliency**
  - PNT solution from multiple systems can be compared to ensure validity of the signals
  - Alternative PNT sources provide continuity of operations when other sources are unavailable
  - Alternative sources of PNT distribution should be as orthogonal to GPS as possible to minimize the number of shared threat vectors

- **PNT sources must all be traceable to the same timescale (e.g. UTC(USNO))**
  - Distribution technologies such as Precise Time Protocol almost always access UTC(USNO) via GPS
  - Without access to UTC(USNO) via independent sources, we are doomed to be dependent upon GPS
  - How does industry access UTC(USNO) without using GPS?



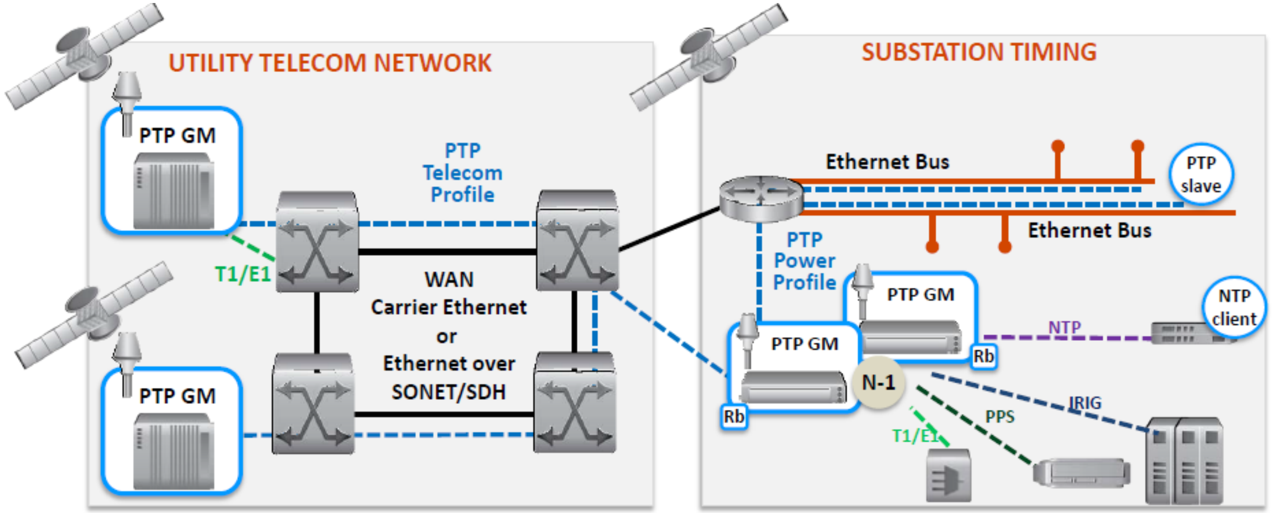
Monitor & Control

Switching - DISABLED
Switcher Status: Switching task is disabled
Active Input:
Switching Mode: Manual

Remote Monitor
Measurement Node: Slave
Input: ToL Ensemble
Reference: Remote Reference
Input Steer Source: 4393
Input Time of Day: 2013-04-03-13:37:37
Reference Time of Day: 2013-04-03-13:37:37
Measurement
Frequency Error

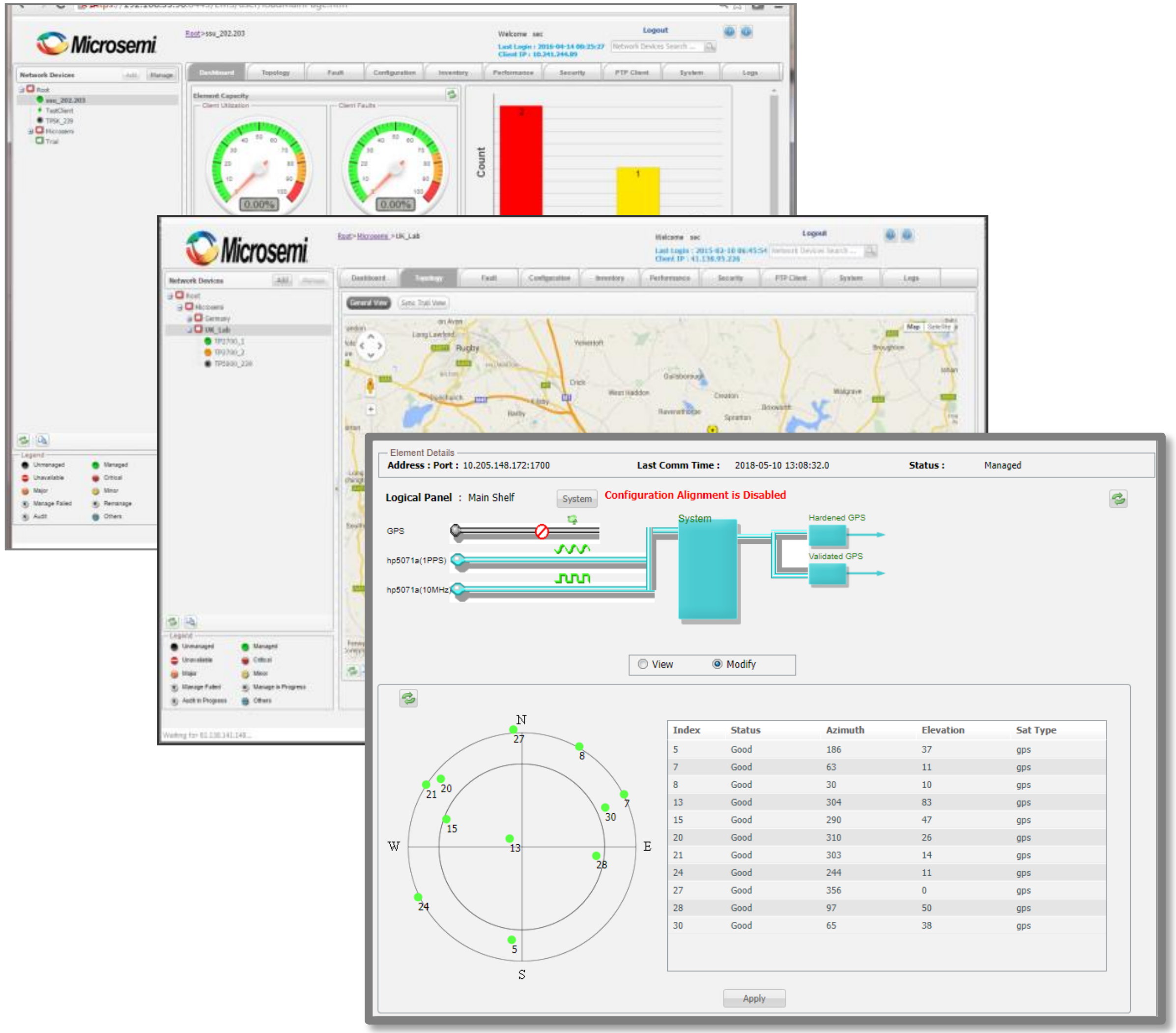
Initialize with Remote Time:
1) Manual Start
2) Synchronize to Remote Time of Day
3) Synchronize to Remote Phase
4) Steer to Remote
5) Steer to GPS

