Best Practices for Improved Robustness of Time and Frequency Sources in Fixed Locations

6 January 2015

This paper is intended as a best practices guide used by those responsible for installing and maintaining time and frequency sources (TFS) in fixed infrastructure locations for Time & Frequency (T&F) operations. Systems that must maintain time and frequency within strict accuracy limits often use Global Positioning System (GPS) receivers as sources of time and time interval. Although GPS has many attributes, there may be times where the radio frequency environment causes degraded or lost GPS signal reception. There are ways to install and operate GPS receivers, along with other timing sources, that enhance the assurance of T&F operations. This paper provides an initial discussion of these best practices. Some best practices associated with other sources of time and frequency are also listed.

In general, a TFS should be routinely monitored to ensure proper operation. This can be done locally by the system operators and/or remotely at system operations centers. Local monitoring should be performed and documented in accordance with preventative maintenance schedules. If a TFS is remotely monitored, maintenance information should be recorded for future reference.

GPS users should report service degradations, disruptions, other incidents or anomalies to the U.S. Coast Guard Navigation Center at 703-313-5900 or visit http://www.navcen.uscg.gov/?pageName=gpsUserInput to submit a report online.

==========

1. GPS-based TFS

For a GPS-based TFS, ensure the following are monitored:

- Any faults, alarms, warnings should result in appropriate response.
- Operational mode (fixed, survey, mobile, etc.). If in fixed mode, then log and determine cause of any computed position changes.
- GPS receiver self-survey position (latitude, longitude, height)
- Note system used for receiver height either Mean Sea Level (MSL) or ellipsoid height.

1.1 GPS Receiver Initialization

Considerations: GPS timing users should be aware that many GPS-based time control and frequency control techniques provide signals that are not usable at their specified accuracies for many hours during initialization (calibration). High-precision timing outputs may require as many as 12 hours for output accuracy to settle to appropriate levels before reliable and accurate T&F data is provided.

Additionally, if a disciplined local oscillator is used, e.g., Rubidium, it can take several days before this backup oscillator settles to its specified characteristics.

Recommended Actions:

- Allow time for the GPS receiver to complete initialization. Refer to the GPS receiver technical manual for initialization time allowance.

- Allow time for the GPS-disciplined oscillator to stabilize. This time varies by oscillator type- consult relevant technical documentation.
- If the receiver has the capability, record average signal strength/Automatic Gain Control level once the stabilization is complete as a benchmark to be checked during routine maintenance
- Utilize the output signal once the stabilization is complete.
- Review operator's manual to ensure local oscillator has sufficient time to settle.

1.2 GPS Outage

Considerations: During a GPS outage or interference event, the TFS may continue to provide timing signals, but quality will degrade over time. When GPS signals are restored, it may take several hours before the TFS is again providing the highest levels of accuracy.

Recommended Actions:

- Monitor the Time and Frequency Distribution Unit (TFDU) for reference source switching. Ensure the Secondary Precise Time and Time Interval (PTTI) Reference Source (SRS) assumes duties as the primary reference source (PRS).
- Once outage is restored, ensure GPS reverts to PTTI PRS.
- Log details of the outage (i.e., time of occurrence, duration of outage, etc.).
- Ensure that the secondary PTTI reference source is of the same accuracy as GPS, or that the secondary source has sufficient holdover time to meet the operational needs of the installation for the expected operational scenario outages.
- Report disruption event to the U.S. Coast Guard Navigation Center as described above.

1.3 GPS Receiver Alarms

Considerations: Most GPS TFS provide some type of holdover or coasting capability during a loss of GPS signals. GPS receivers typically provide some type of visual alarm or indication that incoming GPS signals have been lost. It is extremely important that the alarms are monitored on a regular basis.

Recommended Actions:

- Monitor and respond to GPS receiver alarms/fault indications.
- If the equipment hosting the GPS receiver is network-enabled, configure to send alarm messages to the user/system operator (given the network security is acceptable for the installation). Check and record quality of signal outputs (to establish trend/baseline).
- Ensure that the GPS receiver output alarms do not adversely affect the TFS. For example, the alarms should not cause the TFS to shut down, but instead cause a switch to backup sources of T&F.

