Precision Time and Network Synchronization for the Telecommunications Industry

WSTS May 7, 2026

The opinions contained herein are solely those of this author and nothing should be inferred about the likelihood of the threats described

Irwin Gerszberg AT&T Fellow, Distinguished Inventive Scientist

irwin@att.com 732 -310-6303

AT&T

Irwin Gerszberg

Office: (732) 615-5059 Mobile: (732) 310-6303 Email: irwin@att.com

Irwin Gerszberg AT&T Fellow and Distinguished Inventive Scientist for AT&T Labs in Middletown, NJ. He is responsible for Advanced RF Research technologies on Department of Defense 5G mobility projects, AT&T network resilience, research on new low-cost novel methods to help protect critical infrastructure against nuclear and other electromagnetic threats, solar flares/geomagnetic threats, network timing synchronization threats from GPS jamming and manipulation. He holds a bachelor's degree and a master's in computer science from the New Jersey Institute of Technology and Stevens Institute of Technology. He joined AT&T Bell Labs in 1978 where he spearheaded AT&T's first speech response/voice recognition system. After joining AT&T Labs Wireless unit, he was responsible for the development of numerous advanced wireless technologies and services. Over the years Irwin has made key fundamental contributions to Science and Technology in Digital Subscriber Line, voice over DSL, IP based cable telephony, broadband wireless, broadband over powerline, microcells, satellite, fixed wireless, high-definition Voice, IP telephony, and a vast array of emerging broadband infrastructure initiatives.

He holds an amazing record, 682 patents with the United States Patent Office on advanced technologies covering a vast array of wireless, wired, and emerging broadband technologies. In 2001 Irwin received AT&T's Science and Technology medal. In 2002, Irwin was inducted into the New Jersey Inventors Hall of Fame by the Governor of the State of New Jersey for his innovations and contributions to science and technology in the telecommunications industry. In 2004, Irwin was awarded AT&T's highest honor: The AT&T Fellow Award for his long-term career in pioneering contributions and innovations for the telecommunications industry. In 2014 he led a research team that invented Project AirGig™ which is a technology that enabled Gigabit data transmission on existing electric utility power lines around the globe. In 2019 he built and still runs today, the AT&T Science and Technology Innovation Center in Middletown NJ which houses 150 years of the telecom industry innovations that changed the world and tells the history of innovation from the Alexander Graham Bell telephone to todays modern day infrastructure.

Cellular Service Disrupters – Jamming and Spoofing

Car parked across the street from an MTSO for 3 days with a low power GPS manipulation transmitter can cause major havoc!

Sophisticated GPS manipulation threats, no alarms generated as there is a valid GPS signal

GPS L1 Jammer

$30

GPS jammers available for purchase on the internet

GPS L1, L2, L3, L4,L5 Jammer

$469

GPS L1, L2 Jammer $179

GPS Spoofing HW/ SW Kits

GPS Long Range L1-L5 Jammer

$10,000

Frequency Bands
GPS, GALILEO, GLONASS, BEIDOU

GPS L1
GPS L2
GPS L3
GPS L4
GPS L5

AT&T

GPS Timing Jamming/Manipulation Occurring Globally

Many parts of the world GPS signals are jammed or manipulated on a daily basis, and can't be relied upon

GPS interference occurs due to various factors such as electromagnetic radiation from nearby electronic devices, intentional jamming, atmospheric conditions, and solar activity.

3-30-24 GPS disruptions in the East Mediterranean Sea

3-19-24 Cypress - Continuous GPS alarms 5G base stations.

