ATIS Briefing – March 21, 2017

Economic Critical Infrastructure and its Dependence on GPS.

Briefing question:
If it's critical, then why isn't it uniformly monitored to detect bad actor jamming and spoofing activities?

PRESENTED BY PATRICK DIAMOND, PRINCIPAL, DIAMOND CONSULTING
SUPPORTED BY ATIS MEMBER COMTECH TELECOMMUNICATIONS CORP.

DHS recently identified these 13 economic areas as Critical Infrastructure

- Space Applications
- Precision Agriculture
- Surveying & Mapping
- Power Grids
- Air Traffic Control
- Petroleum Industry
- Supply Chains
- Transit Operations
- Shipping & Maritime Applications
- Financial Markets
- Emergency Services
- Industrial Control
- Telecom

The phrase “Critical Infrastructure” has many connotations. Today’s briefing will consider this in the context of its economic criticality.

- We won’t discuss in detail atomic clocks, satellite operations, IEEE 1588 or any other mechanism for network transfer of time.
- We will ask the question, “If these economic segments are truly critical why aren’t they monitored?”
- We will discuss an idea for monitoring these critical infrastructure applications using an out of band and non-intrusive technique.
- We will discuss the 1 pulse per second signal derived from GPS.
- It is noted 1pps is used to create the paper time scale UTC, Universally Coordinated Time: it’s used to synchronize frequency and phase of radio’s in mobile wireless networks, it’s used in power grids to align synchro-phasers and many more critical application-specific needs for time and phase.
- It is assumed the geographic diameter of a jamming or spoofing event is approximately 10 miles.

How do we rationally segregate economical Critical Infrastructure segments?

- What is characteristically unique about the economic Critical Infrastructure segments?
  - Air Traffic Control, Space Applications, Transportation Infrastructure and Emergency Services are primarily within the government domain.
  - The remaining Infrastructure segments are almost exclusively within the public commercial/industrial domain.
- They all take advantage of the same free GPS signals, using generally the same equipment.
- With the highly diverse application performance needs, disjointed operation, different ownership and control systems, how could these end points be uniformly and effectively monitored?

The only common characteristic of these Critical Infrastructure endpoints is 1pps.

- While the 1pps signal is used differently, it is commonly presented at each end point.
  - The critical component of this signal is the extreme precision of the period between 1pps signals with the "time" or "phase" alignment capability of less than 1µS.
- This deterministic periodicity has enabled highly disparate geographic locations to be synchronized in "phase" and/or "time".
- In a jamming or spoofing action, this precise period between 1pps signals is corrupted.
- Can this corruption be uniformly measured and monitored to detect a bad actor attack? *I believe it can!*