1.4 GPS Antenna Location

Considerations: A GPS receive antenna should be located so that it has a good view of the sky in all directions, avoiding obstructions of the line of sight to GPS satellites. Radio frequency (RF) interference, including co-site interference from nearby transmitting antennas, can degrade GPS performance. Blockage from buildings, terrain and/or vegetation can affect GPS reception as well. Since foliage can block or attenuate GPS

signals, an installation that works in the winter may experience problems in the spring or summer.

Recommended Actions:

- Position each antenna such that it can view as much sky as possible from horizon to horizon and is not obstructed by nearby buildings, terrain, etc..
- Locate the GPS antenna as far as possible from any transmit antennas, especially those that are not highly directional.
- Periodically reevaluate location of antennas to ensure there are no new obstructions or new sources of interference and noise sources.
- Place the antennas on the building roof with a clear view of the sky and away from RF-reflecting objects/structures that potentially produces an effect called multipath which is a common cause of degraded receiver performance.
- Choosing the antenna position in a RF challenging environments may require measurements in different locations to obtain best case receiver performance. In these circumstances, and if the receiver supports it, the installer could select the best placement by monitoring C/No (carrier to noise density ratio) messages out of the receiver to ensure the needed number of satellites-in-view and signal reception. GPS receiver tracking depends on an acceptable C/No which can vary depending on the receiver design quality. The installer should refer to the receiver manufacturer for the optimal C/No range.
- Place the antenna where it cannot be seen from publically accessible locations, or deny view of the antenna from public locations using an RF-transparent material (such as a solid plastic fence). Even better, place the antenna where a roof line or structure blocks direct line of sight to the antenna from publically accessible locations.
- Review operator's manual for required separation from other GPS antennas.

1.5 GPS Antenna Types

Considerations: Most GPS receiver systems use a simple Fixed Radiation Pattern Antenna (FRPA) that provides gain across the sky while providing some suppression of signals from out of band frequencies (i.e., frequencies not used by the GPS signals). Interfering signals (intentional or unintentional) can be received by the antenna and can degrade or deny GPS signal reception. FRPAs can cost as little as $100.

The Controlled Radiation Pattern Antenna (CRPA) is a more robust phased array antenna made up of several GPS antenna elements. When combined with antenna electronics that perform advanced signal processing, interference arriving from specific directions can be suppressed, while GPS signal reception is maintained. The use of CRPA antennas in time and frequency applications is immature, and a number of policy and technical factors need to be considered. Among the technical factors are the introduction of additional variable signal delays and phase center motion that can affect accuracy in timing applications. CRPA antennas with associated antenna electronics can cost tens of thousands of dollars.

A choke ring antenna is designed to reject multipath arriving from low elevations, including reflections from the ground. They are typically used for survey application.

They can also be used to suppress interference arriving from low elevation angles, and testing shows that some models are superior to others at such interference suppression. Choke ring antennas cost upwards of $1000.

When GPS timing receivers are at surveyed locations, they should be able to use signals from as few as one GPS satellite to provide time outputs. Often, signals from two or three GPS satellites are preferred for redundancy and better accuracy. Specialized antennas can be used that offer greater attenuation of interference arriving from low elevations than do choke ring antennas, with upward-facing beamwidths that still provide signals from several GPS satellites. These antennas can use either specialized designs like horns, or CRPAs with antenna electronics designed to form nulls at the horizon. These devices are developmental items at this time.

Recommended Actions:

- Depending on the location and site requirements, choose the most appropriate GPS antenna, in accordance with requirements. Sites should inventory available antennas and connect GPS receivers to antennas that provide better interference mitigation in accordance with mission priorities.
- Document antenna location, specifications, and characteristics.
- Conduct regular antenna maintenance in accordance with manufacturer recommendations.
- Sites should take inventory of available antennas and feed receivers from more capable antennas in accordance with mission priorities. Note that switching of antennas produces changes in the reported GPS position and timing. If the antenna, antenna location, or antenna cable length are changed, the receiver needs to be re-initialized.