3-11-24 Poland reports of GPS jamming

3-6-24 East Africa GPS Disruptions

2-23-24 South China Sea loss of GPS

2-14-24 GPS down for 3 hours

2-9-24 South China Sea GPS interference/manipulation

2-7-24 90 min. GPS outage Columbus Ohio

1-27-24 East Africa GPS disruptions

1-23-24 Mediterranean Sea GPS disruptions

1-19-24 Yemen and Saudia Arabia GPS manipulation

1-18-24 Haifa Israel seaport GPS disruptions and manipulation

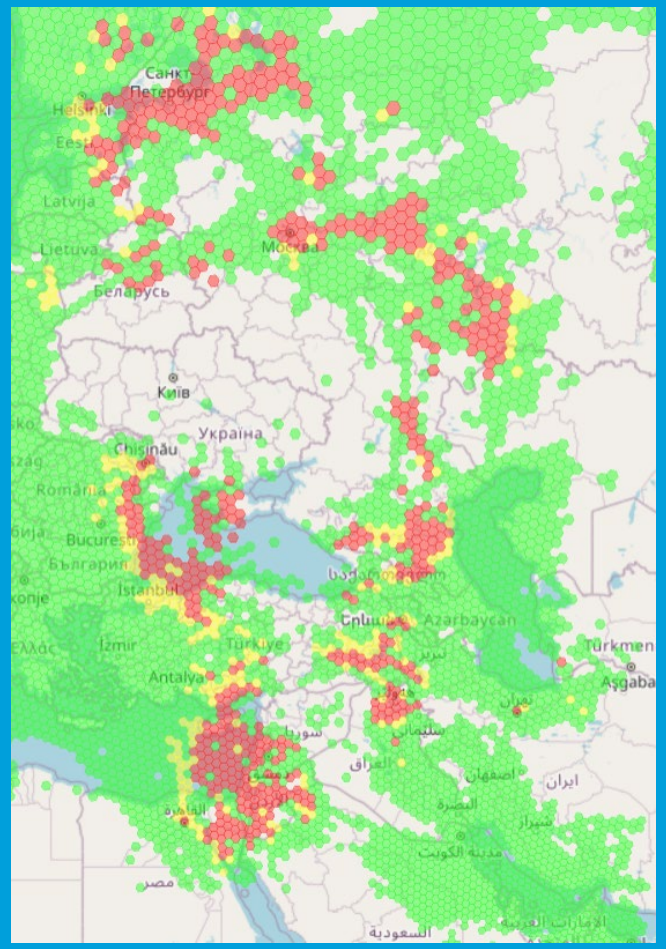
1-14-24 Ocean City, NJ GPS disruption

12-16-23 Middle East GPS outages

4-22-24 Thousands of British flights reported GPS jamming near Baltic region

Addressing GPS Timing Jamming/Manipulation/Interference

1) Most of Europe now uses network-based Precision Time Protocol (PTP) services due to the risk of GPS jamming and spoofing within their countries.
2) Many countries have even gone a step further and have deployed time scale systems, their own references.
3) Some US carriers replacing with network based PTP timing services in all application, due to the concerns with GPS
4) Some companies use both L1, L2 and L5 frequencies along with multiple sources like GPS and Galileo for redundancy with PTP.



GPS Jamming Map, June 10, 2024

gpsjam.org

AT&T

Challenging GPS Antenna Location

The impact of non-ideal antenna location includes reflections, multipath, line of sight blockage and both intentional and unintentional jamming

We need lock on 4 satellites 24x7
GPS typically will have 5 satellites visible
GALILEO typically will have 5 satellites visible
Newer GPS receivers with simultaneous operation provide access to satellites simultaneously.
3 frequency bands L1, L2 and L5 which enhance performance and resists jamming

