Vulnerability Assessment of the Infrastructure that Relies on the Global Positioning System (GPS)

13th ITS World Congress and Exhibition

9 October 2006

Michael E. Shaw
Director, National Coordination Office for Space-Based Positioning, Navigation, and Timing

Overview

- Background/Factors
- Findings/Recommendations
- Spectrum Protection

Background

- The Global Positioning System (GPS) provides worldwide navigation, positioning, and timing services
  - Ever increasing applications across multiple critical infrastructures, both nationally and internationally
- There is a growing awareness of the safety and economic risks associated with loss or degradation of the signals
- Public policy must ensure safety and economic viability are maintained, even in the event of loss of GPS service

Background (cont'd)

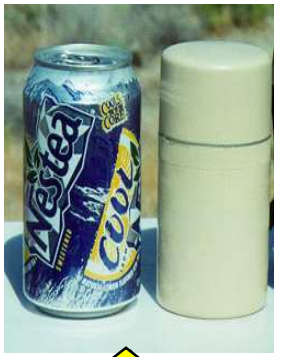
- 1998 - National Policy on Critical Infrastructure (PDD-63) tasked a GPS Vulnerability Study
  - To examine the potential impact of loss of GPS service
    - Safety, operational, environmental, and economic
- 1999 - Department of Transportation initiated the study of potential vulnerabilities of GPS
  - Covered all modes of transportation, telecommunications, banking, and commerce
  - Focused on critical applications
  - Completed through Volpe National Transportation Center

Factors of GPS Vulnerability

- Unintentional interference
  - Radio Frequency Interference (RFI)
  - GPS testing
  - Ionospheric; solar max
  - Spectrum congestion

- Intentional interference
  - Jamming – denial of use
  - Spoofing – counterfeit signals
  - System damage
    - GPS constellation, ground control segment

Noise Jammer



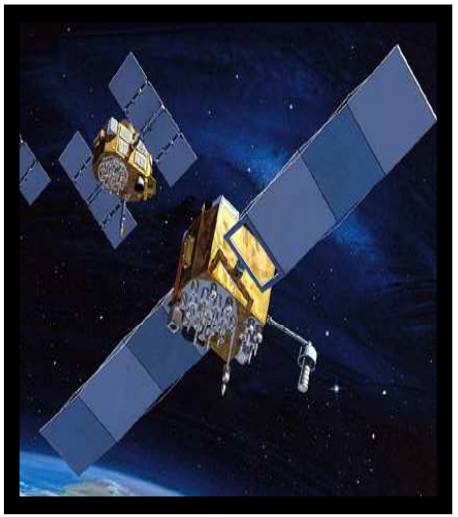
1 Watt Jammer

- Inherent vulnerabilities in all systems that use radiofrequency spectrum

Factors of GPS Vulnerability (cont'd)

- Unique GPS characteristics
  - Very low signal power
  - Currently a single civil frequency
  - Known signal structure
- Growing use of GPS encourage a disruption industry
  - Jamming techniques well known
  - Devices available, or easily built
- Spectrum competition from non-radionavigation systems
- Human factors
  - Errors, over-reliance, lack of knowledge/training

Consequences of Loss/Degradation of GPS



- Situation dependent on …
  - Transportation mode involved
  - Duration of loss/degradation
- Impact of loss can be
  - Minimal - Quick recovery
  - Operational - Reduced effectiveness and efficiency
  - Safety - *Potential* for loss of life, environmental, economic damage, or security risk
- Timing and synchronization
  - Timing linked to transportation, commerce, and banking
  - Outage can disrupt communications/networks

Vulnerability Assessement

- September 10, 2001 – Released Volpe Report on "A *Vulnerability Assessment of the Transportation Infrastructure Relying on the GPS*"
  - GPS users are subject to signal loss or degradation
  - Awareness and planning can mitigate worst vulnerabilities
  - Impossible to mitigate all vulnerabilities
  - 16 recommendations
- 2002 – Secretary of Transportation formally accepted the Report and approved an action plan

