VULNERABILITY ASSESSMENT OF THE TRANSPORTATION INFRASTRUCTURE RELYING ON THE GLOBAL POSITIONING SYSTEM

Final Report

August 29, 2001

Prepared by

John A. Volpe National Transportation Systems Center

for

Office of the Assistant Secretary for Transportation Policy
U. S. Department of Transportation

(This page deliberately left blank)

TABLE OF CONTENTS

Table of Contents iii
List of Figures v
List of Tables v
Executive Summary 1
1 Introduction 1
1.1 Purposes 1
1.2 Background 1
1.3 Scope 3
1.4 Approach 4
2 The Rapidly Evolving Transportation Uses of GPS 5
2.1 Availability of GPS to Civilian Users 5
2.2 GPS Transportation Uses and Navigation Requirements 5
2.2.1 Aviation 6
2.2.2 Maritime 10
2.2.3 Surface 14
2.2.4 GPS as a Timing Source 20
2.2.5 Critical Applications 23
3 Assessment of GPS Vulnerabilities 25
3.1 GPS Vulnerabilities to Unintentional Disruption 25
3.1.1 Ionospheric Interference 25
3.1.2 Unintentional Radio Frequency (RF) Interference 26
3.1.3 Human Factors in the Use of GPS 28
3.2 GPS Vulnerabilities to Intentional Disruption 29
3.2.1 Shutdown 30
3.2.2 Jamming, Spoofing, and Meaconing 30
4 GPS Vulnerability Mitigation Strategies 35
4.1 Mitigation of Unintentional Interference 35
4.1.1 Spectrum Management and Legal Action 35
4.1.2 Detection and Location Capability 35
4.1.3 GPS Modernization 35
4.1.4 Jam-Resistant User Equipment 36
4.2 Mitigation of Intentional Interference 36
4.2.1 Jamming 36
4.2.2 Spoofing 39
5 Assessment of Transportation Infrastructure Vulnerabilities 41
5.1 Aviation Vulnerability 42
5.1.1 Navigation (Oceanic, En Route, Terminal, NPA, PA) 43
5.1.2 Air Traffic Control Surveillance 44
5.1.3 Airport Surface Guidance and Surveillance 44
5.1.4 Communications System Timing 44
5.2 Maritime Vulnerability 45
5.3 Surface Vulnerability 46
5.3.1 Rail Assessment 46
5.3.2 ITS Assessment 47

5.4 Summary of Application Vulnerabilities 47
6 Transportation Infrastructure Risk Mitigation Strategies 49
6.1 Backup Strategies 50
6.2 Backup Navigation Systems 51
6.2.1 Loran-C 51
6.2.2 Other Satellite Navigation Systems 53
6.2.3 Loran-C/Inertial Systems 53
6.2.4 GPS/Inertial Systems 53
6.2.5 VOR/DME 54
6.2.6 Instrument Landing System (ILS) 55
6.3 Backup Surveillance Systems 55
6.3.1 Loran-C Based ADS 55
6.3.2 Multilateration 55
6.4 Backup Timing and Control 56
7 Findings and Recommendations 57
Appendix A. GPS Vulnerabilities 63
A.1 Causes of the Vulnerabilities 63
A.2 GPS Disruption Mechanisms 64
A.2.1 Unintentional Disruption Mechanisms 64
A.2.2 Intentional Disruption Mechanisms 70
A.3 Further Details of GPS Vulnerability 77
Appendix B. GPS Vulnerability Mitigation Strategies 79
B.1 Mitigation of Unintentional Interference 79
B.2 Mitigation of Intentional Jamming and Spoofing 82
B.3 Mitigation Strategies by Mode 84
Acronym List 91
References 95

LIST OF FIGURES

A-1 Illustration of Range Gate Capture Technique 74
A-2 GPS Signal Structure 78

LIST OF TABLES

2-1 GNSS Aviation Operational Performance Requirements 7
2-2 Mode S SSR Performance Requirements 9
2-3 ADS-B Accuracy Requirements 9
2-4 Navigation Sensor Requirements for Airport Surface Applications 10
2-5 Maritime Operational Performance Requirements 15
2-6 Critical Maritime Integrity Parameters 15
2-7 Railroad Navigation and Positioning Requirements 18
2-8 ITS Navigation System Accuracy Requirements 20
2-9 Communication Networks Synchronization Requirements 21
2-10 The ANSI T1 Standard Hierarchy of Clocks 21
5-1 Application Vulnerability and Risk Summary 48
6-1 Alternative Backup Strategies 50
6-2 Backup System Configurations 52

(This page deliberately left blank)

EXECUTIVE SUMMARY

BACKGROUND

The President's Commission on Critical Infrastructure Protection was established on July 15, 1996 by Executive Order 13010. The Commission conducted a 15-month inquiry into a broad range of infrastructure vulnerabilities, including those of the information and communications infrastructure. In the information and communications infrastructure, the most significant projected vulnerabilities found by the Commission were those associated with the modernization of the National Airspace System (NAS) and the plan to adopt the Global Positioning System (GPS) as the sole basis for radionavigation in the U.S. by 2010. In October 1997, the Commission recommended an assessment of the vulnerability of the transportation infrastructure relying on the use of GPS. Specifically, the report recommended a three-part assessment:

- *Fully evaluate actual and potential sources of interference to, and vulnerabilities of, GPS before a final decision is reached to eliminate other radionavigation and aircraft landing guidance systems.*

- *Sponsor an independent, integrated assessment of risks to civilian users of GPS-based systems, projected through the year 2010.*

- *Base decisions regarding the proper federal navigation systems mix and the final architecture of the modernized NAS on the results of that assessment*.

In response to recommendations of the Commission, on May 22, 1998, The White House issued Presidential Decision Directive 63 (PDD-63) [1][1]. The instruction in the Presidential Directive assigned to the Department of Transportation (DOT) was:

The Department of Transportation, in consultation with the Department of Defense, shall undertake a thorough evaluation of the vulnerability of the national transportation infrastructure that relies on the Global Positioning System. This evaluation shall include sponsoring an independent, integrated assessment of risks to civilian users of GPS-based systems, with a view to basing decisions on the ultimate architecture of the modernized NAS on these evaluations.

Civilian uses of GPS are growing rapidly. This is largely due to the quality of the service GPS provides, its ease of use, and low user cost. Not only is GPS found in obvious positioning and navigation applications, it is becoming a utility whose presence within some supporting systems (such as a timing reference for the national power grids and telecommunications systems) is not readily apparent. The civil transportation infrastructure, seeking the increased efficiency made possible by GPS, is developing a reliance on GPS that can lead to serious consequences if the service is disrupted, and the applications are not prepared with mitigating equipment and operational procedures.

[1] Numbers in square brackets, [#], refer to a reference entry in the numbered list in the "References" section.

In recent years, the potential for intentional, malicious disruption of GPS has been recognized. These disruptions can range from limited denial of GPS service caused by a low power, localized jammer to more catastrophic incidents that could result in the denial of GPS service over large geographic areas and for extended periods of time. An extremely damaging - although highly unlikely - scenario for loss of GPS service could theoretically result from a direct attack on the GPS satellites. The vulnerability of GPS and other U.S. civil and military space assets was discussed in the "Rumsfeld report [2]." The heightened awareness of this type of threat may help to ensure that future planning addresses the potential, however unlikely it seems today, "..for the GPS system..to experience widespread failure or disruption. [2]" The report concludes, "An attack on elements of U.S. space systems during a crisis or conflict should not be considered an improbable act."

SCOPE OF ASSESSMENT

This report responds to the directive concerning assessing the risks to the transportation infrastructure resulting from the degradation or loss of the GPS signal. This study includes analysis of civilian aviation, maritime, and surface uses of GPS, assessing the ways in which users might be impacted by a short or long term GPS outage, and recommending steps that the U.S. Government and user community might take to minimize the safety and operational impacts of such outages. This study is intended to consider operations extending at least to 2010, so that some speculation about the intended use of GPS, its augmentations, and alternative navigation systems and methods was necessary.

Quantifying the threat to civilian users of GPS due to deliberate disruption involves assigning likelihood values to the possible threat scenarios for all of the transportation modes. Although this hasn't been done in this assessment, it is important to realize that only a small percentage of scenarios are likely to represent serious threats; that is , threats that would put civilian lives, the economy, or the environment at risk, and that have some possibility of happening. It is expected that threats due to unintentional disruption of the GPS signal will become apparent and dealt with during the planning, design, testing, and implementation phases of the GPS system upgrades and augmentations.

STUDY APPROACH

The study was structured to:

- Determine critical civil transportation applications of GPS – areas where the effects of GPS vulnerability are believed to be critical and where the safety or operational consequences of disruptions are significant.
- Determine navigation system requirements for each of the critical civil transportation applications, to serve as a baseline for measuring the degree to which GPS signal degradation or loss can be tolerated.
- Assess the vulnerability of GPS to signal degradation.
- Assess current approaches to mitigating GPS signal degradation.

- Assess the vulnerability of critical civil transportation applications to the unmitigated degradation or loss of the GPS signal.
- Assess risk mitigation strategies to protect the U.S. transportation infrastructure in case of significant outage or failure of GPS.
- Provide recommendations for actions to further analyze identified risks and strategies, and for developing policy decisions on future navigation system architectures.

FINDINGS AND RECOMMENDATIONS

Three sets of findings and recommendations are made relative to:

- Overarching issues related to GPS vulnerabilities
- Mitigating the vulnerabilities of the GPS signal to disruption or loss
- Mitigating the vulnerabilities of the transportation system resulting from disruption or loss of the GPS signal

OVERARCHING ISSUES RELATED TO GPS VULNERABILITY

Findings

- There is growing awareness within the transportation community of the risks associated with the GPS system being the only means for position determination and precision timing. The risks are a function of the probability of intentional and unintentional interference and the transportation-related consequences of loss of the GPS signal. The probability of interference is, in turn, a function of the vulnerabilities of the GPS system to disruption and the threats that could be made against the GPS system.

- Like any radionavigation system, GPS is vulnerable to interference that can be reduced but not eliminated. Because of the increasing reliance of transportation upon GPS, the consequences of loss of the GPS signal can be severe (depending upon its application), in terms of safety and environmental and economic damage to the nation, unless the threats are mitigated.

- There are many augmentations to GPS (for example, the aviation Local Area Augmentation System - LAAS) that improve the basic GPS accuracy, reliability, availability, and integrity. However, even with these augmentations, use of GPS still can be disrupted and transportation services thus impaired. These impairments could range from mere inconvenience to major disruption of the national transportation infrastructure. The more serious consequences are very unlikely to occur, and can be avoided by awareness, planning, and supplementing GPS with a backup system or operational procedures when it is used in critical applications (applications in which the consequences of GPS loss could be catastrophic without ensuring that mitigating options are available).