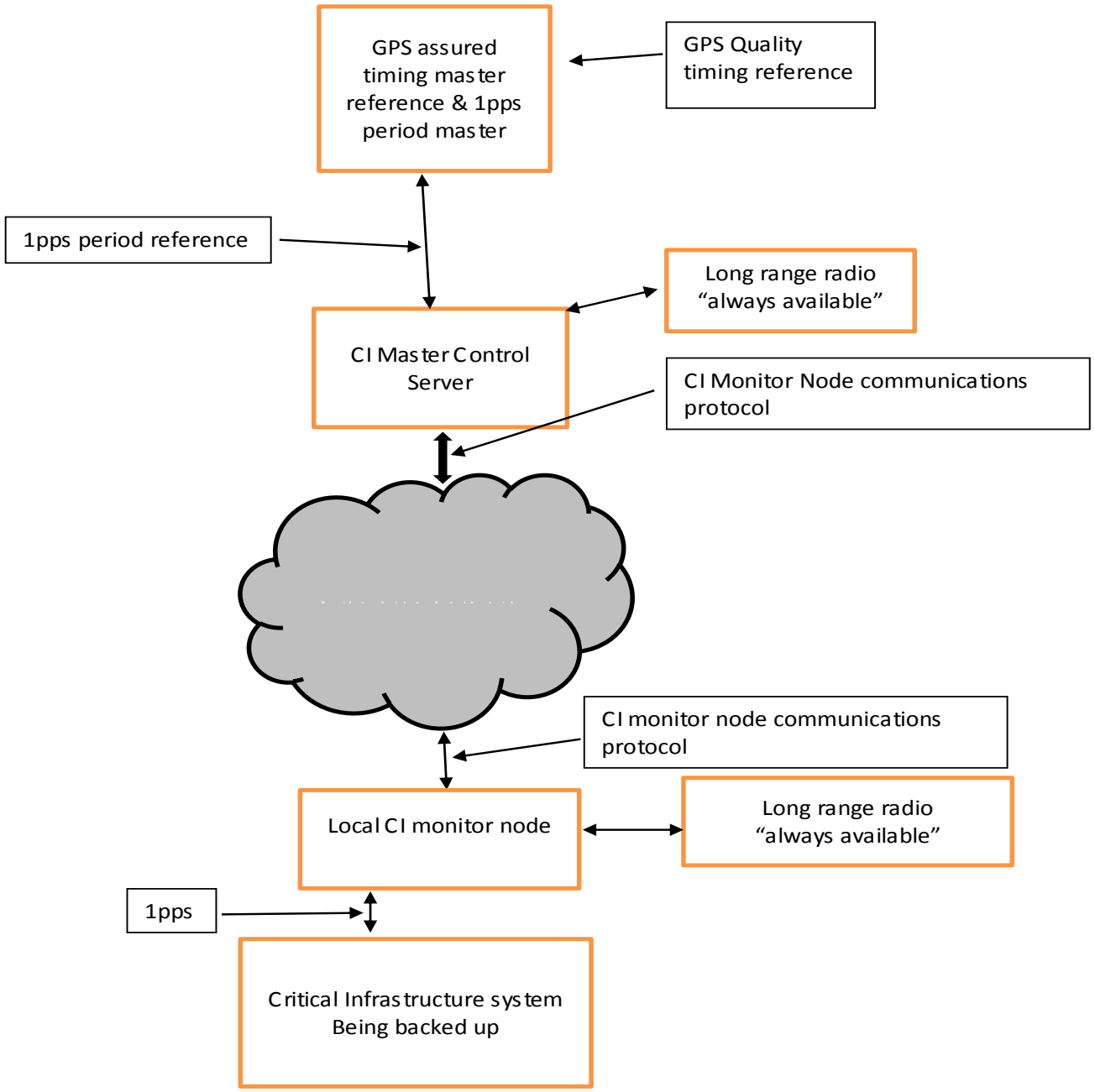
1pps is an electrical signal when output from GPS Receivers.

- The 1pps signal is not of specific interest here, but rather the period between them. This period is the fundamental value used by economic Critical Infrastructure applications.
- This 1pps signal is in the frequency domain, and the period between them is in the time domain. Here we care about the time domain.
- A well-known method of measuring time domain intervals is using time stamps. This is basically a period counter that logs the "counts" between frequency events, producing a numeric representation of this period. The best known method for producing, measuring and managing these period counts is found in IEEE 1588: Precision Time Protocol.

What if it were possible to correlate the periods between 1pps signals on a wide scale?

- I will discuss such a capability in clearly understandable detail.
- This methodology is currently in a theoretic state; however, numerous experts in the time synchronization industry have peer reviewed the theory and agree it is viable.
- The individual elements of this technique are well understood and off the shelf.
- In-use techniques for capture and transfer of time periods are borrowed and implemented.
- Time synchronization algorithms are not implemented.

Critical Infrastructure 1pps Monitoring System Block Diagram



What is the principal operational characteristic of the CI 1pps period monitoring methodology?