1.6 GPS Antenna Cables

Considerations: GPS receivers are connected to the GPS antenna by a cable. Cables and connectors can become loose, corroded or broken and must be periodically inspected for wear and damage. Long cable length can introduce signal delays and attenuation, which must be accounted for when determining placement of an antenna. In some cases, extremely long cables and additional adaptors may cause unacceptable signal strength loss. The GPS antenna and cable are an important part of the system and should be inspected regularly for serviceability.

Recommended Actions:

- Ensure all cables are connected properly.
- Routinely inspect cables for loose, bent, kinked, or frayed wires and connectors, especially after adverse weather and outages.
- Only install manufacturer recommended antenna, cable, and receiver combinations. Cables come in 50, 75, and 300 ohm impedance versions - mixing versions will degrade the performance of a TFS. Make sure the cable’s impedance matches that of the antenna and GPS receiver.
- Cables and connections must be protected to prevent wear and tear which leads to degraded impedance matches.

- Minimize the number of adapters and splitters installed in the signal paths to minimize signal degradation.
- Verify that cable lengths of the GPS system match those prescribed in the operations manual. Any alterations or user specific cable lengths should be entered into the GPS receiver system to correct for the effect on timing accuracy.
- Calibrate delays from antenna location, cables, electronics, and other hardware in accordance with the user manual or other instructions.

1.7 Fixed and Mobile Mode Settings for GPS

Considerations: Generating an accurate estimate of time within a GPS receiver is a complex calculation derived from estimating the straight-line distance of the GPS receive antenna from the satellites and determining the position in the sky of each satellite being tracked. If the receiver is in a fixed location, changes in satellite distances are very predictable, as they are solely due to earth correlation and satellite orbital motion prescribed in its ephemeris. If the GPS receiver is moving, satellite distance estimates have to be adjusted to compensate for x, y, and z motion of the GPS receiver itself. Most GPS receiver systems have settings that can designate whether the receiver is stationary (i.e., at a fixed site) or mobile. If available, GPS receivers should be placed in the appropriate mode to match the nature of the host platform or site. This will enable the receiver to calculate the most accurate time estimate.

Recommendation:

- If available, GPS receivers should be operated in an appropriate mode to match the nature of the site (i.e. fixed for stationary sites, mobile for moving sites or platforms).
- As part of routine maintenance or system trouble shooting, the GPS system's mode should be verified. Additionally, for sites using fixed, the GPS antenna's position coordinates of the site entered into the GPS system should be verified. If there is a discrepancy, enter the correct coordinates in accordance with the operator's manual.
- The position computed by the GPS receiver should be compared against its known location continually in order to detect interference.

2. Network Time Protocol (NTP) services

While NTP does not provide the same accuracy as GPS, it may be useful for applications that do not require the accuracy of GPS. GPS can be used to set up an NTP server.

NTP is one the most essential services to maintain accurate timekeeping and clock synchronization across networks. Accurate time is critical for applications such as crypto synchronization and maintaining quality-of-service (QoS) for telephony. Therefore, proper configuration and operation of NTP servers and clients is crucial to maintain a robust network. Therefore, the following sections offer a collection of best practices intended to help assure the robustness of NTP.

2.1 NTP Version

Considerations: NTP software updates should be checked on a recurring basis to ensure any new vulnerabilities are addressed. The most current NTP software updates are located at http://www.ntp.org/downloads.html in accordance with service network policy.

Recommended Actions:

- The network manager of the TFDU should maintain a file or log of NTP software/firmware versions of each client.
- Keep NTP updated.

