Resilient PNT Services for Transportation

Learn About Timing for Transportation Infrastructures

The virtual Primary Reference Time Clock is an innovative architecture that delivers precise timing for transportation with reduced reliance on Global Navigation Satellite System (GNSS)-based timing signals.

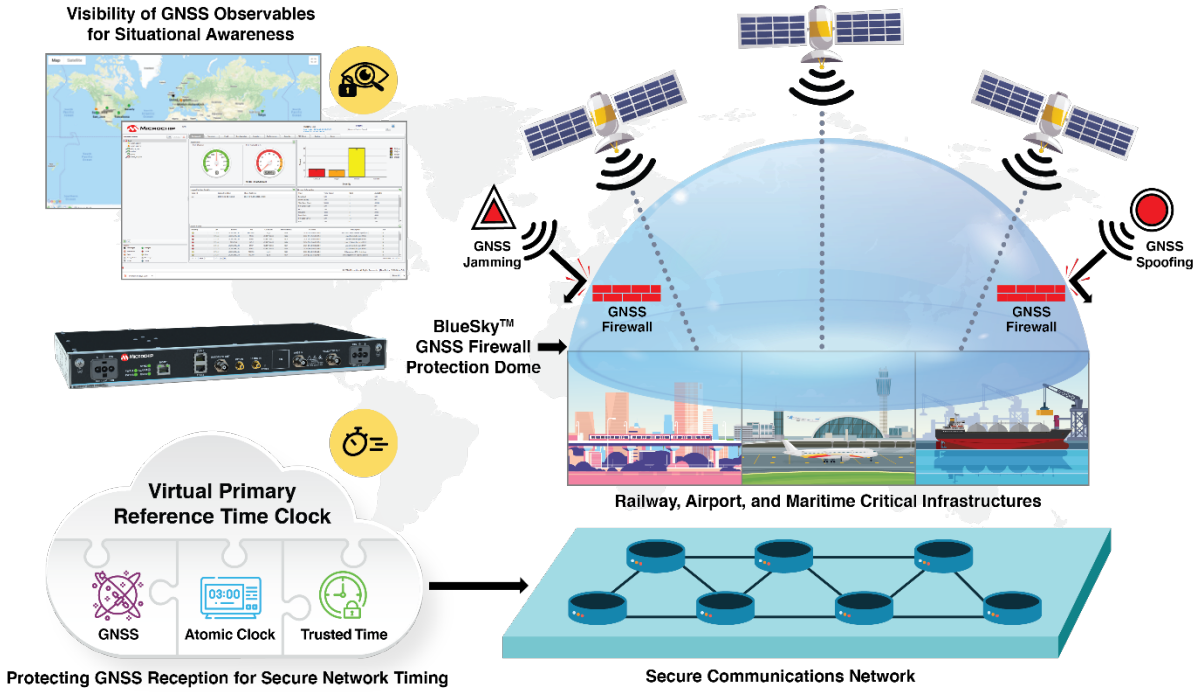
Critical infrastructure (CI) transportation—such as aviation, railway or maritime—relies on the use of Positioning, Navigation and Timing (PNT) services delivered by Global Navigation Satellite System (GNSS) for operational efficiency, reliability and, most importantly, public safety. GNSS is used for a range of airport operations including asset management and mapping vehicle movement, railways depend on GNSS for controlling a train's velocity over varying terrain and large container ships use GNSS for navigating through crowded waterways and safely docking at seaports to load, unload and track cargo.

CI transportation makes use of the full range of PNT services provided by GNSS. Because the protection and security of GNSS-delivered PNT services is a matter of public safety, CI transportation applications not only require extremely high accuracy but also security, resiliency and recoverability that can withstand any threat that can disrupt GNSS signal reception, whether intentional or unintentional.

Since the use of GNSS for position and navigation is so pervasive in CI transportation applications, it is no coincidence that spoofing threats intended to misdirect or create a false position reading are widely reported, whether on the ground, at sea or in the air. Examples include large cargo vessels at sea being guided off course as well as confirmed cases of drones being taken off course and flying in unauthorized airspace.

Learn About vPRTC Architecture | **Download GNSS Visibility White Paper** | **Watch the Webinar Replay**

Resilient PNT Services for Transportation



Protecting and securing GNSS reception begins with the ability to determine the quality of the live-sky GNSS signal. This visibility is best achieved by monitoring key GNSS observables which are used to calculate position, navigation and time. Examples of GNSS observables include tracked satellite count, RF power level, carrier-to-noise ratio and phase-time-deviation measurements. Just as a network firewall detects and protects against network attacks, a GNSS firewall delivers visibility of jamming and spoofing threats to alert transportation operations of untrusted sky-based signals.

CI transportation operators not only depend on position and navigation services delivered by GNSS, they also rely on timing services from GNSS for their secure and private network communications. These networks deliver critical voice communications and telemetry data throughout airport facilities, to train stations and rail yards and to shipmasters and port administration authorities. Networks must be built to support high-speed transport of data and high-reliability wireless communications. This must be achieved with extremely low levels of network latency and the ability to time stamp events at dispersed locations. All these requirements depend on timing services from GNSS.

Resilient PNT Services for Transportation

To support secure and private network communications, the Virtual Primary Reference Time Clock (vPRTC) is a highly secure and resilient network-based timing architecture that blends our secure GNSS firewall technology, high-precision atomic system clocks and a portfolio of trusted time solutions to meet the expanding needs of modern critical infrastructures such as those required by CI transportation.

The combination of GNSS visibility and the vPRTC architecture provides CI transportation operators with a dual-purpose solution for the use of PNT services as delivered by GNSS. It provides situational awareness about the health of GNSS reception by monitoring and evaluating key GNSS observables in real time to determine if there is risk in the use of PNT delivered by GNSS. It also offers a layer of protection that enables a more responsible use of PNT services, including greater resiliency if live-sky delivery of PNT by GNSS is disrupted, degraded, or worse, becomes unavailable. Like a network firewall, this solution creates a dome of protection that strengthens the overall use of PNT services by GNSS for CI transportation infrastructure.