U.S. DOT/Volpe Center

Vulnerability Assessment

of the Transportation Infrastructure Relying on GPS

DOT/OST Outreach Meeting

October 5th, 2001

Dr. James V. Carroll

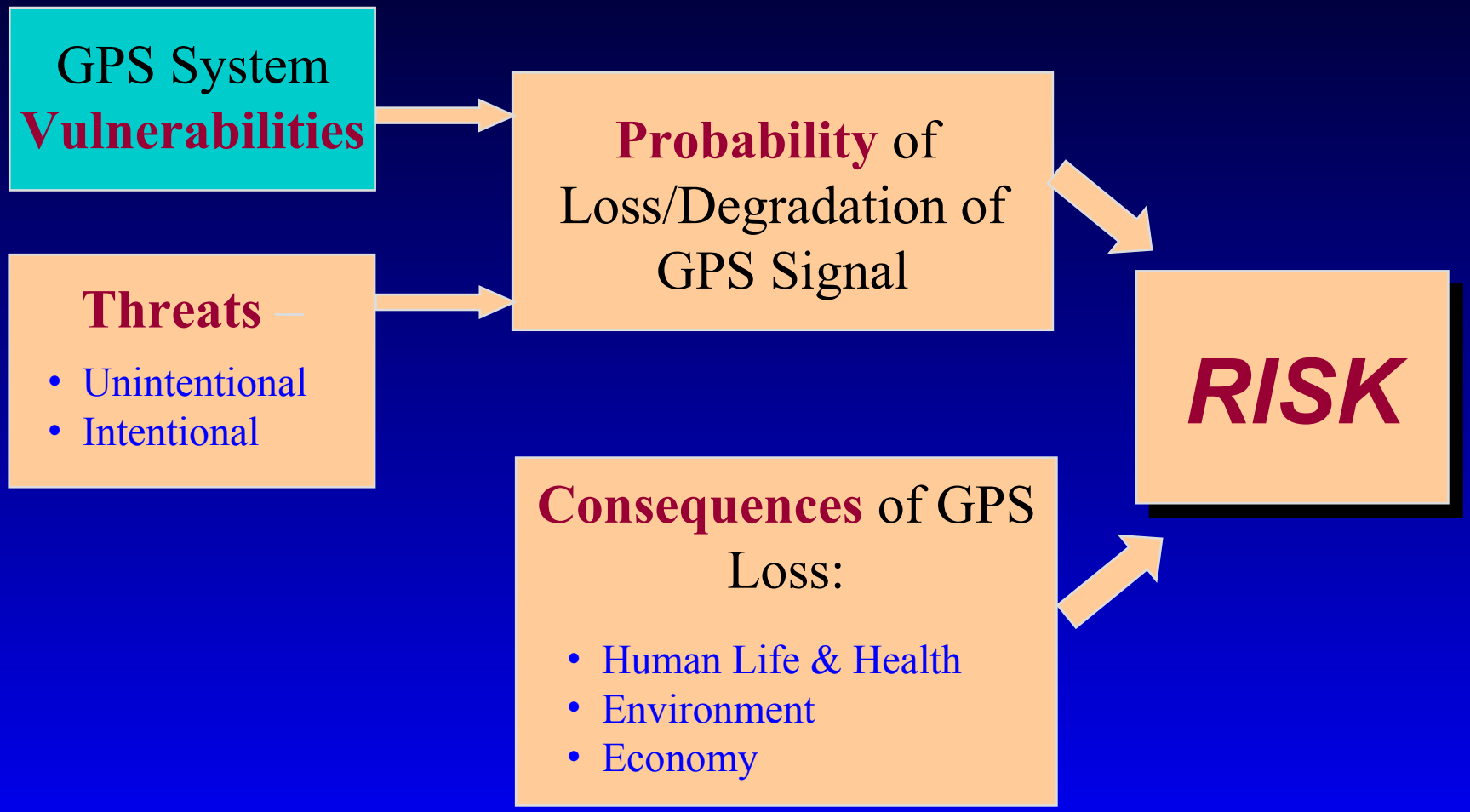
Briefing Outline

- **Overview**
- **Risk, Vulnerabilities & Disruption Mechanisms**
- **Mitigating Vulnerabilities**
- **Findings & Recommendations**
- **Summary**
- **Conclusion**