Plot History: 14.00 days



Visibility: Reporting GPS Anomalies

- **Ability of a system or its operators to quickly recover from anomalous GPS events is greatly aided by real-time diagnostics and reporting**
  - Knowing is half the battle: Knowing that GPS is suspect reduces time spent identifying and localizing the issue
  - Most users don't actively monitor the health of GPS and the install and forget culture needs to be changed
- **Potential for Industry to sense and report on GPS health is high due to the number of deployed GPS receivers**
  - Need an established mechanism or process that enables industry to report GPS issues
  - Need an established mechanism for distributing that information to other industry users



Element Details
Address : Port : 10.205.148.172:1700 **Last Comm Time :** 2018-05-10 13:08:32.0 **Status :** Managed

Logical Panel : Main Shelf System Configuration Alignment is Disabled

○ View ● Modify

Index	Status	Azimuth	Elevation	Sat Type
5	Good	186	37	gps
7	Good	63	11	gps
8	Good	30	10	gps
13	Good	304	83	gps
15	Good	290	47	gps
20	Good	310	26	gps
21	Good	303	14	gps
24	Good	244	11	gps
27	Good	356	0	gps
28	Good	97	50	gps
30	Good	65	38	gps

Summary

Summary

1. Actively defending GPS systems in critical infrastructure is an industry responsibility but government must openly share threat information

2. Access to UTC(USNO) is required for industry to fully participate in providing additional PNT distribution systems

3. Industry can leverage significant assets in the monitoring of GPS health but needs a mechanism for reporting issues

GPS Threat Protection Stack	
Ensure the integrity of GPS signals by using a GPS firewall to analyze signals and update threat information	
Improve the resiliency of GPS systems by using inertial references and alternative PNT sources	
Provide visibility to system operators by quickly identifying and reporting on GPS anomalies	

Thank you!

Microsemi, a wholly owned subsidiary of Microchip Technology Inc. (Nasdaq: MCHP), offers a comprehensive portfolio of semiconductor and system solutions for aerospace & defense, communications, data center and industrial markets. Products include high-performance and radiation-hardened analog mixed-signal integrated circuits, FPGAs, SoCs and ASICs; power management products; timing and synchronization devices and precise time solutions, setting the world's standard for time; voice processing devices; RF solutions; discrete components; enterprise storage and communication solutions, security technologies and scalable anti-tamper products; Ethernet solutions; Power-over-Ethernet ICs and midspans; as well as custom design capabilities and services. Learn more at www.microsemi.com.

Microsemi Headquarters
One Enterprise, Aliso Viejo, CA 92656 USA
Within the USA: +1 (800) 713-4113
Outside the USA: +1 (949) 380-6100
Sales: +1 (949) 380-6136
Fax: +1 (949) 215-4996
email: sales.support@microsemi.com
www.microsemi.com

Microsemi makes no warranty, representation, or guarantee regarding the information contained herein or the suitability of its products and services for any particular purpose, nor does Microsemi assume any liability whatsoever arising out of the application or use of any product or circuit. The products sold hereunder and any other products sold by Microsemi have been subject to limited testing and should not be used in conjunction with mission-critical equipment or applications. Any performance specifications are believed to be reliable but are not verified, and Buyer must conduct and complete all performance and other testing of the products, alone and together with, or installed in, any end-products. Buyer shall not rely on any data and performance specifications or parameters provided by Microsemi. It is the Buyer's responsibility to independently determine suitability of any products and to test and verify the same. The information provided by Microsemi hereunder is provided "as is, where is" and with all faults, and the entire risk associated with such information is entirely with the Buyer. Microsemi does not grant, explicitly or implicitly, to any party any patent rights, licenses, or any other IP rights, whether with regard to such information itself or anything described by such information. Information provided in this document is proprietary to Microsemi, and Microsemi reserves the right to make any changes to the information in this document or to any products and services at any time without notice.