Resilient Positioning, Navigation, and Timing for Critical Infrastructure

Homeland Security
Science and Technology

THE ROLE OF POSITIONING, NAVIGATION, AND TIMING IN CRITICAL INFRASTRUCTURE

Accurate positioning, navigation, and timing (PNT) is necessary for the functioning of many critical infrastructure (CI) sectors. Precision timing is one aspect that is particularly important, with one microsecond level or better synchronization often being required by numerous infrastructure systems, such as the electric grid, communication networks, and financial institutions. Currently, the primary source of distributed and accurate timing information is through the Global Positioning System (GPS). However, GPS' space-based signals are low power and unencrypted, making them susceptible to both intentional and unintentional disruption. To address GPS vulnerabilities in CI, the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) program focuses on four areas:

- Vulnerability and Impact Assessment
- Mitigations
- Outreach and Education
- Diversifying Timing Technologies

VULNERABILITY AND IMPACT ASSESSMENT

To better understand vulnerabilities at the end-user equipment level, testing and evaluation is being conducted on an array of commercial GPS receivers used within the CI sectors. This will help characterize their behavior under various scenarios and identify key vulnerabilities. Analysis is also being performed to better understand the national impacts and consequences of timing disruptions to CI. These system-level risk and impact assessments will help prioritize mitigation efforts.

MITIGATIONS

Mitigations range from implementing best practices to developing improved, more secure hardware. Examples include improving situational awareness by developing the capability to detect and automatically alert users of jamming or spoofing events, working with equipment manufacturers to ensure newer product lines are more robust against existing threats, and developing new antenna designs optimized to minimize jamming and spoofing effects on GPS receivers.

OUTREACH AND ENGAGEMENT

A key element of this program is outreach to stakeholders to educate them on threats, vulnerabilities, impacts, and mitigations. Equipment manufacturers and CI owners and operators are a crucial part of this effort. For example, S&T led an industry working group to develop a conformance framework that defines levels of security and resilience for timing equipment, which is in the process of becoming a standard.

Most CI sectors rely heavily on GPS to provide PNT information

DIVERSIFYING TIMING TECHNOLOGIES

In addition to mitigation capabilities, S&T is assessing complementary timing technologies to reduce reliance on a single system (e.g., GPS). This effort is driven by National Security Presidential Directive-39 (NSPD-39) of 2004. Alternative timing technologies will not only provide new sources of robust timing data, but will also hamper jamming and spoofing attempts, as having complementary timing sources enables comparison and validation of timing data.

THE FUTURE OF RESILIENT PNT

Executive Order 13905, Strengthening National Resilience through Responsible Use of PNT Services, promotes the responsible use of PNT services by the federal government and CI owners and operators. S&T and the Cybersecurity and Infrastructure Security Agency (CISA) will strive to make PNT an integral part of the overall risk analysis process.

PARTNERS, STAKEHOLDERS, PERFORMERS

Partners include other DHS components and federal agencies. Stakeholders include GPS equipment manufacturers, PNT technology providers, CI owners and operators, industry groups, and federal civilian agencies. Performers include the HSSEDI™ FFRDC.

Contact Us: GPS4Critical-Infrastructure@hq.dhs.gov