



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-11-025-01—FEDERAL AVIATION ADMINISTRATION GPS TESTING

January 25, 2011

OVERVIEW

The US Federal Aviation Administration (FAA) has issued two flight advisories identifying planned Global Positioning System (GPS) temporary outages and the affected areas, due Department of Defense testing. During testing, the GPS signal may be unreliable or unavailable. ICS-CERT is issuing this advisory as a follow up to yesterday's alert^a to notify industrial control systems (ICS) owners and operators whose control systems employ GPS for timing reference or positioning data of possible intermittent GPS service during the testing.

FAA ADVISORIES FOR GPS TESTING

CHLK GPS 11-06

Location: Porterville, CA^b Date: January 16 through January 23, 2011.

Duration: This test has been completed.

CSFTL GPS 11-01

Location: Brunswick, GA^c Dates: January 20 through February 11, 2011;
February 15 through February 22, 2011.

Duration: Multiple test events, with each test active for 45 minutes followed by 15 minutes of off time.

IMPACT

During testing, "GPS will be unreliable and may be unavailable within a circle having a radius of 370NM and centered at 304906N/0802811W or the location known as 105.25 degrees and 52.1 NM from the SSI VOR at FL400; decreasing in area with a decrease in altitude to a circle with a radius of 325NM at FL250; a circle with a radius of 260NM at 10,000FT MSL and a circle with a radius of 215NM at 4,000FT AGL." See Figure 1.

^a http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-11-024-01.pdf

^b FAA, "Flight Advisory GPS Testing CHLK GPS 11-06 January 16–23, 2011, Porterville, CA," http://www.faasafety.gov/files/notices/2011/Jan/Flight_advisory_porterville_GPS.pdf, accessed January 24, 2011.

^c FAA, "Flight Advisory GPS Testing CSFTL GPS 11-01 January 20–February 11, 2011, and February 15–22, 2011, Brunswick, GA," http://www.faasafety.gov/files/notices/2011/Jan/GPS_Flight_Advisory_CSFTL11-01_Rel.pdf, accessed January 24, 2011.