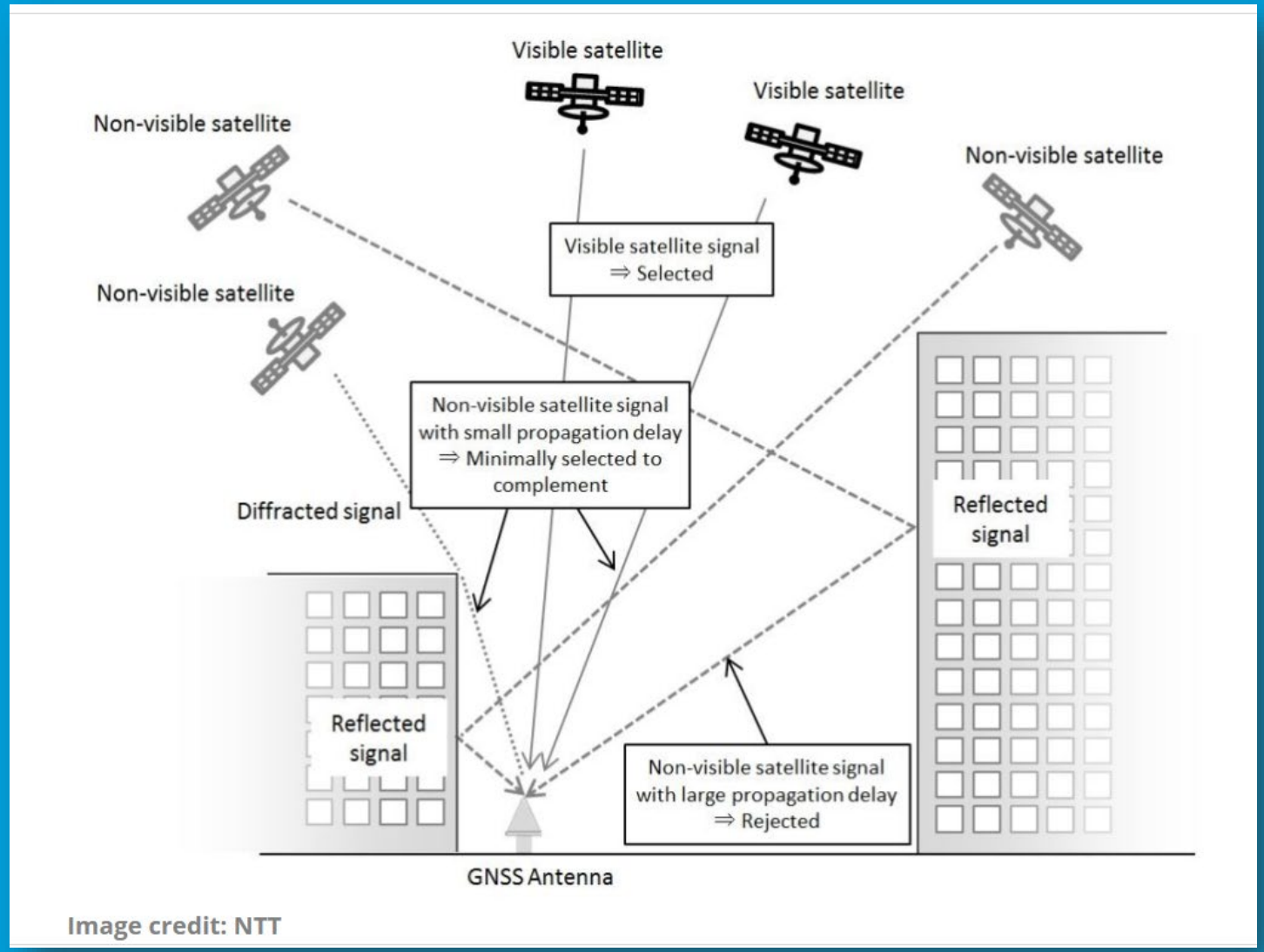