- As GPS further penetrates into the civil infrastructure, it becomes a tempting target that could be exploited by individuals, groups or countries hostile to the United States. The potential

for denying GPS service by jamming exists. The potential for inducing a GPS receiver to produce misleading information exists. Loss of GPS satellites or the Operational Control Segment could also impact GPS service, but attacking these elements can be more challenging and likely would produce a more aggressive U.S. Government response than jamming GPS users.

Recommendations

- Public policy must ensure, primarily, that safety is maintained even in the event of loss of GPS. This may not necessarily require a backup navigation system for every application. Of secondary but immediate importance is the need to blunt adverse environmental or economic impacts. The focus should not be on determining the nature of the backup systems and procedures, but on which critical applications require protection.

- Because requiring a GPS backup will involve considerable government and user expense, it is recommended that the transportation community determine the level of risk each critical application is exposed to, what level of risk each application can accept, the costs associated with lowering the risk to this level, and how such costs are to be funded.

MITIGATING THE VULNERABILITIES OF THE GPS SIGNAL TO DISRUPTION OR LOSS

Unintentional Disruption

Findings

- The GPS service is susceptible to unintentional disruptions from ionospheric effects, blockage from buildings, and interference from narrow and wideband sources. Some natural phenomena such as ionospheric distortions and scintillation can be predicted. These disruptions are most noticeable for users of single-frequency (L1) receivers.

- GPS-based timing synchronization is being used both for transportation-related digital communication links and other applications such as telecommunications, banking, commerce, and the Internet. Critical communications systems such as the FAA NEXCOM digital air/ground communication system rely on timing synchronization between ground sites. Other aviation data links rely directly upon GPS for timing synchronization. This is recognized within the FAA, which is planning the system to mitigate the consequences of loss of timing synchronization. A possible synchronization source is the GPS signal.

Recommendations

- Continuation of on-going GPS modernization programs involving higher GPS broadcast signal power and the eventual availability of three civil frequencies should be encouraged.

- The Federal Communications Commission (FCC), FAA Office of Spectrum Policy and Management, National Telecommunications and Information Administration (NTIA), the

Departments of State and Defense, and other agencies should continue to vigorously support and protect the spectrum for GPS and its applications.

- GPS receivers involved in critical maritime and surface applications should be certified by the appropriate regulatory authorities. These authorities should recommend receiver performance standards for non-critical applications.

- Efforts must be taken to create and heighten awareness among the aviation, maritime, and surface user communities of the need for mitigation to degradation or loss of the GPS signal through unintended interference from such sources as VHF signals, mobile satellite services, ultra wideband communications, and broadcast television.

- Systems and procedures to monitor, report, and locate unintentional interference should be implemented or utilized in any application for which loss of GPS is not tolerable. Mitigation of signal blockage impacts should be addressed as much as possible in the GPS application system design process. RFI incidents that affect critical transportation applications should be reported to users as potential hazards to navigation, and users need to be trained in recognizing degradation or loss of the GPS signal, how to switch to an alternate navigation system or procedure if called for, and how to switch back to GPS when it recovers performance.

Intentional Disruption

Findings

- The GPS signal is subject to degradation and loss through attacks by hostile interests. Potential attacks cover the range from jamming and spoofing of GPS signals to disruption of GPS ground stations and satellites.

Recommendations

- Continuing assessments should be made of the applicability of military anti-jam technology, including receiver and antennas, to the civil sector. U.S. government agencies should be encouraged to identify the more promising anti-jam technologies, and to work with industry to make them affordable and suitable for civilian applications.

- The DOT should coordinate with the DoD to ensure that appropriate anti-spoofing technologies are available to civilian applications, should the need arise. It is important to identify observables that may indicate spoofing in civil safety-critical receivers. In addition, DOT should develop independent information to determine the validity and extent of possible civil spoofing threats.

- Within the limits of security requirements, the civil sector transportation community should be apprised of on-going threats and take effective countermeasures to those threats. Civil users should be encouraged to report GPS outages.

MITIGATING THE VULNERABILITIES OF THE TRANSPORTATION SYSTEM TO LOSS OR DEGRADATION OF THE GPS SIGNAL

Findings

- As with any radionavigation system, the vulnerability of the transportation system to unintentional and intentional GPS disruption can be reduced, but not eliminated. There is a growing awareness within the transportation community that the safety and economic risks associated with loss or degradation of the GPS signal have been underestimated. The GPS system cannot serve as a sole source for position location or precision timing for certain critical applications. Public policy must ensure that safety is maintained, even in the event of loss of GPS. Utilization of backup systems and procedures to GPS in applications where the consequences of losing GPS are unacceptable will ensure optimum safety.

- Backups for positioning and precision timing are necessary for all GPS applications involving the potential for life-threatening situations or major economic or environmental impacts. The backup options involve some combination of: (1) terrestrial or space-based navigation and precision timing systems; (2) on-board vehicle/vessel systems; and (3) operating procedures. Precision timing backups include cesium clocks or Loran-C for long-term equivalent performance, or rubidium or quartz clocks. The appropriate mix for a given application will result from careful analysis of benefits, costs, and risk acceptance.

Recommendations

- Create awareness among members of the domestic and global transportation community of the need for GPS backup systems or operational procedures, and of the need for operator and user training in transitions from primary to backup systems, and in incident reporting, so that safety can be maintained in the event of loss of GPS, in applications that cannot tolerate that loss.

- Encourage all the transportation modes to give attention to autonomous integrity monitoring of GPS signals, as is being done in the aviation and maritime modes (Receiver Autonomous Integrity Monitoring, RAIM).

- In an effort to provide the greatest benefit to the users, encourage the development of affordable vehicle-based backups such as GPS/inertial receivers, and, in the event Loran-C becomes a viable backup to GPS, aviation certifiable Loran-C receivers, and GPS/Loran-C receivers. All GPS receivers in critical applications must provide a timely warning when GPS positioning and timing signals are degraded or lost. Conditions for setting the warning indicator in the receiver, and for displaying it to users, should be standardized within each mode.

- Conduct a comprehensive analysis of GPS backup navigation and precise timing options including VOR/DME, ILS, Loran-C, inertial navigation systems, and operating procedures. Consideration must be given to: (1) the cost of equipage for both general and commercial users – national and international in aviation uses; (2) navigation and precision timing

system capital and operating costs; and (3) operating procedures and training costs associated with the need for situation awareness when the GPS signals are degraded or lost.

- Continue the Loran-C modernization program of the FAA and USCG, until it is determined whether Loran-C has a role as a GPS backup system. If it is determined that Loran-C has a role in the future navigation mix, DOT should promptly announce this to encourage the electronics manufacturing community to develop new Loran-C technologies.

- DOT should take an active role in developing a roadmap for the future navigation infrastructure that will be stated clearly in the Federal Radionavigation Plan, and will be followed by the DOT modes and navigation user communities in their navigation activities.

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.

(This page deliberately left blank)

1 INTRODUCTION

1.1 PURPOSES

The purposes of this study are to: assess the vulnerability of the U.S. national transportation infrastructure to degradation or loss of the Global Positioning System (GPS) signal; provide an independent, integrated assessment of impacts to civilian GPS users arising from the degradation or loss of GPS service; provide approaches to mitigate these impacts; and provide the basis for policy decisions on the future navigation system infrastructure.

1.2 BACKGROUND

The Global Positioning System (GPS) is a satellite navigation system developed by the United States military that provides accurate navigation signals to essentially any place in the world. In 1983, the United States announced that the Standard Positioning Service (as the civilian signal of GPS is known) would be made available to all users on a continuous, worldwide basis, for the indefinite future, free of any direct user charge. In January 1993, the Department of Transportation (DOT) and the Department of Defense (DoD) signed a Memorandum of Agreement on the civil use of GPS. In December 1993, the GPS satellite constellation was declared operational for civilian use. In 1997, DoD and DOT announced an agreement assuring civil users of GPS the availability of a second frequency. A second frequency is important for many civilian uses of GPS, to reduce susceptibility to GPS disruptions and ensure integrity under nominal conditions. In January 1999, a third civil frequency was announced.

Enhanced coverage, improved accuracy, and rapidly decreasing user equipment costs have resulted in a rapid rise in the use of GPS in the national transportation infrastructure. GPS uses promise to improve the safety of our transportation systems and increase their operational effectiveness.

Existing and planned uses of GPS include: a radionavigation aid; a source of accurate vehicle position as part of new improved surveillance systems; and a timing reference for much of the national power grids and telecommunications networks [3,4,5]. One can safely assume that in the near future, the transportation system will become more reliant on GPS. It has been suggested that GPS has the capability to serve as the only navigation system that the United States need operate and that users need to employ (see, for example [6], concerning aviation).

Since GPS has come into widespread use, certain limitations and vulnerabilities of the GPS signal and provider/user equipment have become evident. These limitations are in the areas of accuracy, reliability, integrity, and availability, and have prevented early decisions about the proper role of GPS in the national mix of radionavigation systems. Several GPS augmentation programs have been initiated to improve these limitations, and progress is being made to minimize these limitations.

However, GPS is vulnerable to unintentional and intentional radio frequency interference. The system is vulnerable also, albeit at much lower probability, to natural and intentional physical damage. Many technical improvements are being planned for GPS, such as increasing the signal

strength and number of frequencies, and improving vehicle antennas. These can reduce, but may not eliminate, the potential for short term, reduced geographic coverage area, and intermittent outages. There also is considerable attention within the community given to eliminating as much as possible the chance of damage to the GPS system itself – the satellites and the Operational Control Segment.

In recent years the potential for intentional, malicious disruption of GPS has been recognized. These disruptions can range from limited denial of GPS service caused by a low power, localized jammer to more catastrophic incidents that could result in the denial of GPS service over large geographic areas and for extended periods of time.

An extremely damaging - although highly unlikely - scenario for loss of GPS service could theoretically result from a direct attack on the GPS satellites. The vulnerability of GPS and other U.S. civil and military space assets was discussed in the "Report of the Commission to Address United States National Security Space Management and Organization," [2][1] (the "Rumsfeld report"). Increasing civil use of space for purposes such as research, communications, navigation, timing, and imaging generates in the U.S. a relative dependence on its space assets which, coupled with growing space-oriented capabilities of potential adversaries, requires the U.S. to take seriously even low-probability risks. They should not be ignored.