- The ultimate goal of the monitoring system is to detect when a UUT is being jammed or spoofed.
  - This detection process will measure the "rate of change" of the period samples.
- The technique is to collect 1pps period samples from the target community of CI end points. Samples from each end point will be continuously collected at ~1 second intervals.
  - These samples will be mathematically combined to compute the standard deviation rate of change across the entire community.
  - This computed standard deviation rate of change will be compared to an assured 1pps measured period.
  - A modified form of the Kalman linear quadratic estimation method will process the samples for outliers from the standard deviation value. These outliers will be considered as potential jamming or spoofing candidates.

What is the performance goal of the CI 1pps monitoring methodology?

- The phase and time performance targets for the economic Critical Infrastructure applications are quite diverse. It is important to keep in mind the reason for this monitoring and detection technique is to locate CI end points under jamming or spoofing attack.
  - The 1pps time period change detection threshold target is 1µS from the computed standard deviation value.
    - This 1µS change could occur from sample to sample, which more than likely would indicate a jamming event, or potentially a receiver failure.
    - The 1µS change could be an accumulated value occurring over several samples which could indicate a spoofing event. In this case it is reasonable to increase the sample rate to compute a pattern of change and establish an early potential fault flag of this end point.
- Real-time comparison of the computed deviation to an assured 1pps period value will eliminate erroneous results.

What is the system architecture for CI 1pps period monitoring methodology, server?

- The heart of the system is a series of high performance commercial grade cloud servers with open system OS and virtual machine capability.
  - Co-located with each server is an assured GPS system with long term holdover, greater than 72hrs. Each server would be backed up by 2 other servers. The period sample database for each would be constantly mirrored to the backups.
  - It is estimated each server could simultaneously support 1500 CI end points.
  - The computation applications would be written in the Python programming language to assure portability to other open OS systems.
  - Code obfuscation techniques would be employed to prevent bad actor hacking.
  - Typical data transfer packet size estimated at 64 bytes.

What is the system architecture for CI 1pps period monitoring methodology, CI node?

- Each CI end point would have a CI monitoring node to measure the 1pps signal period and produce a 64-bit time stamp with 4nS granularity.
- Each CI monitoring node would have 2 mechanisms for transfer of period time stamps to servers.
  - The there are 3 transfer technology candidates.
    - Wide area packet ethernet for those CI locations with backhaul connectivity.
    - IoT 50Kbs Unlicensed band radio for all locations, for building penetration to inbuilding systems and alternate route for backhaul failure.
    - NB-LTE for outdoor CI locations without backhaul connectivity.

What is the reporting method for CI 1pps period monitoring?

- The objective for this system is to monitor and detect jamming and spoofing events regardless of the CI end point.
  - In order for this to be accomplished, the CI stakeholders need to have an incentive to participate in the program.
  - This universal monitoring can be accomplished through creating a location database of each CI end point being monitored.
  - The benefit to each CI stakeholder is a uniform method of notification of jamming and spoofing attacks in real time, to include the locations being attacked.
  - The benefit to the DHS is immediate notice of the physical locations jamming and spoofing attacks are occluding in real time.
  - All participants would have secure gateway access to the servers monitoring their CI end points.
- The open system architecture offers a near unlimited set of context syntax for easy integration into stakeholders current monitor and control systems.

What is the objective for today's CI 1pps period monitoring system briefing?

- It is understood this is a new and unique idea for monitoring and detecting of GPS CI jamming and spoofing attacks.
  - The genesis of this idea is a universal recognition of GPS CI end points' vulnerability to jamming and spoofing attacks.
  - The motivation for this idea sharing is a common need amongst vulnerable CI stakeholders both government and commercial.
  - The pretext of the system design is non-intrusive to the CI systems and an out of band secure method of monitoring and detecting attacks.
- Our goal today is to stimulate the CI stakeholder community to in-depth topical discussion on this idea and any others these discussions may spawn.

Thank you for taking the time to listen to this presentation. Hopefully it stimulated thought on Critical Infrastructure vulnerability protection techniques.

We look forward to your comments.

Sponsored by

For more information, contact Sameer Vuyyuru
Sameer.Vuyyuru@comtechtel.com