Assessment Overview

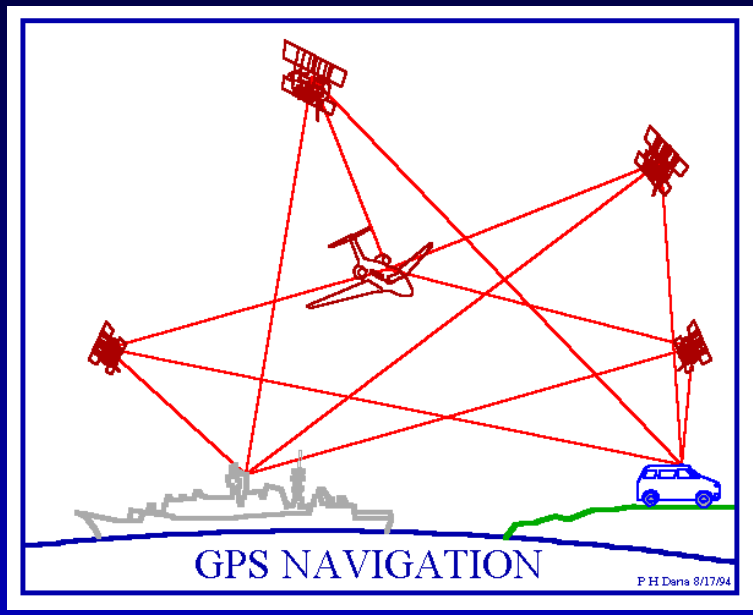
- **Report Assessed Possible Impact to Civilian Users**
  - **GPS-Based Systems in the United States**
  - **Projected Over 10 Years**
- **Covered All Transportation Modes**
  - **Also Telecommunications, Banking, Commerce**
- **This Briefing ••**
  - **Examines Vulnerabilities**
  - **Recommends Mitigations**
- **BOTTOM LINE:**
  - **GPS Users are Vulnerable to Signal Loss or Degradation**
  - **Awareness & Planning Can Mitigate the Worst Vulnerabilities**
  - **The Vulnerability Will Not be Fully Eliminated**

Risk Considerations



Civil Transportation Uses

- **Aviation**
  - **Navigation, ATC, Surface Guidance**
- **Maritime**
  - **Harbor, Inland Waterway**
  - **Traffic Service**
- **Surface**
  - **Railroads**
  - **Intelligent Transportation Systems**
- **Transportation Infrastructure**
  - **Timing; Communication Networks; Power Grids**



Timing & Synchronization Uses

- **Global Fiber Networks**
  - **SDH, SONET**
- **Global Wireless Networks**
  - **PCS, GSM, TDMA, CDMA**
- **Transportation & Public Safety**
  - **National Airspace System (VDL, NEXCOM, UAT)**
  - **Land, Rail, Marine**
- **GPS Features:**
  - **Low Cost, High Reliability & Performance**
  - **Big Asset for Synchronization of Digital Networks**
  - **GPS (and Cesium, Loran-C) - Stratum 1**

Factors Impacting GPS Vulnerability

- Very Low Signal Power
- Single Civil Frequency
  - Known Signal Structure
- Spectrum Competition
- Worldwide Military Applications Drive a GPS Disruption Industry
  - Jamming Techniques are Well Known
  - Devices Available, or Can be Built Easily

GPS Timing for EW

GPS System Vulnerabilities

- Unintentional Interference
  - Radio Frequency Interference (RFI)
  - GPS Testing
  - Ionospheric; Solar Max
  - Spectrum Congestion
- Intentional Interference
  - Jamming
  - Spoofing – Counterfeit Signals
  - System Damage
- Human Factors
  - User Equipment & GPS SV Design Errors
  - Over-Reliance
  - Lack of Knowledge/Training