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

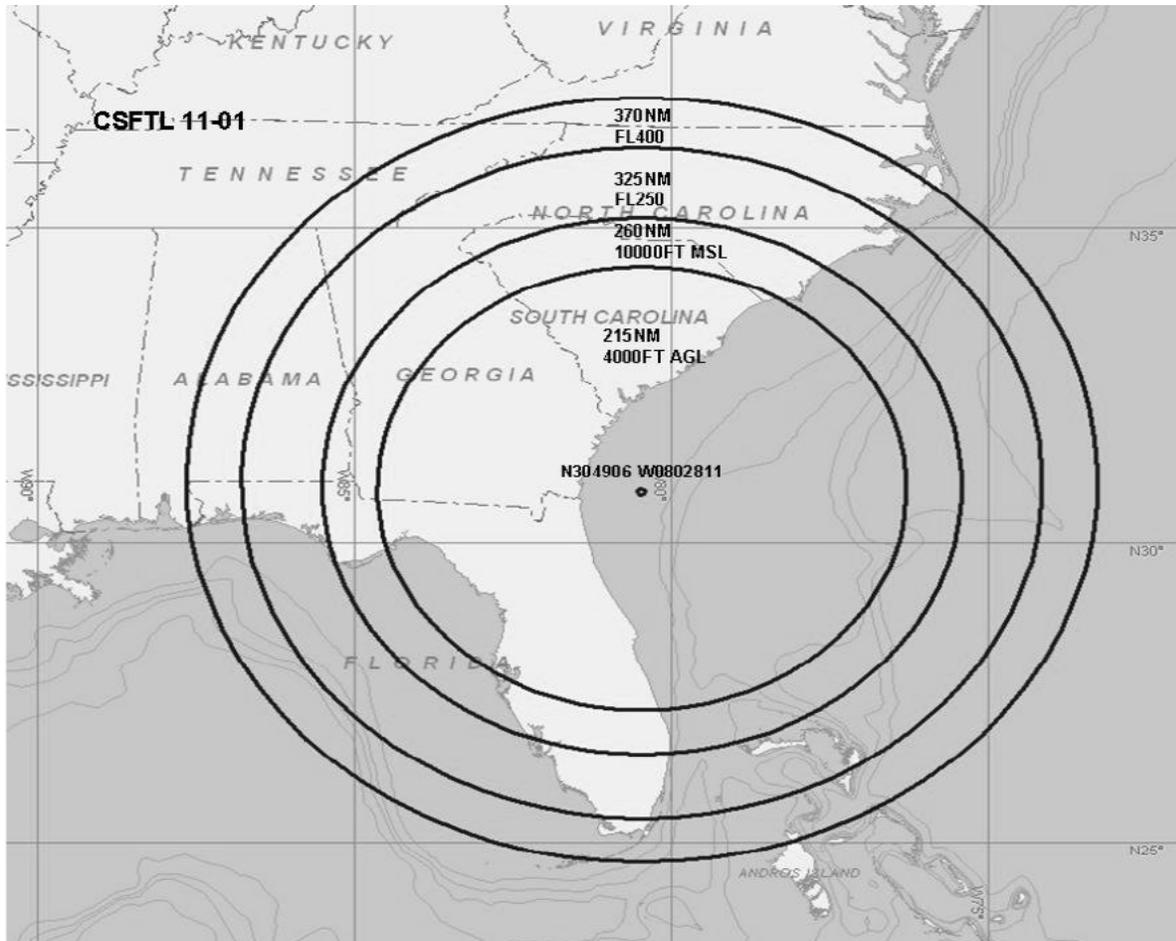


Figure 1. FAA GPS Testing Impact Map.

The ICS-CERT contacted the FAA for detailed information on the potential impact area. According to the information provided by the FAA, the effective impact range decreases significantly with decreasing altitude and the impact radius at or near ground level (sea level) will be about 20 miles. That radius precludes significant impact to land-based control systems.

The potential impact at sea level is limited to any marine systems in the area. The ICS-CERT recommends that marine owners and operators should prepare for possible GPS service disruptions in that area. The ICS-CERT recommends that marine system operators contact the Coast Guard for assistance or more information. Contact the US Coast Guard (local notices for mariners) at: 703-313-5800.

ICS-CERT recommends that organizations evaluate the impact of this GPS testing based on their environment, architecture, and GPS implementation.



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

BACKGROUND

GPS is widely used in control system environments, particularly as a timing reference signal for cellular based remote terminal units (RTUs), for intelligent electronic devices (IEDs) used in the energy sector, and for position detection in railroad positive train control (PTC) applications.

The loss of the GPS timing reference for cellular base control systems for extended periods could have significant impact on the integrity of data passed to the supervisory control and data acquisition (SCADA) system from the affected RTUs or IEDs.

Rail systems that employ GPS for PTC applications generally have backup position detection systems. Therefore, while the extended loss of the GPS position signal would reduce the precision of the system's position detection, it should not significantly impact rail operations.

MITIGATION

In the short term, ICS owners and operators can do little to mitigate a GPS jamming (interference) situation.

Equipment with jam-to-noise ratio detection that provides notification of interference would allow control systems to switch to alternate timing methods for the duration of the interference. Cellular equipment can be adapted to provide interference detection, but is not currently widely available for control system applications.^d

Long term, ICS owners and operators of control systems that are reliant on GPS timing signals (i.e., cellular RTUs, IEDs) should consider including integrated backup timing systems to accommodate the temporary loss of GPS due to interference or actual failure.

Organizations should follow their established internal procedures if any suspected malicious activity is observed and report the findings to ICS-CERT for tracking and correlation against other incidents. ICS-CERT reminds organizations that proper impact analysis and risk assessment should be performed prior to taking defensive measures.

ICS-CERT CONTACT

For any questions related to this report, please contact ICS-CERT at:

E-mail: ics-cert@dhs.gov

Toll Free: 1-877-776-7585

For Control System Security Program Information and Incident Reporting: www.ics-cert.org

d. Logan, Scott; J911: Fast Jammer Detection | GPS World, November 1, 2010, <http://www.gpsworld.com/wireless/infrastructure/j911-fast-jammer-detection-10720>, accessed January 25, 2011



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

DOCUMENT FAQ

What is an ICS-CERT Advisory? An ICS-CERT Advisory is intended to provide awareness or solicit feedback from critical infrastructure owners and operators concerning ongoing cyber events or activity with the potential to impact critical infrastructure computing networks.