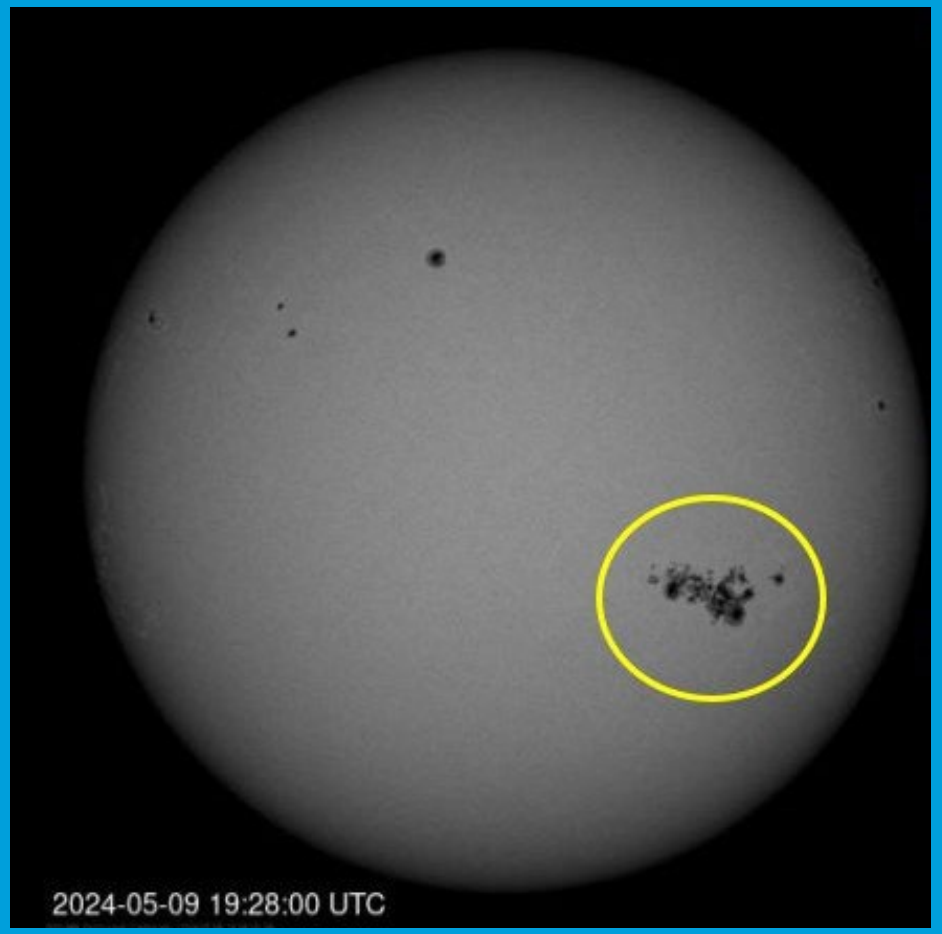