The Rumsfeld report publicly recognizes the potential for significant, wide ranging, and long term outages of GPS based upon hostile or terrorist action ([2], page 23). The heightened awareness of this type of threat may help to ensure that future planning addresses the potential, however unlikely it seems today, "..for the GPS system..to experience widespread failure or disruption. [2]" The report concludes, "An attack on elements of U.S. space systems during a crisis or conflict should not be considered an improbable act." The U.S. military, cognizant of the system limitations, is taking steps to harden its GPS dependent systems against the threat.

DoD recognizes that there are vulnerabilities in GPS and especially the C/A (civil - "coarse/acquisition") code that can be exploited to deny use or disrupt accurate use of the system. As knowledge of the military uses of GPS and its vulnerabilities becomes more widespread world-wide, the military prudently is implementing additional capabilities to protect its critical systems from such exploitation, and to fulfill its mandate to protect itself and the U.S. from hostile forces that may try to use the C/A code.

As the penetration of GPS into the civil infrastructure continues unabated, it becomes an increasingly tempting target that could be exploited by malicious persons or countries. If this results in a loss of GPS service, it could, in turn, result in:

- Transportation service disruption and resulting economic impact
- Environmental damage
- Property damage
- Serious injury or fatality
- Loss of confidence in a transportation mode
- Liability to the service provider

[1] Numbers in square brackets, [#], refer to a reference entry in the numbered list in the "References" section.

Despite these concerns, GPS will continue to be used in transportation because it provides unique capabilities and operational efficiencies. The challenge is to maximize the benefits while minimizing the risks. It is imperative, therefore, that the mechanisms and effects of disruption be known completely, so that suitable backup systems are available and effective equipment and training can be introduced to minimize the potential threat to public safety, the integrity of the transportation infrastructure, and the environment.

The President's Commission on Critical Infrastructure Protection was established on July 15, 1996 by Executive Order 13010. During the subsequent 15 months the Commission conducted inquiries into a broad range of infrastructure vulnerabilities, including those of the information and communications infrastructure. In the information and communications infrastructure, the most significant projected vulnerabilities found by the Commission were those associated with the modernization of the National Airspace System (NAS) and the plan to adopt the Global Positioning System (GPS) as the sole basis for radionavigation in the U.S. by 2010. An assessment of the vulnerability of the transportation infrastructure relying on use of GPS was recommended in the October 1997 Commission report. Specifically, the report recommended three parts in the assessment:

- *Fully evaluate actual and potential sources of interference to, and vulnerabilities of, GPS before a final decision is reached to eliminate other radionavigation and aircraft landing guidance systems.*

- *Sponsor an independent, integrated assessment of risks to civilian users of GPS-based systems, projected through the year 2010.*

- *Base decisions regarding the proper federal navigation systems mix and the final architecture of the modernized NAS on the results of that assessment*.

In response to recommendations of the Commission, The White House published Presidential Decision Directive 63 (PDD-63) [1] on May 22, 1998. The instruction in the Presidential Directive assigned to the Department of Transportation (DOT) was:

The Department of Transportation, in consultation with the Department of Defense, shall undertake a thorough evaluation of the vulnerability of the national transportation infrastructure that relies on the Global Positioning System. This evaluation shall include sponsoring an independent, integrated assessment of risks to civilian users of GPS-based systems, with a view to basing decisions on the ultimate architecture of the modernized NAS on these evaluations.

This report responds to the directive concerning the risks to the transportation infrastructure resulting from the degradation or loss of the GPS signal.

1.3 SCOPE

This study analyzes civilian aviation, maritime, and surface users of GPS, the ways in which they might be impacted by a short or long term GPS outage, and steps that the U.S. Government and user communities might take to minimize the safety, operational, and economic impacts of such

outages. The threats to reliable GPS operation were assessed qualitatively, and included the effect of natural phenomena (for example, sunspots), unintentional (for example, certain TV broadcast frequencies, cell phone emissions), and intentional interference (for example, spoofing and jamming). Vulnerabilities of GPS to signal degradation can result in a range of consequences including degradation of guaranteed service performance, full denial of the service, and acceptance of misleading navigation information. Disruption and damage that result in long term GPS outages that could be caused by hostile actions far less overt than full scale war also are considered. Risks to civil users of GPS were assessed qualitatively, to aid in identifying critical applications, or uses, of GPS. That is, applications for which serious consequences may result if GPS becomes unusable, and if there are no procedures or backup systems to mitigate the loss.

The time frame for this analysis extends through the next ten to fifteen years. Implicit in much of the discussion, then, is the assessment of GPS-based systems that are not in service today, such as the aviation systems.

1.4 APPROACH

The approach followed in this study employed the steps listed below and this report is organized accordingly:

Chapter 2: Determine critical civil transportation application of GPS – areas where the effects of GPS vulnerability are believed to be critical and where the safety or operational consequences of disruptions are significant. Determine navigation system requirements for each of the critical civil transportation applications, to serve as a baseline for measuring the degree to which GPS signal degradation or loss can be tolerated.

Chapter 3: Assess the vulnerability of GPS to signal degradation.

Chapter 4: Assess current approaches to mitigating GPS signal degradation.

Chapter 5: Assess the vulnerability of critical civil transportation applications to the unmitigated degradation or loss of the GPS signal.

Chapter 6: Assess risk mitigation strategies to protect the U.S. transportation infrastructure in case of significant outage or failure of GPS.

Chapter 7: Provide findings and recommendations for actions to analyze further identified risks and strategies, and for developing policy decisions on future navigation system architectures.

2 THE RAPIDLY EVOLVING TRANSPORTATION USES OF GPS

Civilian uses of GPS are growing rapidly. This is largely due to the quality of the service GPS provides, its ease of use, and low user cost. Not only is GPS found in obvious positioning and navigation applications, it is becoming a utility whose presence within some supporting systems (such as a timing reference for the national power grids and telecommunications systems) is not readily apparent. The civil transportation infrastructure, seeking the increased efficiency made possible by GPS, is developing a reliance on GPS that can lead to serious consequences if the service is disrupted, and the applications are not prepared with mitigating equipment and procedures. This chapter outlines some of the transportation users and usage of GPS, and the requirements these applications place upon GPS accuracy, reliability, integrity, and availability.

2.1 AVAILABILITY OF GPS TO CIVILIAN USERS

Although GPS was created to meet military needs, one signal transmitted by each GPS satellite has been available to non-military users of all nations since inception of the system. Following the destruction of Korean Air Lines flight KAL-007 when it went off course near Sakhalin Island, Russia on August 31, 1983, President Reagan offered free use of the "GPS C/A coded signal" to the civilian community. The C/A coded signal and the supporting infrastructure and policies are called the GPS Standard Positioning Service (SPS). Federal government policy on the civil use of GPS is:

SPS is available to all users on a continuous, worldwide basis, for the indefinite future, free of any direct user charge [7].

In January 1993, the Department of Transportation (DOT) and the Department of Defense (DoD) signed a Memorandum of Agreement on the civil use of GPS. In December 1993, the GPS satellite constellation was declared operational for civilian use. In 1997, DoD and DOT announced an agreement assuring civil users of GPS the availability of a second frequency. A second frequency is important for many civilian uses of GPS. In January 1999, a third civil frequency was announced. In May 2000, convinced that theater denial of GPS is a feasible and appropriate policy, DoD turned off the Selective Availability feature. Hostile GPS users can be denied the service via jamming within the theater of operations, while civil users outside the theater are not denied the service. The Selective Availability decision now makes the un-degraded GPS C/A-code signal accuracy accessible to civil users worldwide.

2.2 GPS TRANSPORTATION USES AND NAVIGATION REQUIREMENTS

This section describes several modal (for example, aviation, maritime, and surface) civil applications of GPS. As part of this description, applications whose present or potential vulnerability to the degradation or loss of GPS will have serious to catastrophic consequences are defined to be "critical applications." These are summarized in Section 2.2.5. Criticality is defined in terms of risk to human life and economic and environmental damage. Each application description contains a set of GPS-related requirements, applicable to the subset of critical applications also. Requirements are needed to determine the degree to which the application can tolerate loss or degradation of the GPS service.

There is an awareness that most modal applications, whether or not they currently utilize GPS, also have available alternate navigation systems or procedures. The assessments in this report attempt to factor in the present and planned role of these alternative navigation methods.

2.2.1 AVIATION

This section describes aviation applications of navigation (oceanic, en route, terminal, nonprecision approach (NPA) and precision approach (PA)), and to a lesser extent air traffic control surveillance and airport surface navigation. At the present time, GPS is not the primary navigation system in the National Airspace System, but it is a key element to enhancing safety and efficiency of civil air travel in the U.S., in the near future. The issue is, when augmented GPS is fully implemented in the NAS, to what degree must GPS in aircraft be supplemented with other navigation systems or operational procedures in order to maintain safe operations if GPS is degraded or lost? The other systems and procedures are in place today, but many are planned for eventual phase out for economic and efficiency reasons. Critical aviation applications include approach and landing operations. They depend on the navigation mix to offset loss of GPS.

The use of GPS is expected to increase the safety and efficiency of operations both within the U.S. National Airspace System (NAS) and on a global basis. The extremely accurate position, velocity, and timing information available from GPS and its augmentations will be used to support future Communication, Navigation, and Surveillance (CNS) and Air Traffic Management (ATM) initiatives. These initiatives include replacement of two-dimensional (2D) nonprecision approaches with 3D guidance for all terminal operations; reduction of aircraft separation for en route operations; creation of new area navigation (RNAV) routes that support more direct routing; and implementation of GPS-based Automatic Dependent Surveillance (ADS). ADS-B is initially meant to support aircraft-to-aircraft operations and ground-based surveillance in regions where radar-based surveillance is either physically or economically infeasible (such as Alaska or the Gulf of Mexico). A decision on deployment throughout the NAS has yet to be made. Implementation of GPS also is planned to save costs by allowing for a reduction in the number of ground-based navigation aids, as well as a reduced set of avionics in the aircraft.

In October 1996 the FAA published the *National Airspace System Architecture, Version 2.0* [8]. The navigation systems planning timeline in this document showed that all current air navigation aids will be phased out by 2010. Only GPS and augmented GPS systems were to be provided for civil aviation by the government after 2010. The *1996 Federal Radionavigation Plan* [9] included the *Radionavigation System Operating Plan* that showed only GPS-based navigation aids after 2010.