1 Watt Jammer

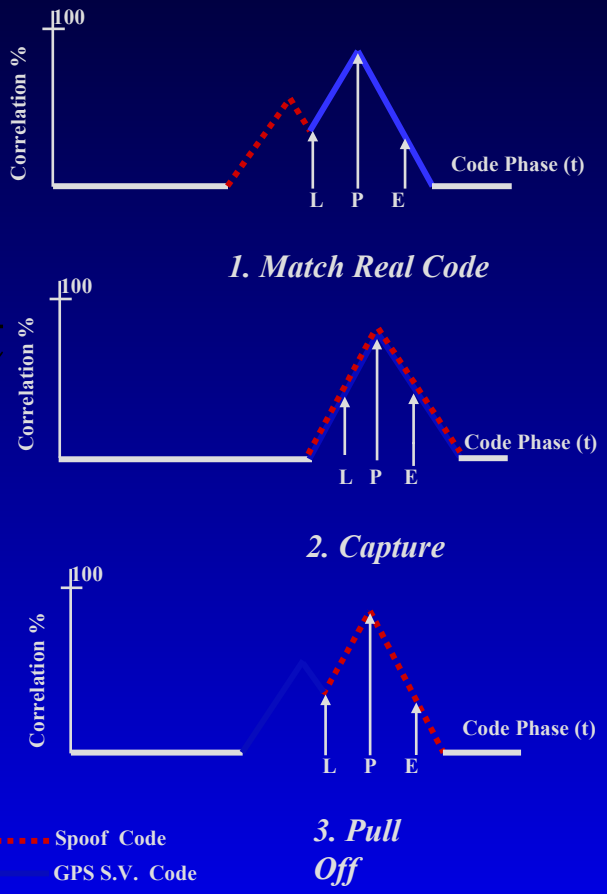
Disruption Mechanisms - Jamming

- **Jamming Power Required at GPS Antenna**
  - **On order of a Picowatt (10^{-12} watt)**
- **Many Jammer Models Exist**
  - **Watt to MWatt Output – Worldwide Militaries**
  - **Lower Power (<100 watts); "Hams" Can Make**
- **Jamming Signal Types**
  - **Narrowband**
  - **Broadband**
  - **Spread Spectrum - PRN Modulation**

Russian Jammer

Disruption Mechanisms - Spoofing/Meaconing

- Spoof – Counterfeit GPS Signal
  - C/A Code Short and Well Known
  - Widely Available Signal Generators
- Meaconing – Delay & Rebroadcast
  - Applicability of EW Components
- Possible Effects
  - Long Range Jamming
  - Injection of Misleading PVT Information
- No "Off-the-Shelf" Mitigation



Successful Spoof

Consequences of GPS Loss/Degradation

- **Depending on …**
  - **Transportation Mode Involved**
  - **Duration of GPS Loss/Degradation**
- **Impact Can Be**
  - **Minimal** - **Quick Recovery**
  - **Operational** - **Reduced Effectiveness & Efficiency**
  - **Safety** - **Potential Loss of Life, Environmental, Economic Damage**
- **Timing & Synchronization**
  - **GPS Outage Can Disrupt Communications/Networks**

Impact of GPS Loss on Timing Applications

- **Long-Term Outage (~ 2 or More Weeks)**
  - **Possible Severe Damage**
- **Shorter-Term Outages**
  - **With Planning - Manageable**
- **Many Timing Services are Involved:**
  - **E-911**
  - **GSM Wireless**
  - **CDMA Wireless**
  - **Tele-Medicine**
  - **Digital Video, Teleconferencing**

Mitigating GPS System Vulnerabilities

- **For Unintentional Disruptions -**
  - **GPS Spectrum Protection Efforts**
  - **GPS Modernization**
- **For Intentional Disruptions -**
  - **Military Anti-Jam Technology**
  - **Characterize Civil Spoof Effects\Observables**
- **Vulnerability Cannot Be Fully Eliminated**

Mitigation of User Risk

- **Implement Appropriate Mitigation Strategies**
  - For Each Individual Mode, Choose or Maintain Appropriate Backup System or Procedure
  - Be Cognizant of Timing Applications
  - Reflect Interference Impact in Application Designs
  - Implement Systems to Monitor/Report/Locate Interference
  - Assess Applicability of Military Anti-Jam Technology
- **Encourage User Training in Use of Backups**
- **Determine Tolerable Levels of Risk and Cost for the Critical Infrastructure Applications**
  - Determine Costs of Lowering Risks to an Acceptable Level

Findings (1 of 3)

- **Transportation Community is Aware of Risks in Using Sole Means GPS in Critical Applications**
- **GPS is Vulnerable to Radiofrequency Interference**
- **GPS Augmentations (e.g., WAAS, NDGPS) Improve**
  - **Accuracy**
  - **Availability**
  - **Reliability**
  - **Integrity**

BUT: Use of GPS Can Still be Disrupted

Findings (2 of 3)

