DHS Science and Technology Directorate

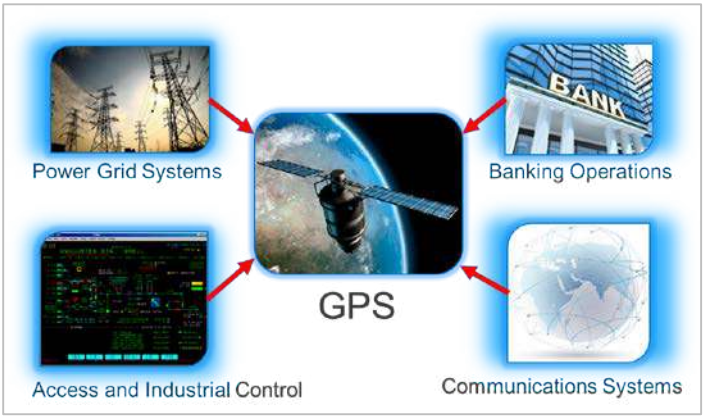
GPS Vulnerabilities for Critical Infrastructure

GPS's Role in Critical Infrastructure

Accurate position, navigation and timing (PNT) is necessary for the functioning of many critical infrastructure 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's space-based signals are low-power and unencrypted, making them susceptible to both intentional and unintentional disruption.

To address GPS vulnerabilities in critical infrastructure, this program focuses on four areas:

- Vulnerability and Impact Assessment;
- Mitigations;
- Outreach and Education; and
- Complementary Timing Technologies.



Most critical infrastructure sectors rely heavily on GPS to provide position, navigation, and timing information.

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 critical infrastructure sectors. This will help characterize the GPS receivers' 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 critical infrastructure. 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. This part of the program focuses on several different types of mitigations. 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 to existing threats, and developing new antenna designs optimized to minimize jamming and spoofing effects on GPS receivers.

Outreach and Education

A key element of this program is outreach to a number of different stakeholders to educate them on threats, vulnerabilities, impacts, and mitigations. The equipment manufacturers are a key part of this effort—test results will be used to engage and inform manufacturers on the need for more secure and robust equipment. Critical infrastructure owners and operators are also key stakeholders to educate on the current and evolving threats, best practices, and mitigations.

Complementary Timing Technologies

In addition to mitigation capabilities, complementary timing technologies will be developed to reduce reliance on a single system (GPS). This effort is driven by National Security Presidential Directive-39 (NSPD-39) of 2004, which mandates the development of alternate PNT capabilities to augment GPS.

Alternate timing technologies will not only provide new sources of robust timing data, but they will also hamper jamming and spoofing attempts, as having complementary timing sources enables comparison and validation of timing data.

Homeland Security
Science and Technology

To learn more about this program, contact Sarah Mahmood, Program Manager, at SandTFRG@hq.dhs.gov.

2016-04-13