In January 1999, the updated *National Airspace System Architecture, Version 4.0* [10] stated that approximately 600 VOR/DME, 500 ILSs, and 280 NDBs would be retained to support en route navigation and instrument operations at about 2,400 airports in the NAS, should there be a disruption in GPS/WAAS service. In a similar fashion, the *1999 Federal Radionavigation Plan* [7] characterized augmented GPS (WAAS and LAAS) as a primary rather than a sole means navigation system and provided for a sustained operations capability in the event of a disruption in satellite navigation service. This reflects comments made by FAA Administrator Garvey, “All

the analysis we've seen to date, says we will always have a backup navigation system on the ground" [11].

Navigation (Oceanic, En Route, Terminal, Nonprecision Approach, Precision Approach)

It has been suggested [6,8,10] that GPS has the capability to serve as the only navigation system that the United States need operate and that users need to employ. However, DOT and the FAA have recognized the GPS vulnerability issue and GPS augmented by WAAS is slated to be a primary-means, not a sole-means navigation system. The operational performance requirements for navigation in applications from oceanic navigation to precision are provided in Table 2-1. These are based on FAA and International Civil Aviation Organization (ICAO) requirements for use of a Global Navigation Satellite System (GNSS) [7,12,13].

The FAA currently has certified GPS for primary means oceanic use and as a supplemental system for domestic en route through nonprecision approach (NPA) operations. As a supplemental navigation aid, GPS cannot be the only navigation system carried onboard the aircraft. Typically the other navigation equipment is VOR/DME avionics.

The GPS system itself does not have an integrity monitoring capability that can satisfy the stringent requirements for aviation. Therefore other techniques must be applied to ensure that the pilot is provided with a timely warning if GPS should not be relied upon for navigation. When an augmentation system is not used, two available techniques are the Receiver Autonomous Integrity Monitoring (RAIM) and Fault Detection and Exclusion (FDE) algorithms, which are internal to the GPS receiver. These algorithms use measurements from additional

Table 2-1. GNSS Aviation Operational Performance Requirements [7,12,13]

Operation	Accuracy (95%)	Integrity	Continuity	Alert Limit	Time to Alert	Availability
Oceanic	12.4 nmi	$1\text{-}10^{-7}$/hr	$1\text{-}10^{-5}$/hr	4.0 nmi	2 min	0.99 to 0.99999
En Route	2.0 nmi	$1\text{-}10^{-7}$/hr	$1\text{-}10^{-5}$/hr	2.0 nmi	1 min	0.99 to 0.99999
Terminal	0.4 nmi	$1\text{-}10^{-7}$/hr	$1\text{-}10^{-5}$/hr	1.0 nmi	30 sec	0.99 to 0.99999
NPA	220 m	$1\text{-}10^{-7}$/hr	$1\text{-}10^{-5}$/hr	0.3 nmi	10 sec	0.99 to 0.99999
APV I	220 m (H) 20 m (V)	$1\text{-}2\text{x}10^{-7}$/ approach	$1\text{-}8\text{x}10^{-6}$/ 15 sec	0.3 nmi (H) 50 m (V)	10 sec	0.99 to 0.99999
APV II	16 m (H) 8 m (V)	$1\text{-}2\text{x}10^{-7}$/ approach	$1\text{-}8\text{x}10^{-6}$/ 15 sec	40 m (H) 20 m (V)	6 sec	0.99 to 0.99999
Cat. I	16 m (H) 4.0 to 6.0 m (V)	$1\text{-}2\text{x}10^{-7}$/ approach	$1\text{-}8\text{x}10^{-6}$/ 15 sec	40 m (H) 10 - 15 m (V)	6 sec	0.99 to 0.99999
Cat. II	6.9 m (H) 2.0 m (V)	$1\text{-}1\text{x}10^{-9}$/ 15 sec.	$1\text{-}4\text{x}10^{-6}$/ 15 sec	17.3 m (H) 5.3 m (V)	1 sec	0.99 to 0.99999
Cat. III	6.2 m (H) 2.0 m (V)	$1\text{-}1\text{x}10^{-9}$/ 15 sec.	$1\text{-}2\text{x}10^{-6}$/ 30 sec (L) $1\text{-}2\text{x}10^{-6}$/ 15 sec (V)	15.5 m (H) 5.3 m (V)	1 sec	0.99 to 0.99999

(redundant) satellites to develop an over-determined navigation solution, thereby allowing a faulty satellite to be detected (RAIM) and excluded (FDE). RAIM/FDE primarily is used for oceanic through nonprecision approach operations.

Although the availability requirement in Table 2-1 varies from 0.99 to 0.99999, the FAA goals are 0.999 for oceanic operations, 0.99999 for en route through NPA phases of flight, and 0.999 for precision approach. Some locations may require 0.99999 for precision approach.

Augmentations to GPS are required for several reasons, including improving the accuracy to conduct precision approaches and improving the availability of integrity monitoring. The Wide Area Augmentation System (WAAS) is an augmentation to GPS that determines GPS integrity and differential correction data on the ground through a network of monitor stations and a central processing facility. It then uses geostationary satellites to broadcast integrity messages and differential corrections, as well as a ranging signal, to the aircraft on the GPS L1 frequency. Following operational approval, WAAS signals can be used to improve GPS accuracy, availability, and integrity throughout CONUS. The WAAS will be interoperable with other satellite-based augmentation systems such as the European EGNOS and the Japanese MSAS.

The Local Area Augmentation System (LAAS) is another augmentation to GPS which will be used to support terminal area navigation and CAT I through CAT III precision approach operations. The LAAS ground system consists of multiple reference antennas/receivers at an airport, a processing station, VHF data broadcast equipment, and optionally ground-based pseudolites[2]. The GPS signals received by the multiple reference/monitoring antennas are processed to obtain the differential correction and integrity information, which is then broadcast to the aircraft via the VHF data link.

Air Traffic Control Surveillance

Currently, the principal method used by the Air Traffic Control (ATC) system for surveillance of airborne aircraft is the Secondary Surveillance Radar (SSR). SSRs are used for surveillance of terminal areas surrounding large and mid-sized airports and for en route airspace above and between terminal areas. In the 1990s, some older SSRs have been replaced by Mode S SSRs Key Mode S performance specifications are listed in Table 2-2.

ADS-B accuracy requirements established by the RTCA Minimum Aviation System Performance Standards (MASPS) are given in Table 2-3. The requirements for aircraft on the airport surface necessitate LAAS augmentation.

Airport Surface Navigation

Surveillance on the airport surface currently is performed by the ASDE-3 radar, which is deployed at 34 major airports. A new system, ASDE-X, is being developed for use at 25 additional airports. ASDE-X includes three sensor capabilities: a radar, a multilateration system that determines the location and identity of aircraft, and ADS-B, which receives aircraft

[2] Pseudolites broadcast GPS satellite-like signals from one or more locations on an airport.

broadcasts of aircraft-derived position from ADS-B equipped aircraft. The FAA has recognized a need for more widely deployed, lower cost system that will improve guidance and situational awareness for air traffic controllers, pilots, and vehicle drivers at less busy airports. A system

Table 2-2. Mode S SSR Performance Parameters

Parameter	Specification
Range:	
Terminal	60 to 100 nmi
En Route	200 to 250 nmi
Scan Period:	
Terminal	4 to 6 sec
En Route	8 to 12 sec
Availability	0.99995
Range Accuracy:	
Bias	30 ft
Jitter	25 ft
Azimuth Accuracy:	
Bias	0.003 deg
Jitter	0.068 deg
Sensitivity	-95 dBm
Detection Probability	0.99
False Alarm Probability	10^{-6}

Table 2-3. ADS-B Accuracy Requirements [14]

Parameter	Aircraft Location	
	Airborne	Surface
Horizontal Position	20 m	2.5 m
Horizontal Velocity	0.25 m/sec	0.25 m/sec
Vertical Position	30 ft	N/A
Vertical Velocity	1 ft/sec	N/A

based on ADS-B, perhaps one derived from the ASDE-X equipment, is a strong candidate for this role.

RTCA DO-247 [15] describes the role of GNSS in supporting future airport surface operations. This vision is expected to heavily influence future FAA airport surface system developments. RTCA envisions GPS and ADS-B as key components of this future system, which is known as the Advanced Surface Movement Guidance and Control System (A-SMGCS). Suitably equipped aircraft will "see" other surface aircraft. By overlaying all aircraft locations within a given vicinity on a moving map display, pilot situational awareness can be significantly improved under low visibility conditions.

The four primary functions of A-SMGCS concept are surveillance, routing, guidance, and control. Operational performance requirements (accuracy, integrity, continuity, and availability) for navigation sensors in airport surface use are provided in Table 2-4.

Since A-SMGCS will require high accuracy, GPS will not be able to satisfy the requirements without augmentation. WAAS and LAAS are envisioned as the two primary augmentations;

however these system architectures, as currently defined, will be insufficient to satisfy the surveillance sensor requirements for all visibility conditions.

Although the future ADS-B is to be based primarily on GPS for the position and velocity information, this information also may come from other navigation sources and radar. It should be noted that, like transponder-based SSR surveillance systems, a GPS-based system would not cover unequipped vehicles.

Table 2-4. Navigation Sensor Requirements for Airport Surface Applications [15]

Requirement	Visibility Condition		
	1, 2	3	4
Accuracy	10 m	2.2 m	1.5 m
Integrity	$1\text{-}10^{-5}$/hr	$1\text{-}10^{-6}$/hr	$1\text{-}10^{-7}$/hr
Continuity	$1\text{-}10^{-3}$/hr	$1\text{-}4\text{x}10^{-4}$/hr	$1\text{-}3\text{x}10^{-4}$/hr
Alert Limit	8 m	6 m	TBD
Time to Alert	10 sec.	2 sec.	2 sec.
Availability	0.95	0.999	0.999

2.2.2 MARITIME

Maritime GPS applications are expanding rapidly. The applications include supporting the U.S. Coast Guard in its regulatory, defense, safety, and law enforcement missions as well as a variety of commercial, and recreational activities. This section describes maritime GPS use, and requirements for GPS to be used for the critical maritime operations.

GPS and its augmentations are mandated for limited civil maritime use at this time. U.S. law (Title 33, CFR) governs GPS use in Automatic Identification Systems (AIS), an international standard recently approved by the International Maritime Organization (IMO). All vessels meeting certain size and function standards[3], that also are required to provide automated position reports to a Vessel Traffic Service (VTS), must do so with shipborne AIS equipment. The equipment, a differential GPS (DGPS) receiver, a marine band (medium frequency) beacon receiver capable of receiving DGPS error correction messages (see the MDGPS system description below), and a Digital Selective Calling (DSC) VHF-FM transceiver, has to:

- Provide position, velocity and time (PVT) and course information from DGPS with accuracies set by Title 33, CFR
- Receive and comply with commands broadcast as a DSC message
- Transmit the vessel PVT information, course over ground and the ship's Lloyd's identification number to a VTS
- Display a visual alarm when the MDGPS system cannot provide the required error correction messages, and
- Display tow RTCM type 16 messages, one of which must display the position error in the position error broadcast.

