

Use of Positioning, Navigation, and Timing Services in the Sector

The Water and Wastewater Sector uses Positioning, Navigation, and Timing (PNT) services to locate physical assets, such as valves or vehicles. PNT also provides timing signals for supervisory control and data acquisition (SCADA) systems.

Accurate and synchronized time is important in SCADA systems for data logging as well as for time-based controls. For example, some water systems may use time—not a measurement of level, flow, or pressure—as the basis for:

- Filling tanks, reservoirs, or towers.
- Releasing water from peaking wells.
- Conducting filter backwashes and other operations.

Altering system time could affect those physical processes, with cascading impacts.

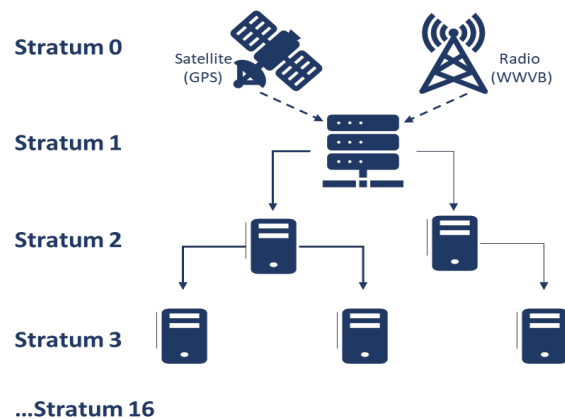
Since water utilities across the country use PNT services differently, utility managers should engage their facility operators and information technology personnel to better understand how their utility uses PNT services and to assess vulnerabilities to PNT disruption. Even if the risk to delivering core services is assessed as low, PNT disruptions may still pose challenges for a utility.

Sources of Time for SCADA Networks

Utilities use different timing sources depending on their needs for accuracy and precision. Many utilities rely on a network time server that accepts input from at least one Stratum 0 or Stratum 1 source and uses an internal “holdover” clock to maintain time synchronization if connection to external sources is lost. Examples of time sources include:

- **Global Positioning System (GPS) receivers.** GPS and other global navigation satellite systems provide highly accurate time. However, the signals are relatively weak and can be lost intermittently, jammed, or spoofed.
- **Radio broadcasts.** The National Institute of Standards and Technology (NIST) provides shortwave, low frequency, and high-frequency radio time signals synchronized to coordinated universal time (UTC) on stations WWW, WWVB, and WWVH.

- **Internet time servers.** NIST Internet Time Service provides access to Stratum 1 servers synchronized to a reference time source. The Network Time Protocol (NTP) Pool Project provides access to clusters of Stratum 1 and Stratum 2 servers. NTP also allows for selecting up to 10 specific, static time server sources from the internet. Risks of receiving time over the internet parallel cyber risks generally. Packets may be intercepted and spoofed; newly discovered vulnerabilities may be exploited; and some users and servers may not have updated to latest versions of software.
- **Internal clock(s).** Some utilities prefer to avoid risk exposure from external time sources and rely on one or more internal time sources that meet their tolerance for time accuracy, precision, and stability. Examples include rubidium oscillators and oven-controlled quartz crystal oscillators.



Strata Under the Network Time Protocol (NTP)

A “stratum level” indicates a device’s distance from a Stratum 0 reference time source, like GPS. Stratum 0 devices do not distribute time directly but provide time input to Stratum 1 servers, which distribute time to Stratum 2 clients and servers, and so on through Stratum 15. Stratum 16 devices are unsynchronized. Latency and internal device “drift” degrade timing accuracy as the stratum level increases.

Mitigating Timing Risks

Timing disruptions in utility SCADA systems may create costly regulatory and compliance issues related to data logging, or even physical consequences where time-based controls are used (e.g., overflowing tanks, broken lines, and pressure loss). To minimize risk, utilities should consider these mitigation actions:

- **Maintain ability to monitor and conduct operations “manually” when SCADA systems are unavailable.** Document, train, and exercise processes to maintain continuity of service manually, regardless of the cause of a SCADA disruption. Cross-train staff as needed to ensure sufficient personnel to sustain manual operations.
- **Incorporate timing considerations into cyber risk and vulnerability assessments.** The foundational NIST PNT Profile (see Resources) builds on the NIST cybersecurity framework. Utilities should consider timing-related risks from expanding automated operations or using virtual machines, which require synchronizing guest operating systems to a host. Utilities should also stay abreast of time coding issues such as the recurring GPS rollover or the “year 2038 problem” for 32-bit systems.
- **Use redundant time sources.** Using a variety of time source types (e.g., directly from GPS and radio, or NTP Stratum 1 servers getting time from a variety of Stratum 0 sources) reduces risk of not having accurate time inputs. Using multiple sources of the same type (e.g., multiple dispersed GPS antennas, multiple internal clocks) also reduces risk from any single component failure.
- **Limit external exposure where possible.** Determine whether and how often your system needs to synchronize time externally with each time source to maintain a desired level of accuracy.
- **Maintain general cyber hygiene.** General cybersecurity best management practices will contribute to reducing risk.

Mitigating Positioning and Navigation Risks

Loss of GPS could make it difficult for utilities to locate buried valves or other assets in an emergency. As with timing risks, utilities should prepare to “manually” locate assets in the event of GPS outages. This may involve development and maintenance of hardcopy backup maps and location inventories (“valve cards,” etc.); it should also include training and exercising manual operations. Since most utilities have limited staff bandwidth to sustain manual operations, cross-training staff to expand the pool of personnel may help.



Many water utilities use GPS to locate valves more quickly when responding to water main breaks.

Resources

- **Environmental Protection Agency Recourses:**
 - **Analyze Consequences:** [Water Health and Economic Analysis Tool](#)
 - **Assess Risks:** [Vulnerability Self-Assessment tool](#)
- **Cybersecurity and Infrastructure Security Agency (CISA):** www.cisa.gov/pnt
- **National Coordination Office (NCO) for Space-Based Positioning, Navigation, and Timing:** www.gps.gov
- **NIST:** [Foundational PNT Profile](#)

