Protecting Critical Infrastructure with Resilient PNT

With the new Executive Order on Resilient Positioning, Timing and Navigation (PNT), signed by President Donald J. Trump on February 12, 2020, the federal government sets an urgent priority on protecting critical infrastructure from rising threats to Global Navigation Satellite Systems (GNSS) and PNT signals.

Importantly, the order seeks to strengthen national resilience by identifying and promoting the responsible use of positioning, navigation, and timing services by the Federal Government and critical infrastructure owners and operators.

Without which, rapidly emerging threats could affect sectors such as communications, information technology, energy, transportation, financial services, govern-
ment facilities and emergency services.

**How will the PNT Executive Order protect critical infrastructure?**

The U.S. government plans to release sector-specific PNT profiles that will describe:

- Critical systems, networks and assets that depend on PNT services.
- The risks of service disruption and manipulation.
- The potential consequences such risks may have on the critical infrastructure.
- Standards, guidelines and sector-specific requirements to address the associated risks.

**What PNT technology is currently available to address these threats?**

(Discover what is resilient PNT from Orolia, a the world leader in resilient positioning, navigation and timing (PNT) solutions that improve the reliability, performance and safety of customers’ critical, remote or high-risk operations. Courtesy of Orolia.)
The rise of unintentional and deliberate GPS jamming and spoofing attacks over the past few years have led to the development of new PNT technologies, which are able to address most of the PNT vulnerabilities of critical infrastructure.

**Vulnerability Assessments**

Understanding critical infrastructure vulnerabilities and defining what would happen during PNT service disruption and manipulation are key to securing systems against attacks, and a range of testing systems are available to simulate existing or future threats like jamming and spoofing.

“PNT threats are constantly evolving,” explains Stephane Hamel, GNSS Testing and Simulation Director at Orolia, a global leader in GPS/GNSS and PNT solutions for military and commercial applications.

(Learn More. Orolia’s Assured PNT Defense Platform is an innovative turnkey solution to the threats and vulnerabilities of GPS/GNSS, ensuring military forces the continuity of trusted PNT data needed for mission success. Courtesy of Orolia.)
“It’s important to recognize that any successful PNT protection program must be built within a living process of continuous improvement to identify, defeat and anticipate new threats.”

**Protection**

Proven technologies should be used to effectively reduce the occurrence of PNT service disruption or manipulation.

Multi-frequency and/or multi-GNSS receivers reduce risk by leveraging multiple signal sources.

**Blocking antennas** can be used to reject terrestrial interference coming from the horizon, and **Controlled Radiation-Pattern Antennas** (CRPA) can reject strong directional signals in the GPS band to prevent compromised signals from entering electronic equipment.

**PNT cybersecurity measures** at the network level, coupled with...
secure time servers that are approved for use in government networks, are effective ways to prevent PNT cyber-attacks.

**Detection**

Software and hardware-based technologies are available to detect signal jamming and spoofing, providing real time alerts to effectively reduce critical infrastructure vulnerability.

Choosing the right solution involves a trade-off between the complexity of threat scenarios and the level of false alarms that can be tolerated, both of which affect the solution’s cost.

**Mitigation**

GPS threat detection can suffice to address vulnerabilities, provided that alternative PNT sources are available to take over when GPS is compromised.

Alternative PNT sources like oscillators, inertial sensors or digital maps are only effective if GPS
disruption is temporary, meaning a few minutes for navigation and positioning, and a few days for timing.

By contrast, the STL signal on the Iridium satellite network is a commercially available PNT service that is fully independent of GPS and traceable to UTC, which can be used as a backup during longer GPS outages.

Another option is in-line jamming suppression technology, which counteracts the most common GPS jammers and typically reduces their jamming range by a factor of 100 through a small piece of equipment installed between the antenna and the receiver.

What’s next?

Critical infrastructure programs now need to assess and identify risks, choose appropriate Resilient PNT technology and define an ongoing monitoring and improvement program.

The good news is that proven Resilient PNT technology is available today.

“We can’t afford to wait for a major or fatal PNT disruption to trigger action,” said Jean-Yves Courtois, CEO of Orolia.

“Key initiatives like the PNT Executive Order provide essential awareness that these threats exist, and confirm the need to respond today with proven solutions that can keep critical infrastructure running smoothly.”
Orobia's **SecureSync** time and frequency reference solutions synchronize critical military and commercial operations where failure is not an option.

- Combining precision master clock technology with exceptional configurability, **SecureSync** delivers the industry’s highest standards for extreme reliability, security, redundancy, and flexibility in a rugged, modular, cost effective form factor.