[3] The IMO Carriage Requirement for AIS applies to all ships of 300 gross tonnage and upwards engaged on international voyages and cargo ships of 500 gross tonnage and upwards not engaged on international voyages, and passenger ships irrespective of size. The carriage compliance dates range from July 1 2002 to July 1 2007. Many U.S. ships subject to the Bridge-to-bridge Radiotelephone Act also may be required to carry AIS equipment.

Universal AIS (UAIS) is a shipboard broadcast transponder system, operating in the VHF marine band, and capable of sending AIS information and ship length, beam, type, draft, and hazardous cargo information on a ship-to-ship and ship-to-shore basis. UAIS uses Self-Organizing Time Division Multiple Access (SOTDMA) technology to handle over 2,000 reports per minute[4] and updates as often as every two seconds. Heading information and course and speed over ground are normally provided by all AIS-equipped ships. Other information, such as rate of turn, angle of heel, pitch and roll, and destination and ETA also could be provided, depending in part on particular VTS needs.

UAIS is backwards-compatible with DSC systems, allowing shore-based Global Marine Distress and Safety (GMDSS) systems to identify and track AIS-equipped vessels, and UAIS will fully replace existing DSC-based transponder systems (which have much slower data transfer rates).

The AIS equipment and data link must conform to International Electrotechnical Commission (IEC), National Marine Electronics Association (NMEA), IMO, and International Telecommunication Union (ITU) standards. The transponder normally works in an autonomous and continuous mode, regardless of whether the vessel is in open seas or coastal/inland waterways. Transmissions, at 9,600 kilobytes, generally are made over a different radio channel than the received data, to avoid interference problems. The system provides for automatic contention resolution between itself and other stations, and communications integrity is maintained even in overload situations. Coverage range is similar to other VHF applications – broadcasts can "see" around bends and behind islands with moderate-height hills. In open waters, the range is about 20 nautical miles, and with the aid of shore-side repeater stations – if the vessel is "in view" – ship and VTS station coverage can be improved considerably.

The 1997 ITU World Radio Conference designated two VHF radio frequencies for AIS: 161.975 MHz (AIS1, channel 87B) and 162.025 MHz (AIS2, channel 88B). In the U.S., AIS1 is owned by a private company, MariTEL, and AIS2 by the federal government. The USCG is applying for authority from the Department of Commerce/NTIA to use AIS2 for AIS operation in the U.S., having obtained a Memorandum of Agreement with MariTEL. The primary AIS standard is ITU-R Recommendation M.1371-1, expected to be adopted by June 2001.

Although adherence to these standards will greatly improve safety and efficiency in maritime operations, there are at present no fully compliant AIS systems, nor have recently proposed marine GPS receiver certification standards been implemented. Increasing use of and resulting reliance on GPS make it necessary to examine the impact of the loss of GPS on maritime operations. The navigation standards for AIS can only be met by a global navigation satellite system such as GPS, which also can provide the necessary timing precision. The loss of ability to use GPS therefore will greatly reduce the effectiveness of AIS.

[4] This is an IMO standard. UAIS actually can provide 4,500 reports (time slots) per minute.

Maritime Operations

Selected maritime operations that can involve use of GPS and augmented GPS[5] are:

- Vessel navigation, according to phases or zones:
  - Oceanic
  - Coastal
  - Harbor and harbor approach (HHA)
  - Inland waterway and constricted channel
- Vessel Traffic Services (VTS) Surveillance
- Search Missions
- Resource Exploration
- Aids to Navigation (ATON) Positioning
- Area Surveying, Engineering, and Construction.

The maritime DGPS augmentation available in U.S. waters is the Marine Differential GPS (MDGPS) navigation service. MDGPS, operated by the U.S. Coast Guard, attained Full Operational Capability (FOC) on March 15, 1999. Many other maritime nations have deployed differential GPS systems similar to the U.S. MDGPS.

MDGPS has been designed to provide differential service to mariners operating in U. S. coastal and major inland waterways. MDGPS comprises over 55 remote DGPS broadcast sites, or reference stations, and two control stations. The system makes maximum use of the existing medium frequency marine radiobeacon sites and equipment.

Pseudorange corrections computed at a reference station are broadcast in the 285–325 kHz band by modulating the existing radiobeacon signals without interfering with the utility of the beacon for traditional direction finders. The differential correction information is formatted in accordance with the standards established by the Radio Technical Commission for Maritime Services, Special Committee 104 (RTCM SC-104). Predictable accuracy for users in the coverage area often is much better than the 10-meter 2drms performance specification. This is due often to a combination of using a high-end receiver or being close to the transmitting reference station. System integrity is provided through an integrity monitor located at each broadcast site. Notification of an out-of-tolerance condition can be provided within 6 seconds of its occurrence.

Augmented GPS (DGPS) already has demonstrated the ability to add greatly to the safety of most maritime operations. It is a reliable navigation aid in poor weather and where constricted channels or traffic congestion increase the risk of an adverse event. The USCG Ports and Waterways Safety System (PAWSS), now being planned for several key U.S. ports, will utilize DGPS and the emerging Universal AIS (UAIS) technologies.

[5] In this section, "augmented GPS" will refer unless specifically noted otherwise to the USCG maritime DGPS service, provided to all of the coastal (out to about 50 nautical miles) and major inland waterways in the Conterminous United States (CONUS), and to nearly all of the similar waterways in Alaska, Hawaii, and Puerto Rico.

In addition to the evident navigation and safety benefits that result from maritime use of augmented GPS, there are other benefits:

- Augmented GPS provides potentially high accuracy to determine keel clearance in HHA areas. This knowledge can be used either to reduce the operating margin of uncertainty to add more cargo, or to split the added margin between more cargo and added safety. Either way, with more average cargo on vessels, costs and traffic are reduced, and safety enhanced.
- Much like aviation free flight, augmented GPS in HHA can reduce spacing of vessels in a channel, because of greater location certainty.
- The increased accuracy of augmented GPS can aid re-acquisition of signal (for example, due to passing under a bridge) by reducing the receiver search time.

In addition to its role in AIS, many vessels are equipped with GPS-based autopilots. This is done to exploit the obvious PVT capabilities of GPS. These systems, like most others, have failed to work, or were improperly installed or used. Sometimes the autopilot failure, even if not caused by a GPS problem, makes matters worse by continuing to provide believable, albeit false, information. See Section 3.1 and Appendix A for details on the Royal Majesty incident.

Vessel navigation adheres to different sets of requirements, defined in part by the following navigation phases or zones.

Oceanic. Ocean navigation is that phase in which a ship is beyond the continental shelf (200 meters in depth), and more than 50 nautical miles from land, in waters where position fixing by visual reference to land or to fixed or floating aids to navigation is not practical. Ocean navigation is sufficiently far from landmasses so that the hazards of shallow water and of collision are comparatively small.

Coastal. Coastal navigation is that phase in which a ship is within 50 nautical miles of shore or within the limit of the continental shelf (200 meters in depth), whichever is greater, where a safe path of water at least one mile wide, if a one-way path, or two miles wide, if a two-way path, is available. In this phase, a ship is in waters contiguous to major land masses or island groups where transoceanic traffic patterns tend to converge in approaching destination areas; where interport traffic exists in patterns that are essentially parallel to coastlines; and within which ships of lesser range usually confine their operations. Ships on the open waters of the Great Lakes also are considered to be in the coastal phase of navigation.

HHA area. Harbor entrance and approach navigation is conducted in waters inland from those of the coastal phase. For a ship entering from the sea or the open waters of the Great Lakes, the harbor approach phase begins generally with a transition zone between the relatively unrestricted waters where the navigation requirements of coastal navigation apply, and narrowly restricted waters near and/or within the entrance to a bay, river, or harbor, where the navigator enters the harbor phase of navigation. Usually, harbor entrance requires navigation of a well-defined channel which, at the seaward end, is typically from 180 to 600 meters in width if it is used by large ships, but may narrow to as little as 120 meters farther inland. Channels used by smaller craft may be as narrow as 30 meters.

From the viewpoint of establishing standards or requirements for safety of navigation and promotion of economic efficiency, there is some generic commonality in harbor entrance and approach. For analytical purposes, the HHA phase is built around the problems of precise navigation of large seagoing and Great Lakes ships in narrow channels between the transition zone and the intended mooring.

Inland Waterway. Inland waterway navigation is conducted in restricted areas similar to those for harbor entrance and approach. However, in the inland waterway case, the focus is on non-seagoing ships and their requirements for long voyages in restricted waterways, typified by tows and barges in the U.S. Western Rivers System and the U.S. Intracoastal Waterway System.

In some areas, seagoing craft in the harbor phase of navigation and inland craft in the inland waterway phase share the use of the same restricted waterway. The distinction between the two phases depends primarily on the type of craft. It is made because seagoing ships and typical craft used in inland commerce have differences in physical characteristics, personnel, and equipment. These differences have a significant impact upon their requirements for aids to navigation.

Maritime Navigation Requirements

Augmented GPS (DGPS) performance requirements are dictated by four important maritime applications [16]:

- HHA navigation and inland waterways
- VTS surveillance
- ATON positioning
- Area Surveying, Engineering, and Construction

The performance requirements in Table 2-5 do not include the reliability and integrity parameters. Reliability is dependent upon mission time. Integrity normally is quantified by specific performance parameters that can differ depending upon the navigation system under consideration. For GPS, RTCA Special Committee SC-159 has adopted the critical integrity parameters shown in Table 2-6 for aviation use [17]. Values for the performance-restrictive HHA zones, taken from Table 2-6, will drive maritime DGPS integrity requirements. They are felt to be adequate also for marine DGPS use, using the values as shown [16].

2.2.3 SURFACE

The surface transportation applications studied here deal with positive train control (PTC) systems being developed to improve the safety and efficiency of U.S. railroads, and elements of the Intelligent Transportation Systems (ITS) being developed to improve the safety and efficiency of U.S. highways and transit systems. Both use GPS as a source of location and speed information. In these cases, the loss or degradation of the GPS signal would most likely result in reduced efficiency rather than a direct safety hazard. However, for certain ITS applications, a reduced efficiency of operations, especially in locating accident victims for timely attention, could result in delays that, in the case of hazardous materials response or medical emergency could result in environmental damage or loss of life. Thus, ITS/emergency response and some hazardous materials transport operations are classified as critical applications.