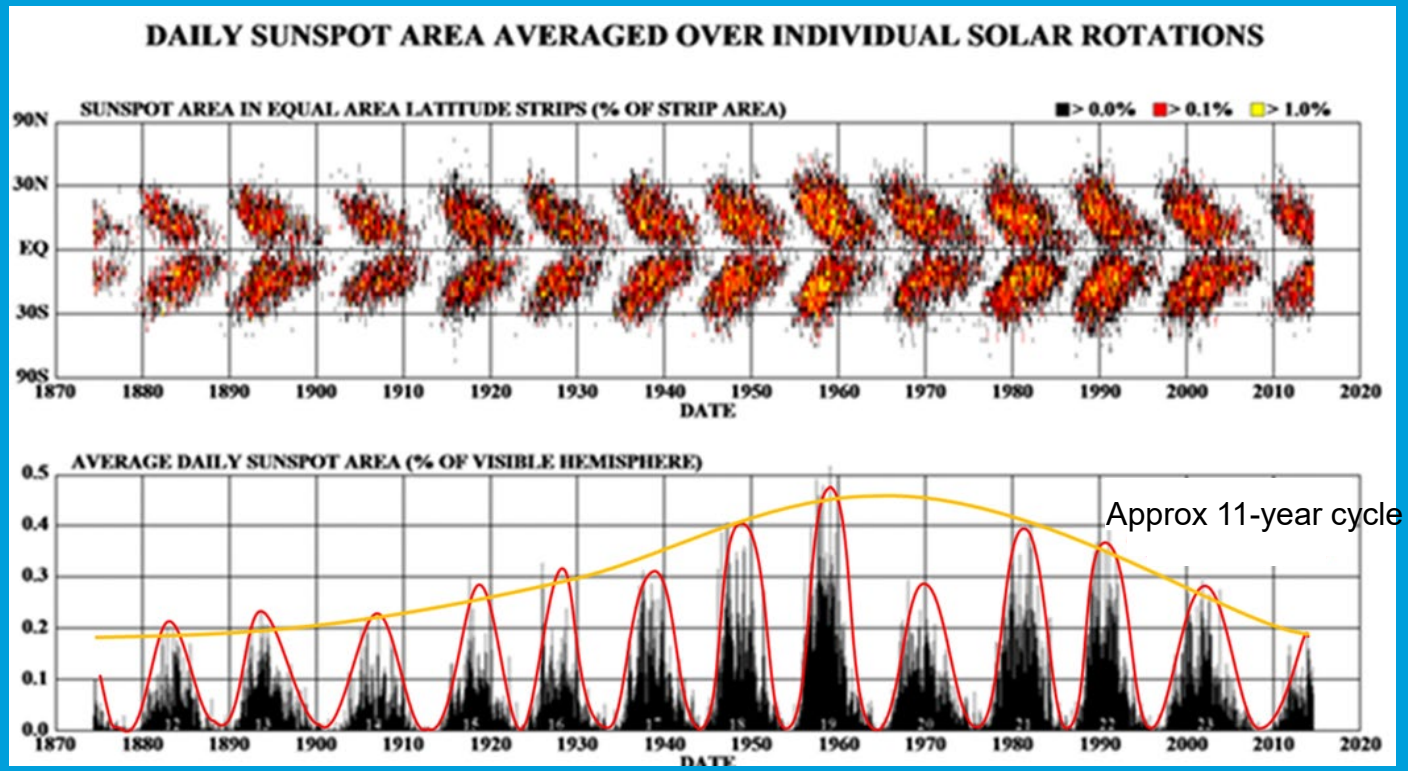
Image credit: NTT

AT&T

Solar Cycles and Patterns

Our bright sun that gives us life also has a dark side





The sun is a ball of super-hot plasma, roughly 890,000 miles across; a million Earths would fit within its volume. At the Sun's core is an ongoing fusion reaction that has been continuously converting 5 million tons of hydrogen to helium, every second, for the last 4.51 billion years

GPS Denied Environment Design Compliance Goals

- Do not depend on GPS or Galileo as a sole timing source
- Be able to withstand attacks from hostile jamming and spoofing
- Use resilient fiber network architectures with backup paths
- Be able to withstand long term GNSS outages (weeks, months, years)
- Deploy networks of cesium atomic clocks (for holdover) as they don’t depend on GNSS
- Use network synchronization from multiple sources via Fiber if available
- Never use hostile nation GNSS constellations

Telecom Network Timing Synchronization is Critical

GPS Jamming, Interference or Manipulation - Loss of MTSO and Cell Site Network Timing

Estimated Potential Effects of Complete Network Synchronization Loss

- 30-60 Minute Timing Loss: C-Band and mmWave **complete outage**, handsets continue to use Sub 6GHz FDD Bands only
- 3-4 Hour Timing Loss: FDD NR Radios **complete outage** FDD LTE Radios continue to operate normally
- 72 Hour Timing Loss: FDD LTE **performance degradation**, some features may not be available
- Very Powerful Solar Storms cause long term GPS timing drift, networks can go out of spec effecting RAN customer performance
- Short duration GPS outages are normal, occur from: heavy rain, or even birds on the GPS antenna
- Handsets can rely up GNSS for accurate location data during 911 emergency calls

Severe Space Weather Threats

5G timing requirement is 1,500 nanoseconds to UTC, however there are time budget allocations for 5G.

For network-based timing services using PTP you allocate 1,000 nanoseconds to the network time error budget

The end device/application, (BBU or radio) is allocated 400 nanoseconds.

The GPS timing receiver is allocated 100 nanoseconds of the total budget.

The GPS receiver drifting outside the 100 nanoseconds can be problematic when you are using Precision Timing Protocol as the primary or the backup.