2.2 Authenticated NTP

Considerations: Since NTP is used to ensure accurate log file timestamp information, NTP could pose a risk if a malicious user were able to falsify NTP information. To launch an attack on the NTP infrastructure, a hacker could inject time that would be accepted by NTP clients by spoofing the IP address of a valid NTP server. To mitigate this risk, the time messages must be authenticated by the client before accepting them as a time source.

Recommended Actions:

- If possible, connect to United States Naval Observatory (USNO) or National Institute of Standards and Technology (NIST) NTP servers.
- To enhance security from threats contained within the firewall, the time server should use the access control and authentication facilities in NTP to restrict access to the service.
- If possible, only authenticated NTP packets should be accepted. The server should also accept packets from only known, approved sources.
- For communicating with the time server for status and control it is best to use a secure protocol such as Secure Shell (SSH) and/or Simple Network Management Protocol (SNMP) version 3 (encrypted SNMP). (Note: SNMP vl and v2c are not secure).

2.3 Using Multiple NTP Input Sources

Considerations: NTP is a fault-tolerant protocol that will automatically select the best of several available time sources to synchronize to. Multiple candidates can be combined to minimize any timing errors.

Recommended Actions:

- Utilize at least two or more (three or more is strongly recommended) USNO or NIST traceable NTP servers with the lowest possible stratum to minimize/eliminate timing errors.
- Include at least two reference sources for the input. Having available several time sources, NTP can select the best candidates to build its estimate of the current time. Even when a network connection is temporarily unavailable, NTP can use measurements from the past to estimate current time and error.

2.4 NTP Output Scalability

Considerations: A synchronization network may consist of several reference clocks. Each node of such a network can exchange time information either bidirectional or unidirectional. The network can be designed to propagate time from one node to another, with UTC(USNO) or UTC(NIST) reference clocks being the underlying time

source.

Recommended Actions:

- Reduce the number of stratum levels between the client and the reference source.

2.5 NTP Spoofing

Considerations: NTP is founded on the User Datagram Protocol (UDP), and is highly susceptible to IP spoofing. The NTP protocol uses UDP port 123.

Recommended Actions:

- Blocking the non-authenticated ports at the firewall is essential for network perimeter security.

2.6 NTP Server compromise

Considerations: Knowing the correct time is not only crucial for proper network functioning but also for security. Compromising an NTP server opens the door to more sophisticated attacks that include NTP poisoning, replay attacks, obfuscation/alteration of logging data, denial of service (DOS), and distributed denial of service (DDOS).

Recommended Actions:

- To provide security through separation and isolation, the NTP server should only be connected to the management network. This enables the NTP server to provide time using a more secure path to managed devices.
- Security is maximized when the time server is installed within the network firewall. The time server acquires time from the GPS, via an antenna, with no threat to network security. It then distributes the time to the clients over the network within the firewall.
- In addition, security is further enhanced if risky protocols such as FTP, Telnet, Time and Daytime can be disabled.

2.7 NTP Security Information

Considerations: NTP users are strongly urged to take immediate action to ensure that their NTP daemon is not susceptible to use in a reflected denial-of-service (DDOS) attack.

Recommended Actions:

- Reference the NTP Security Notice site for vulnerability and mitigation details, located at: http://support.ntp.org/bin/view/Main/SecurityNotice
- NTP Security related bugs, confirmed or suspected, are to be reported by email to security@ntp.org

3. Other

3.1 Cesium Clock Life Expectancy

Considerations: Cesium clocks can run out of Cesium. Cesium beam tube lifetimes vary from

5 to 12 years depending on the unit purchased. Cesium clocks require periodic calibration to maintain specified characteristics.

Recommended Actions:

- Verify with manufacturer specifications on the suggested lifetime of cesium tubes.
- Identify and log installation date and plan for replacement as it approaches end of life.
- If the vendor recommends calibration of the frequency reference(s), adhere to the recommended calibration interval.

3.2 Cesium HAZMAT

Considerations: Cesium tubes are considered hazardous material (HAZMAT).

Recommendations:

- Use proper HAZMAT procedures for shipping the Cesium tube or any assembly containing the Cesium tube to the repair or refurbishment depot.