Table 2-5. Maritime Operational Performance Requirements [7]

Operation	Accuracy (2drms)		Coverage	Availability	Fix Interval	Fix Dimension	Ambiguity
	Predictable	Repeatable					
Oceanic – Safety	1-2 nmi	-	Worldwide	99% fix at least every 12 hours	15 min	Two	Resolvable with 99.9% confidence
Oceanic – Resource Exploration	10-100 m	10-100 m	Worldwide	99%	1 min	Two	Resolvable with 99.9% confidence
Oceanic – Search Operations	0.1-0.25 nmi	0.25 nmi	National Marit. SAR regions	99%	1 min	Two	Resolvable with 99% confidence
Coastal – Safety	0.25 – 2 nmi		US coastal waters	99.7%	2 min	Two	Resolvable with 99.9% confidence
Coastal – Search, En-forcement	0.25 nmi	300-600 ft	US coastal areas	99.7%	1 min	Two	-
Coastal – Resource Exploration	1.0-100 m	1.0-100 m	US coastal areas	99%	1 sec	Two	-
HHA – Safety	8-20 m	8-20 m	US harbor entrance & approach	99.7-99.9%	6-10 sec	Two	Resolvable with 99.9% confidence
HHA – Resource Exploration	1-5 m	1-5 m	US harbor entrance & approach	99%	1 sec	Two	Resolvable with 99.9% confidence
HHA – Engineering/Consulting	5 m horiz. 0.1 m vert.	5 m horiz. 0.1 m vert.	Entrance, channel, jetties, etc.	99%	1-2 sec	Two or Three	Resolvable with 99.9% confidence
Inland Waterway – Safety	2-5 m	2-5 m	US Inland Waterway Systems	99.9%	1-2 sec	Two	Resolvable with 99.9% confidence
Inland Waterway – construction	5 m horiz. 0.1 m vert.	5 m horiz. 0.1 m vert.	US Inland Waterway Systems	99%	1-2 sec	Two or Three	Resolvable with 99.9% confidence

Table 2-6. Critical Maritime Integrity Parameters

Integrity Parameters	Value
Protection limit	13-32 m, for 8-20 m accuracy, respectively
Time to alarm	10 seconds
Total alarm rate	2000-500 outages/10^6 hour
Probability of missed detection	6.7×10^{-6} per hour

Surface operations can rely on GPS in two ways, positioning and timing. The service usually uses on a communications link that may also depend on GPS for timing. In either use, loss or degradation of the GPS signal may have a potentially hazardous or catastrophic effect for vehicles reporting or responding to a medical emergency or hazmat incident, unless alternatives to GPS can be used. Large and persistent disruptions may have undesirable economic impact.

A Nationwide Differential GPS (NDGPS) system is being established to provide differential corrections for users outside of the coverage of the USCG maritime DGPS Service. Seven

federal agencies from the Departments of Transportation, Defense, and Commerce are now expanding MDGPS to meet the requirements of surface users in the U. S.

NDGPS broadcasts MSK-modulated signals in the maritime radiobeacon band (285-325 kHz) and uses the same RTCM SC-104 standard, as does the USCG DGPS service. The predictable accuracy of the NDGPS service within all established coverage areas is better than 10 meters (2drms) [7]. Accuracy degrades at a rate of approximately one meter per 150 km distance from the broadcast site where it is typically better than one meter. Service availability is expected to be 99.7% for dual coverage areas and 99.9% for single coverage areas. This means that the likelihood that at least one broadcast station will be available to the user is 99.9%, and the likelihood that two stations will be available is 99.7%. Dual coverage is planned for the continental U.S. and in the transportation corridors in Alaska. Pseudorange and range rate corrections will be transmitted at a rate of one set every 2.5 seconds or better.

Positive Train Control

Positive train control (PTC) systems are integrated command, control, communications, and information systems for controlling train movements with safety, precision, and efficiency. PTC systems will improve railroad safety by preventing collisions between trains, casualties to roadway workers and damage to their equipment, and overspeed accidents [18]. PTC systems are comprised of digital data link communications networks, continuous and accurate positioning systems such as GPS/NDGPS, on-board computers on locomotives and maintenance-of-way equipment, in-cab displays, throttle-brake interfaces on locomotives, wayside interface units at switches and wayside detectors, and control center computers and displays.

PTC systems would provide the collision prevention and speed control benefits of traditional Automatic Train Control (ATC) systems (currently in use on less than 5% of the railroad trackage in the U.S.) at a lower cost, and would also provide roadway worker protection and railroad operational efficiency benefits that cannot be obtained with ATC systems. PTC systems issue movement authorities to train and maintenance-of-way crews, track the location of trains and maintenance-of-way vehicles, have the ability to intervene to prevent any violations of the movement authorities, and continually update operating data systems with information on the location of trains, locomotives, cars, and crews. In addition to reducing the probability of collisions and overspeed accidents by two orders of magnitude, PTC systems will also enable a railroad to run scheduled operations and provide improved running time, greater running time reliability, higher asset utilization, and greater track capacity. Pilot versions of PTC were successfully tested a decade ago, but the systems were never deployed on a wide scale as railroad management elected to invest capital in mergers and acquisitions rather than technology. Other PTC demonstration projects are currently in development and testing stages. Deployment of PTC on railroads is expected to begin in earnest later this decade.

The Federal Railroad Administration (FRA) strongly supports development and implementation of communication-based positive train control systems. According to a recent report to Congress [19], "Over a recent 7-year period, railroads experienced at least 876 collisions and other accidents that a fully implemented communications-based PTC system would probably have prevented. The National Transportation Safety Board (NTSB) has listed PTC as one on its 10 "Most Wanted" initiatives for national transportation safety." In a letter on positive train control to Class I Railroad CEOs [20], the former FRA Administrator stated, "Collisions between trains represent the single major category to train accidents responsible for fatal injury."

PTC systems currently under development are being designed to use GPS and NDGPS signals as the principal but not the sole source of positioning information. PTC systems also use calibrated tachometers on locomotives and maintenance-of-way vehicles, digital maps in on-board and control center computers, and wayside interface units that provide switch position indication. Some PTC systems also include inertial sensors. As a result of this redundancy, train and maintenance-of-way vehicle location and speed information can still be provided through tunnels and at other locations and in other circumstances where GPS signals might be disrupted. An earlier version of PTC used transponders mounted on crossties between the rails to calibrate the tachometers, but GPS/NDGPS has the advantage of lower equipment and maintenance costs.

Intelligent Transportation Systems (ITS) for roadways will interact with PTC systems at Highway-Rail Intersections (HRIs). According to [18], "Of the 6,262 United States railroad accidents in 1997, 3,865 occurred at highway-rail grade crossings[6]. These are the largest category of potentially preventable accidents that exist within the railroad industry." Information about train presence and arrival times, generated either by a PTC system or track circuits or off-track sensors, can be provided to highway traffic control centers via the digital data link communications network and to motor vehicle operators via roadside traffic information signs or via dedicated short-range radios to in-vehicle displays or audio warning systems. Similarly, sensors at HRIs will send information to railroad control centers and trains over the PTC data link communications should an HRI be blocked by a stalled vehicle. An architecture for HRIs was developed as part of the ITS National Architectures, and work on the development of standards for intelligent grade crossing has begun ton insure that there will be national interoperability.

GPS Standard Positioning Service signals are being used by railroads for a number of non-train-control, non-safety-critical applications [21]. Railroads are using GPS/DGPS to develop precise maps of their tracks and yards. Commuter railroads, such as Virginia Railway Express in the Virginia suburbs of Washington, DC, Tri-Rail between Miami and Fort Lauderdale, and West Coast Express in Vancouver, BC use GPS to generate train location information for travelers' advisory systems. The train location information gets passed on to customers with dynamics message signs at stations and with maps on the Internet [22]. CSX is using GPS to track the location of their locomotive fleet. Some non-railroad owners of freight cars (for example, First Union) and some shippers (for example, FMC) are equipping their cars and shipments with GPS receivers and cellular telephones to provide car location information directly, bypassing the railroads' information systems. Railroads and the FRA are using GPS/NDGPS on track

[6] Source: Annual Report 1997 Railroad Safety Statistics. This number includes train accidents (including highway-rail crossing) and highway-rail incidents.

inspection cars to pinpoint the exact location of track geometry and rail integrity anomalies. Table 2-7 provides requirements for railroad navigation and positioning. These are based on a 1994 Department of Commerce report to the Secretary of Transportation [23].

Table 2-7. Railroad Navigation and Positioning Requirements

Railroad Application	Accuracy (2drms)	Time to Alarm	Availability	Coverage Area
Train Position Tracking	10-30 meters	5 sec	99.7%	Nationwide
Speed Determination	±1 km/hour for speeds <20 km/hour ±5% for speeds ≥ 20 km/hour	5 sec	99.7%	Nationwide
Train Control	1 meter	< 5 sec	100%	Nationwide
Automated Road Vehicle Warning at Railroad/Road Grade Crossings	1 meter	< 5 sec	100%	Nationwide

Intelligent Transportation Systems (ITS)

In the DOT Intelligent Transportation Systems (ITS) architecture [8], GPS navigation and positioning techniques are used both in autonomous vehicles and in vehicles wirelessly linked to central travel management facilities. DOT and local transportation departments are conducting tests on integrated traffic control and emergency response techniques that rely on GPS data. Various GPS-based, autonomous navigation products are available on the commercial market and incorporated in some new automobiles. Utilization of these systems is expected to increase rapidly. Vehicle location and dispatch for emergency service, motorist mayday services, route navigation for private and rental automobiles, transit fleet management, and tracking and scheduling of commercial shipments are already in use. The integrated systems being tested involve a central traffic control center that receives GPS data from individual vehicles by wireless link. The control center uses the data for optimizing traffic flow through route guidance, locating distressed motorists, mass transit scheduling, and coordinating emergency response.