PTP - Precision Timing protocol

Even 100 Feet of GNSS Spoofing can cause problems

1 ns timing = 11.8 inches (speed of light or free space propagation)

10 ns = 118 inches or 9.8 ft location distance error

100ns = 98 ft location distance error

A 98 ft error in location for a 911 call might be tolerable, but disastrous for network synchronization

ATIS Develop Standards and Best Practices Protecting against Position Navigation Timing and New Emerging Related Infrastructure Threats

Technical Report on resilient timing plans for critical infrastructure operators

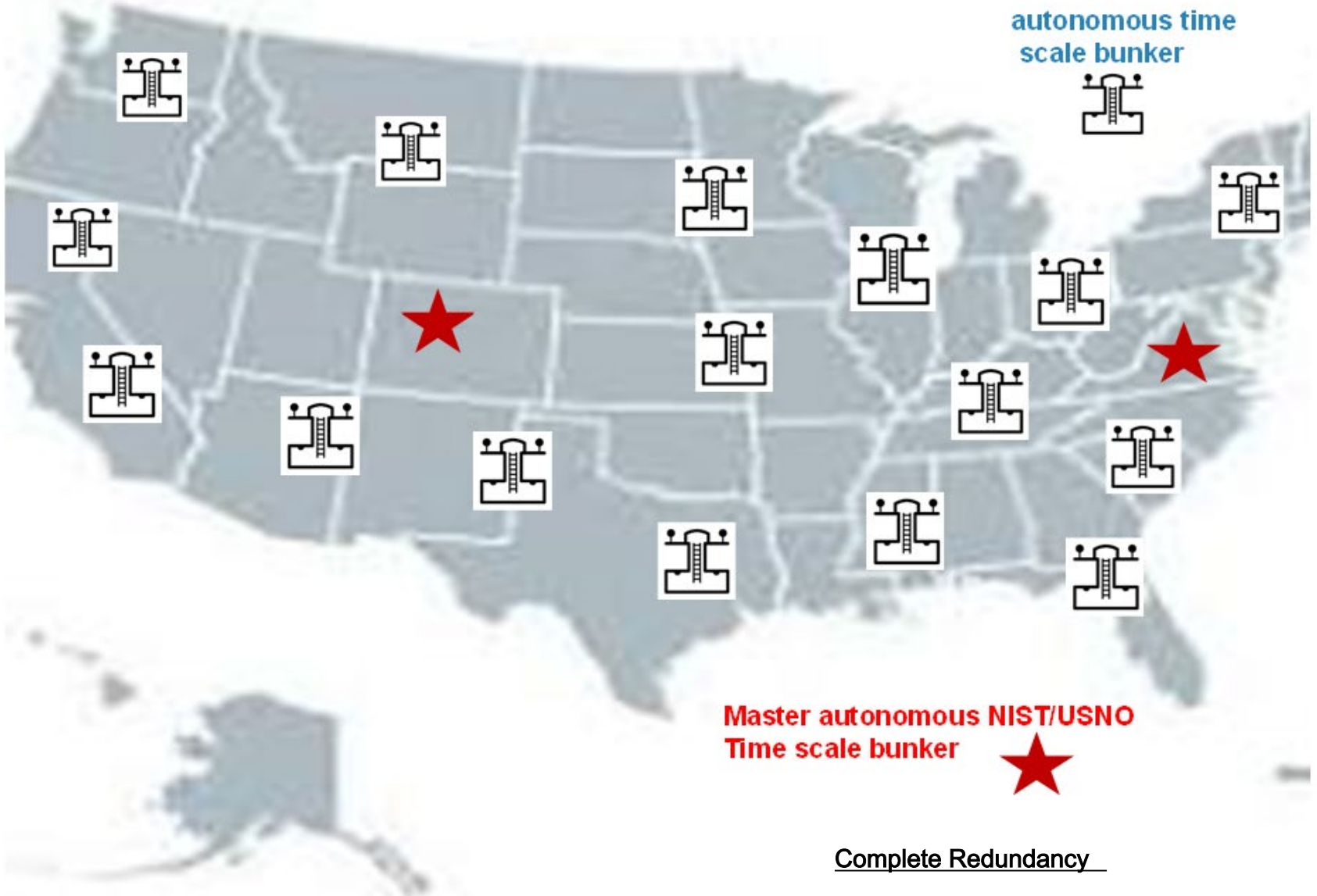
ATIS SYNC-2025-00014

Suggested Critical Infrastructure Target Architecture

Call to Action → ATIS Develop Standards and Best Practices for the Following:

Step 1 -> ATIS Best Practices/ Reference Architecture

1) Telco Critical infrastructure should maintain long term synchronization centrally when primary GNSS is unavailable or when GNSS signal manipulation has been detected.
2) Redundant Pairs of Grandmaster Clocks each with Multi-band/multi-constellation GPS antenna/receiver GPS + GALILEO, GPS Manipulation Detection, plus other non GNSS signals of opportunity
3) Cesium atomic clocks deployed to provide holdover when UTC traceable references are not available. In addition, Government atomic clock interconnections using Two Way Time Transfer (TWTT modems) over resilient dedicated Fiber paths are recommended.



System of autonomous time-scale bunkers

Complete Redundancy

Each Time Scale Bunker Connects to both Master Time Scale Locations

AT&T

Long Term Outage Protection with Autonomous Time Scales

Master autonomous NIST/USNO Time scale bunker

TWTT modems
Example: White Rabbit

autonomous time scale bunker

TWTT modem

PTP or TWTT modem

Fiber

GNSS + Other

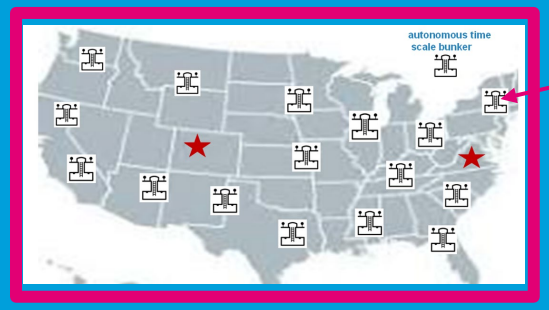
Major Hubs
ePRTC
Dozens

TWTT modem

PTP or TWTT modem

Fiber

autonomous time scale bunker



PRTC

MTSO & CO's
Hundreds

PRTC

Endpoints
100,000+

NIST – National Institute of Standard and Technology

USNO – US Naval Observatory

TWTT - Two-way time transfer

AT&T

Additional Threats to Telecom Network Timing/Synchronization

Solar, HEMP, Directed Energy Pulse Weapons, EMP

Sustainability in Telecom: Energy and Protection (STEP) Committee
ATIS Standard ATIS-0600320

Nationwide Wide Scale Network Threats

Solar Threat

HEMP Upper Atmosphere Threat

Localized Network Threats

Directed Energy Pulse Weapons

EMP Threat

AT&T

Proposed New ATIS Approach for Non-Military Critical Infrastructure

Use existing buildings as is, with minor updates “Re-Start vs Harden to Mil Standard” - revolutionary low cost effective approach

Military standard Mil-Std-188-125-1A does not allow any interruption or downtime in equipment function, but ***commercial and industrial critical infrastructure is not operating in battlefield conditions***, so the design objective of this approach is to enable commercial networks to survive an electromagnetic attack without damage but with very short-term disruption being acceptable.

In simple terms, the goal is to enable an operator to “get knocked down, get up, dust itself off, and immediately get its network up and running automatic” with minimal downtime at reasonable cost via SW auto network re-start.

Protect Networks only to a level that prevents physical equipment damage

ATIS EMP Standard / Best Practices currently being updated based upon technological advancements in shielding & a novel approach to reduce costs:

1) Create new Telecom standard, 40db vs 80db (MIL Spec) building isolation over time via: nano particle paint, fabrics, ceiling/roofing. Work with Government for measuring and verification of new low-cost building materials.
2) Standards based HW watchdog timers on all network elements to perform controlled Re-Start function
3) Standards based alternate Network bldg re-routing architectures for physical building diversity.
4) Create New EMI standards for vendor equipment chipsets (RF, Transport, Switching, Fiber, Devices, etc)

Rather than solve the problem only via HW shielding, employ a novel SW technique at far lower cost to achieve similar results.