Key Findings

- GPS is subject to radiofrequency interference
- GPS augmentations (e.g., WAAS, NDGPS) improve performance, but
  - Will not mitigate the loss of the basic GPS signal
- Use of GPS-based timing synchronization must be assessed, as well as navigation and positioning
- GPS will become an increasingly attractive target as applications proliferate

Recommendations

Vulnerability Mitigation

- Ensure adequate backup systems
- Continue GPS modernization
- Continue spectrum protection
- Enhance interference location capabilities

GPS Receiver Enhancement

- Certify safety-critical GPS receivers
- Develop GPS receiver standards
- Facilitate transfer of DoD anti-jam technology

Risk Awareness

- Emphasize education programs
- Conduct public outreach
- Send letters to industry, state/local Transportation Departments
- Work with GPS Industry Council

Future Direction

- Intermodal radionavigation capabilities assessment
- Make decision on the future of Loran-C
- Develop Federal Radionavigation Plan Roadmap

2005 Federal Radionavigation Plan (FRP)

- Official USG source of radionavigation policy and planning
  - Enable safe transportation and encourage commerce
  - Prepared by Depts of Transportation, Defense, and Homeland Security
- USG policy "not to rely on single system for positioning, navigation, and timing (PNT) for critical applications"
- USG will maintain sufficient backup capabilities to meet:
  - Growing national, homeland, and economic security requirements
  - Civil transportation requirements (i.e. safety-of-life applications)
  - Commercial and scientific demands
- Backups to GPS and other critical applications may be other systems, operational procedures, or combination of both

Current Transportation Backups

Mode	Applications	Backup
Aviation	• Precision Approach • Non-Precision Approach	Traditional Ground-Based Navigation, Procedures
Maritime	• Harbor and Harbor Approach • Constricted Waterways	Conventional Navigation Methods
Land	• Tracking Radioactive Items • Collision Notification	Conventional Procedures, Dead-Reckoning, etc.
Positioning	• Surveying and Geodesy	Optical and Inertial Systems
Timing	• Communications, Power Grids, etc.	Loran-C, WAAS, Clocks

Additional Considerations

- New GNSS signals will improve resistance to interference
  - GPS L5 and Galileo signals/services
  - GPS-Galileo interoperability/compatibility
- But…Galileo is not robust backup to GPS; nor GPS for Galileo
  - Never totally eliminate threat of interference
- Must determine minimum level of backup capability
  - Recognizing budgets are constrained
    - Acceptable from safety and economic impact points of view
    - Consider a “fail soft” versus “equivalent” backup capability
  - Acquiring an “insurance policy” that may never be used

Spectrum Protection

- Protect spectrum for GNSS (GPS, Galileo, etc) and other current/future critical systems from interference
  - Degradation harms wide variety of plans and programs
  - Ultra Wideband, Mobile Satellite Venture, etc.
- Focus areas:
  - Equitable spectrum management and coordination
  - U.S. National Spectrum Management legislation
  - Galileo cooperation for compatibility and interoperability
- Requires vigilance and early action on emerging issues
  - World Radio Conference 2007 rapidly approaching

Conclusion

- GPS and future GNSS systems, like Galileo, will provide ever-growing benefits across many infrastructures
- However, GNSS systems are subject to interference, and other disruptions that can have harmful consequences
- Adequate independent backup systems and/or procedures are in place and must be maintained for critical applications in the future
- Public policy must set the framework to ensure that safety and economic viability are maintained, even with a loss of GNSS service

Contact Information

Michael E. Shaw, Director

National Coordination Office for Space-Based PNT

Herbert C. Hoover Bldg., Rm. 6822

1401 Constitution Avenue, NW

Washington, D.C. 20230

Ph: (202) 482-5809

Fax: (202) 482-4429

michael.shaw@PNT.gov

Presentation and additional information available:

PNT.gov