Emergency Response

The Emergency Response group of ITS services includes emergency notification and response management. Response management services consist of coordinated response and best route. The emergency notification service envisions vehicles will be equipped with a wireless link that either autonomously or upon activation alerts emergency responders of a crash, medical emergency, or breakdown. The data link provides the incident location and information on the scope of the emergency. Coordinated response is designed to alert, allocate, and guide the required police, emergency medical teams, hazmat response, and road clearing crews to a serious incident. The first responder distributes pertinent incident information including position to all

other respondents via a data link from their vehicle, allowing the subsequent arrivals to begin immediately coordinated action without having to assess the situation individually. The Federal Highway Administration (FHWA) and the Department of Justice (DOJ) currently are testing such coordinated response at several Advanced Law Enforcement and Response Technology (ALERT) test beds. The ALERT vehicle provides the incident position from a GPS receiver through a Cellular Digital Packet Data (CDPD) data link. The best route service gives the responders the best route based on the reported incident position, traffic conditions, and signal control capabilities. The location/timing use of GPS in the E-911 system is discussed in Section 2.2.4.

Advanced Vehicle Control and Safety Systems

Most of the services in the ITS Advanced Vehicle Control and Safety Systems group have not been implemented, but ongoing research may lead to deployment of at least some elements in the near future. The services include autonomous vehicle operation and collision avoidance. Autonomous vehicle operation (despite the name) involves centralized control of all vehicles on a section of roadway. Upon entering these areas, the vehicle driver relinquishes control to the service. The central control receives, via a wireless link, status and position information from all vehicles under its control and transmits back control instructions. Collision control architectures are either self-contained systems that use sensors (that is, low power radar) to detect the separation between adjacent vehicles or systems that coordinate multiple vehicles depending on self-reported vehicle positions. The systems can advise drivers to take action or automatically initiate evasive action.

Travel Management

This user service includes autonomous and centralized driver routing. Autonomous routing is provided by a self-contained, on-board GPS-based navigation and map-matching system that provides directions to the user. A centralized routing system requires a wireless link between the vehicle GPS receiver/mapping system and the central (or regional) control station. The drivers are provided directions to their destination based on the vehicles GPS position and the traffic situation on monitored roads. This centralized system also can be used for traffic control through traffic routing, and sign and signal control.

Fleet Management

This group of user services includes transit fleet/traffic management, en route transit information, and security/emergency response. In transit fleet management, a centralized control center monitors the position of all transit vehicles to identify delays and other service problems, monitors vehicle usage, and commands vehicle operators to modify their routes or schedule. A wireless communications link is required between the central control and the vehicles. The en route transit-information user service provides the traveler with real-time status on connecting and alternative transit service. The security/emergency response service provides mayday functionality to the vehicle operator. Alarm information, including the vehicle, position is wirelessly linked to the central control center that dispatches the appropriate emergency response to the vehicle.

The group of ITS services for commercial vehicles includes fleet tracking and management, cargo tracking, hazardous material (hazmat) vehicle location, and hazmat incident response. All require vehicle positions to be determined locally, and wirelessly linked to a central operations center. Commercial fleet tracking and management is similar to transit fleet tracking and management. Cargo tracking can be important when it involves priority shipments such as organs and medicine, or is required for "just-in-time" manufacturing. The positions and contents of hazmat shipments are monitored in real time, and, if required, coordinated emergency response is routed to those positions.

Navigation Requirements

In the 1999 Federal Radionavigation Plan [7] tabulated the requirements for various functions in the ITS architecture. The required system time-to-alarm varies from 1 to 15 seconds depending on the specific implementation scheme. The integrity requirement for transit systems is still to be determined.

The availability requirement for highways and transit systems is 99.7%. This translates to 26.3 outage hours per year, or about a half-hour outage per week. For perspective, the service availability of the GPS is observed to be 99.9% on a global basis on any given day [24]. The 95% accuracy requirements for some ITS functions are shown in Table 2-8.

Table 2-8. ITS Navigation System Accuracy Needs/Requirements [7]

Mode	Accuracy (meters) 95%
Highways	
Navigation and Route Guidance	5-20
Automated Vehicle Monitoring	30
Automated Vehicle Identification	30
Public Safety	10
Resource Management	30
Accident or Emergency Response	30
Collision Avoidance	1
Geophysical Survey	5
Geodetic Control	<1
Transit	
Vehicle Command and Control	30-50
Automated Voice Bus Stop Annunciation	5 (25-30 meters before bus stop)
Emergency Response	75-100
Data Collection	5

2.2.4 GPS AS A TIMING SOURCE

The use of GPS in the telecommunications industry has increased to the point where it plays a critical role for timing and synchronization. It is now the most frequently selected method for precise synchronization [4]. Examples of its use and planned use for critical timing and synchronization include global fiber networks (SDH and SONET) and the global wireless networks (PCS, GSM, TDMA, CDMA, and Wideband CDMA) [5]. The importance of reliable communications to transportation and public safety is pointed out by Butterline and Frodge [5], who note that "GSM wireless and CDMA wireless communications, enhanced emergency

service (E-911), digitized video services distribution, telemedicine, video conferencing are all services which are corrupted or lost completely if the primary reference source to telecommunications synchronization is lost, unavailable, or corrupted."

Recent legislation on E-911 mandates "automatic location broadcast" when the wireless service is used[7]. GPS is the logical source of the location information, and the users are subject to its vulnerabilities (sometimes a safety-of-life issue). Table 2-9 reproduces the timing requirements for communication network synchronization from the 1999 Federal Radionavigation Plan [7].

Table 2-9. Communication Networks Synchronization Requirements

ITS-Associated Communication Networks Synchronization	
Repeatable Accuracy	1 part in 10^{-10} (freq)
Availability	99.7%
Fix Interval	Continuous
Coverage	Nationwide
System Capacity	Unlimited

Standards

The American National Standards Institute (ANSI) accredited T1 standard hierarchy for clocks is given in Table 2-10.

As pointed out in [5], "Only Stratum 1 clocks are completely autonomous. All other clocks must be dependent upon a higher Stratum clock for their timing reference." Lower level clocks must be traceable to a Stratum 1 clock as the Primary Reference Source (PRS) for timing synchronization. GPS is increasingly being used for a Primary Reference Source (a Stratum 1 clock) within a given telecommunications network because it is much cheaper than using cesium clocks.

Table 2-10. The ANSI T1 Standard Hierarchy of Clocks [5]

Stratum	Accuracy	Holdover Stability	Technology
1	1.0×10^{-11}	N/A	GPS/Cesium/Loran
2	1.6×10^{-8}	1.0×10^{-10} per day	Rubidium
3E	4.6×10^{-6}	1.0×10^{-8} per day	Quartz
3	4.6×10^{-6}	3.7×10^{-7} per day	Quartz
4E	3.2×10^{-5}	Not required	Quartz
4	3.2×10^{-5}	Not required	Quartz

Within a telecommunications central office, GPS is used to discipline duplicate rubidium or, in some cases, high performance quartz oscillators. These oscillators provide buffering and isolation between GPS and network timing. As pointed out in [5], "In the event of a GPS signal degradation or interruption, these oscillators will maintain the synchronization quality of the

[7] The Wireless Communications and Public Safety Act of 1999 (October 26). Most states have legislation passed or pending.

telephone network at the ANSI and ITU-T interface standard of $1x10^{-11}$. They will continue to meet this holdover quality for a week to one month, depending on the design parameters used."

The use of GPS for telecommunications synchronization increased significantly with the advent of the Synchronous Optical Network (SONET) employed by most major carriers. SONET uses a ring network configuration (unlike the star configuration used previously by most networks), which allows the network to be self-healing when the ring is broken. Because the self-healing feature only applies to transmission of the payload data and not to synchronization, carriers have created PRS-quality synchronization using GPS at every node on the ring [5].

Deployment of Loran-C and GPS for network synchronization began in the late 1980s and GPS is now the preferred choice because of the accuracy, economy and a long-term commitment of the U.S. Government to system life [5]. As pointed out in [5], "The price of a good GPS timing unit is well under $10K and continues to fall; a good cesium standard is in the $40-60K range."

GPS is currently used as a distributed timing source in large power networks. Conversations with industry representatives indicate that GPS is not critical to safe system operation and they see no need for Loran as a backup to GPS. See [7,25] for an overview of the use of GPS in the power industry.

Digital communications and data links are becoming critical to NAS operations. The FAA currently is using or evaluating the following digital communications systems and links:

- VHF Data Link Mode 2 (VDL-2) utilizes VHF communications frequencies (118-137 MHz band). VDL-2 will offered by ARINC as a commercial service (successor to the Aircraft Communication and Reporting System (ACARS)), and will be installed on most air carrier aircraft. VDL-2 is sometimes referred to as Controller Pilot Data Link Communications (CPDLC), a service based upon VDL-2.

- VHF Data Link Mode 3 (VDL-3) is being implemented by the FAA Next Generation Communication System (NEXCOM) program as the replacement for current VHF voice radios. VDL-3 carries both voice and data, with each ground-station radio providing simultaneously connectivity of up to four sectors worth of aircraft over a single 25 kHz channel using time-division multiple-access technology.

- VHF Data Link Mode 4 (VDL-4) was developed in Europe for air-to-air and air-to-ground transmission of ADS-B data and other data, using one or more 25-kHz VHF channels. In operational service, it is likely that dedicated/worldwide channels would have to be employed. VDL-4 is one of the data links being considered by the FAA for ADS-B, and is being tested by the SafeFlight 21 program.

- Universal Access Transponder (UAT) was developed in the U.S. for air-to-air and air-to-ground transmission of ADS-B data and other data using a carrier frequency near 1000 MHz in the TACAN/DME band (960-1215 MHz). Owing to its wider bandwidth, UAT data rate is significantly higher than those of the VHF data links. UAT is one of the data links being

considered by the FAA for ADS-B, and is being tested at 966 MHz by the SafeFlight 21 program.

- Mode S data link uses the secondary surveillance radar response frequency (1090 MHz), waveforms, and message formats for air-to-air and air-to-ground transmission of ADS-B and other data. Mode S is one of the data links being considered by the FAA for ADS-B, and is being tested by the SafeFlight 21 program.

The planned NEXCOM (using VDL Mode 3), VDL Mode 4, and UAT rely on GPS in varying degrees to provide precise timing for synchronizing message transmissions.

Finally, the maritime AIS standard is being established as a critical tracking, navigation and communications system for U.S. and international waterways and ports. Its use is mandated for most classes of commercial vessels. AIS relies on GPS (making AIS users vulnerable to degradation or loss of GPS) as a source of the timing of SOTDMA transmissions.