- **GPS Will Become an Increasingly Tempting Target as its Civil Uses Proliferate**
  - **Increasing Civil Dependence**
- **GPS is Susceptible to Unintentional Disruptions**
  - **Ionospheric, Solar**
  - **Blockage**
  - **Narrowband & Wideband RFI**
- **Use of GPS-based Timing Synchronization Must be Assessed, Application by Application**
  - **Transportation, Communications, Commerce**

Findings (3 of 3)

- **Military Experience: Hostile Interests Will Attempt to Disrupt/Destroy GPS if They See an Advantage in Doing So**
- **Risk Can be Reduced, But Not Eliminated**
  - **GPS Cannot be Sole Source in Critical Applications**
  - **Safety of Civilians is "Number 1"**
- **Backup Systems or Procedures are Necessary for All Critical Applications Involving GPS**

Candidate Independent Backup Systems

- **Ground-Based Aviation Systems - VOR/DME, ILS**
- **Inertial Systems**
- **Loran-C**
- **Other Satellite Navigation Systems**
- **"Procedures"**
  - **Missed Approach (Radar, Ground Support)**
  - **Maritime: Radar, Radio, Sextant, Lighthouse, etc.**
- **. . . .**

Recommendations (1 of 4)

- **Public Policy Must Ensure Safety if GPS Use is Lost**
- **Acceptable Level of Risk Must be Determined for Critical Applications**
  - **Costs to Lower Present Risk to this Level Must be Determined**
- **Continue GPS Modernization**
  - **More Civil Signals & Improved Code**
  - **Higher Broadcast Power**
- **Continue Spectrum Protection Activities**
- **Enhance Receiver Performance & Certification Standards in All Modes Where Feasible**

Recommendations (2 of 4)

- **All Critical Applications Need Quick Alert of GPS Disruption**
  - **Reporting**
  - **User Training**
- **Civil Community Should Track Military Anti-Jam Developments for Possible Use**
  - **Anti-Spoofing Technology**
  - **Identify, Use Spoof Indicators**

Recommendations (3 of 4)

- **Whenever Possible, Maximize Military-Civil Exchange of System Status, Incipient Threats**
- **Create Awareness of Need for Backups in Critical Applications**
- **All GPS Receivers Used in Critical Applications Need to Provide Integrity Warnings**
  - **Consider Autonomous Integrity Monitoring**
- **Augment, Enhance, and Implement Appropriate Backup Systems or Procedures**
  - **Assess Impact of GPS-Based Timing Loss**

Recommendations (4 of 4)

- **Continue Re-Capitalization and Enhancement of Loran-C**
  - **Modes Should Assess Potential Role of "New" Loran**
  - **Firm Decision Needed Soon - Industry Needs Direction**
- **DOT Take an Active Role in Developing Roadmap for the Future Navigation Infrastructure**
  - **Federal Radionavigation Plan**
  - **Modal Agencies to Assess Risk Impacts**

Report Summary

- **GPS Vulnerability Can be Reduced But Not Fully Eliminated**
- **Augmentations are Important for Integrity, But Can Not Eliminate Disruptions**
- **GPS Disruptions also Impact Timing**
- **Increasing Use Makes GPS a Tempting Target**
- **Independent Backup Systems or Procedures Essential in Critical Civil Transportation Uses**

Main Message to the Civil GPS Community:

GPS provides many benefits to civilian users. It is vulnerable, however, to interference and other disruptions that can have harmful consequences. GPS users must ensure that adequate independent backup systems or procedures can be used when needed.

Conclusion

- **Report available from the U.S. Coast Guard Navigation Center website**

  http://www.navcen.uscg.gov

"If the government expeditiously develops and executes a plan based on these recommendations, there is every reason to be optimistic that GPS will fulfill its potential as a key element of the national transportation infrastructure."

Contacts

Jim Carroll
U.S. Dept. of Transportation
Volpe National Transportation Systems Center
55 Broadway, Kendall Sq., Cambridge, MA 02142
(617) 494-2908; fax: (617) 494-2628
carrollj@volpe.dot.gov

Chuck Rodgers
OPTIMUS Corp.
8601 Georgia Avenue, Suite 700
Silver Spring, MD 20910
(301) 585-7075; fax: (301) 585-7976
Chuck.Rodgers@optimuscorp.com