3.3 Cesium Clock Alarms

Considerations: Cesium Clocks contain alarm and status alerts. Some of the alerts are audible while others are not. In general, the Cesium lock indicator is a great way to determine if it is operating within specifications.

Recommendations:

- Cesium Clock alarms are to be monitored on a routine basis.

3.4 Building Integrated Timing System

Considerations: If the system employs a Building Integrated Timing System (BITS) clock you should also monitor it for alarms. The BITS alarm is often a good indication of system problems.

Recommendations:

- During BITS setup, ensure that the Cesium clock is the primary frequency reference, while GPS provides the time-of-day to the system, which is locked in to the correct GPS “epoch” or second.
- The Primary Reference is often referred to as “PRI” or “Stratum-1”.
- The Rubidium oscillator should be set up as the secondary reference (“Stratum-2”) and the Ovenized Quartz (OCXO) is tertiary (“Stratum-3”).

3.5 Power Supply

Considerations: It is important to ensure that a precise TFS have a reliable and redundant source of power.

Recommendations:

- Use an Uninterruptable Power Source (UPS) to help ensure systems survive short power outages.
- Ensure personnel are trained on UPS system use and specifications.
- Test UPS regularly

- Install a UPS with the ability to hot-swap batteries in order to ensure that disciplined local oscillator does not lose discipline during extended power outages.

3.6 Battery Use

Considerations: Some systems and/or subsystems have field replaceable batteries.

Recommendations:

- Ensure to incorporate battery tests and replacement schedules as part of the preventive maintenance plan.

3.7 Regular System Monitoring

Considerations: Time and Frequency Distribution System (TFDS) require periodic monitoring to verify lack of alarm state and confirm health and status condition.

Recommendations:

- Watch standers should routinely verify that the system is operating properly.
- Log observations.

3.8 Holdover Readiness

Considerations: Verify internal holdover device is being maintained and ready to assume "time duties".

Recommendations:

- Review system technical documentation and perform regular preventative maintenance actions as required to ensure holdover devices are operationally ready and maintain quality if the reference source degrades.
- Ensure that holdover device has sufficient accuracy to meet operational needs for GPS outage scenarios. Consider installing a holdover device along with a sensor that detects interference and switches to the holdover device when needed.

3.9 Environmental Conditions

Considerations: TFDUs and subsystems are very sensitive to environmental conditions.

Recommendations:

- Review system technical documentation to determine local operating ranges.
- Monitor local environmental conditions (i.e. temperature and humidity). Log recordings to assist with trend analysis and log all out of tolerance occurrence.
- If able, contact building unit facilities prior to going out of environmental tolerances to restore HVAC services without degrading ability to provide PTTI services.

3.10 Output Database

Considerations: Each TFDU output provides PTTI data to another component or system.

Recommendations:

- Maintain list and contact information for each of TFDS output circuit (by output port).

- Establish threshold to contact customers as output quality degrades from established baseline. If possible, develop a statistical process control process to determine system degradations prior to outage.
- If possible, contact PTTI data user prior to service disruption and prior to scheduled outages.
- Prior to equipment casualty, determine circuit prioritization and restoration plan to assist "load shedding" implementation based on required accuracies and mission priority.
- Determine alternate method to provide required outputs (re-patch other TFDU system).
- Maintain user agreements that detail responsibilities.

3.11 TFS IP Connections

Considerations: Many TFS have IP (Ethernet) ports. However, TFS often are susceptible to cyber attack via these IP ports. The TFS often have traditional vulnerabilities to cyber attack; e.g., out of date and/or unpatched OS, default or no passwords. The TFS vendors rarely provide cyber patches.

Recommendations:

- Strongly consider not connecting the TFS to an IP network, especially if the OS is old.
- If the TFS is connected, as a minimum, change any default passwords and ensure that authentication of remote users is enabled.
- Check with the TFS vendor on a regular basis to see if software patches are available.