2.2.5 CRITICAL APPLICATIONS

The Volpe Center assessment of modal GPS applications resulted in selection of the following critical applications (see also Table 5-1 in Section 5.4):

Aviation:	Precision and nonprecision approaches
Marine:	Harbor, harbor approach and constricted waterways
Surface:	ITS hazmat and emergency response operations
Communications:	Timing and synchronization

Chapter 5 provides further detail on this selection. For example, critical timing services can be maintained safely from days to several weeks following loss of GPS. Thus, only the extremely unlikely event of damage to a large number of GPS satellites could precipitate a “critical” situation for those communications networks that may lack a timing alternative to GPS. Since not all networks today that rely on Stratum 1 clocks such as GPS have an adequate backup, however, these timing uses of GPS probably should remain classified as critical applications.

(This page deliberately left blank)

3 ASSESSMENT OF GPS VULNERABILITIES

This chapter presents a summary of the vulnerabilities of GPS to disruption and loss. More complete descriptions of these vulnerabilities are contained in Appendices A and B.

The mechanisms to disrupt GPS can be divided into unintentional or intentional disruptions. Unintentional mechanisms include ionospheric effects, interference from other RF emitters, and signal blockage. Intentional disruption mechanisms include jamming, spoofing, meaconing,[8] and deliberate efforts to shut down GPS operation. The potential for denying GPS service by jamming exists. Loss of GPS satellites or the Operational Control Segment could also impact GPS service for long periods, but attacking these elements can be more challenging and likely would produce a more aggressive U.S. Government response than jamming GPS users.

Human errors in the GPS equipment design, system operation, and among users also could threaten safety. Although in most cases a person in the loop is an additional safety factor, human factors can contribute to a problem if there is a lack of understanding of the limitations and vulnerabilities of GPS navigation.

3.1 GPS VULNERABILITIES TO UNINTENTIONAL DISRUPTION

There are numerous causes for unintentional interference or disruption of GPS. These are briefly discussed below, followed by an assessment of the GPS vulnerabilities in the aviation, maritime, and surface environments.

The primary signal characteristic that makes GPS vulnerable is the low power of the signal. A receiver can lose lock on a satellite due to an interfering signal that is only a few orders of magnitude stronger than the minimum received GPS signal strength (10^{-16} watt, equivalently -160 dBw, at the Earth's surface for the L1 C/A code [26]). In addition, a receiver attempting to acquire lock on a GPS signal requires 6 to 10 dB more carrier-to-noise margin than is required for tracking [27].

3.1.1 IONOSPHERIC INTERFERENCE

The ionosphere surrounding the earth at approximately 350 km altitude (F layer) can refract the L band signals of GPS. Small-scale electron density fluctuations can diffract the signal into a pattern of amplitude and phase variations that moves across the surface of the earth. This effect is called scintillation. The resulting group delay is a very important factor in ionospheric GPS interference. Because group delay is, to a first order, inversely proportional to frequency squared, it can be virtually eliminated with a dual-frequency receiver such as one that processes either L2 or L5 in addition to L1.

The range errors can be up to 20 meters for single frequency receivers during solar events such as flares but dual frequency receivers (L2 semi-codeless tracking) can measure and remove these errors. In susceptible areas near the poles and equator, differential correction accuracy may be reduced due to the rapid fluctuation in the ionosphere.

[8] Meaconing is the reception, delay, and rebroadcast of radionavigation signals to confuse a navigation system or user. It is discussed further in this section, under the heading "Deceptive Jamming (Spoofing) and Meaconing."

In addition, the ionosphere can form small scale diffraction gratings that cause signal fading and phase changes, which have their worst effects at the poles and near the ±15 degree latitudes. Fading is particularly a problem for L2 semi-codeless tracking because it does not get the full gain from code correlation in the receiver so its tracking is more tenuous. Scintillation can cause rapid changes in signal phase that can exceed the receiver's tracking loop dynamic capability causing loss of lock. This can affect both L1 and L2 tracking in the susceptible regions mentioned above and is worse in the evening hours before midnight.

3.1.2 UNINTENTIONAL RADIO FREQUENCY (RF) INTERFERENCE

There are concerns about interference from RF transmitters that may produce unwanted signal power in the L1 band. The current systems of concern have been distilled down to mobile and fixed VHF, television channels 23, 66, and 67, the Mobile Satellite Service (MSS), and Ultra Wideband (UWB) communications, over-the-horizon (OTH) radar and personal electronic devices (PEDs) such as cell phones carried on board vehicles and vessels. L2 may experience more interference because the frequency is in a band where radar systems have co-primary allocation, and does not enjoy the same protection for aeronautical safety-of-life applications as the L1 and L5 bands. The extent of L2 vulnerability vis-à-vis L1 and L5, which are allocated to the Aeronautical Radionavigation Service (ARNS), may depend on the degree the bands are monitored and protected for their primary uses by ITU member nations.

The proposed new L5 civil signal at 1176.45 MHz, allocated to Aeronautical Radionavigation Service (ARNS), partially overlaps the frequency band allocated to the military Joint Tactical Information Distribution System (JTIDS) and the Multi-Functional Information Distribution System (MIDS). JTIDS/MIDS and L5 have co-primary allocation. L5will be 6 dB stronger than L1 (1575.42 MHz), which is allocated to the ARNS and the Radionavigation Satellite Service (RNSS) band.

Other satnav systems, such as the proposed Galileo system, may generate unwanted RFI if desired coordination with the GPS policy makers fails to materialize.

Broadcast Television. Interference from TV signals has been observed in at least one case [28]. The best option for minimizing occurrences would appear to be through tightened FCC harmonic/spurious radiation limits, education of TV engineers to maximize voluntary compliance, and enhanced enforcement. Also, all users should be encouraged and instructed to report interference incidents. These efforts should start now, as most stations are not presently transmitting the maximum allowed harmonic power levels. That may change with the arrival of widespread digital TV (DTV), which employs an entirely different signal. Even if these steps were taken, it would be difficult to correct a malfunctioning transmitter within the initial two hours of disruption. The FCC has imposed spurious and harmonic limits on DTV which should, if enforced, protect the use of GPS in aircraft.

VHF Interference. A study conducted by Johns Hopkins University (JHU) [6] indicated that mobile and fixed VHF transmitters might interfere with GPS receivers at ground level as far away as 3.5 and 5.5 nautical miles, respectively. Although there have been reports of interfering signals that have not been identified, there are no confirmed reports of VHF interference from

ground-based transmitters to be found in the literature, despite the use of VHF transmitters and GPS for a decade. This observation does not apply to on-board aircraft equipment. Transmissions from on-board VHF communications equipment have caused significant interference with GPS signal reception. However, this can be managed during GPS installation through the use of an appropriate in-line filter at the transceiver antenna connector [29].

During development of RTCA document DO-247 [15], RTCA SC-159 examined the potential effects of radio frequency interference (RFI) on use of GPS for airport surface applications. The committee first examined those systems that are unique to the airport surface environment and were not included in the previous RTCA SC-159 evaluation of GPS interference described in RTCA DO-235 [30]. The results of the RTCA analysis indicate that there are no RFI concerns from these systems.

Airport surveillance radar, Mode S, and DME do not have harmonics at GPS L1 frequency and therefore do not present an interference concern to GPS. Airport operational service vehicles carry at least one VHF radio for ground control purposes. Emergency vehicles also may carry FM transceivers to monitor the frequencies of local police and fire departments. This equipment can operate near or on the 9^{th} and 10^{th} subharmonics of L1.

Personal Electronic Devices. PEDs include devices such as cellular telephones and two-way pagers, that can cause disruption of GPS signal reception.

Over the Horizon Radar. The JHU report also suggested that more study be done on OTH radar because of the limited public information on such systems. They suggest the threat is minimal due to the small number of these radars and their small beam widths.

Mobile Satellite Service (MSS). Mobile Satellite Service (MSS) communications systems pose two distinct interference threats to the GPS L1 signal. Handheld MSS Mobile Earth Stations (MESs), transmitting in the 1610-1660.5 MHz band, can introduce wideband power in the GPS band, raising the noise level. A compromise has been reached whereby the emissions of a single MSS MES device are limited so that they cannot disrupt GPS aviation receivers. However, concern remains that multiple MSS MESs could cluster in an area (for example, on a highway beneath the approach to a runway or on a beach) and disrupt GPS in aviation, marine and surface vehicles.

Another potential source of GPS interference are the spurious and harmonic emissions from geostationary satellites that transmit in the 1525-1559 MHz band. To date, these emissions are unregulated by the ITU. The two leading U.S. MSS vendors, Iridium and Global Star, are having financial difficulties and their future is in doubt. However, market conditions may change and other vendors may enter the market.

A recent proposal to place MSS space-to-earth transmissions in the 1559-1567 MHz band adjacent to L1 presented a potential threat to GPS signals and a significant threat to its growth. Satellite emissions could interfere with the WAAS geostationary satellite signal which has a 1 dB weaker signal than GPS satellites. This proposal was defeated at the June 2000 World Radiocommunication Conference (WRC).

Ultra Wideband Radar and Communications. Ultra wideband (UWB) radar and communications systems generate extremely short pulses that produces a low power signal with a very wide

bandwidth (0 – 3 GHz according to one vendor). If the pulse transmit times are not sufficiently randomized, there may also be spikes in UWB device output spectra. For many narrowband systems, the average amount of power in their spectrum from a wideband system is negligible. , Because the GPS signal power is so small, however, GPS operation may be affected. Initial tests sponsored by the DOT and NTIA have shown that UWB can disrupt GPS and cause loss of lock. NTIA currently is performing additional UWB-GPS testing to quantify the effects of many different UWB system characteristics (duration, repetition rate, etc) produced by different electronic designs and antennas [31]. The FCC has yet to rule on whether to establish criteria that permit the operation of low-power UWB devices without license or the need for frequency coordination, pending a review of the upcoming test results.

3.1.3 HUMAN FACTORS IN THE USE OF GPS

The human factors impact on the GPS system, equipment and users also could threaten safety. Although in most cases a person in the loop is an additional safety factor, human factors can contribute to a problem if there is a lack of user understanding of the limitations and vulnerabilities of GPS navigation. Most of the accidents to date involving use of GPS have been traced to human factors. The National Transportation Safety Board (NTSB) has reported use of non-differential GPS for altitude information resulting in pilots crashing into terrain, pilots programming handheld receivers in flight resulting in accidents, and loss of battery power on handheld GPS receivers also causing accidents [32].

A recent paper presented by NASA at the Ohio State Symposium on Aviation Psychology [33] suggested that pilots are more likely to take greater poor weather risks when the airplane is equipped with a GPS than when only older navigational instruments (for example, VOR, ADF) are available. The NASA Aviation Safety Reporting System (ASRS) database [34] also provides numerous accounts of pilots traveling into restricted airspace while using GPS since it gives them the flexibility to not have to fly the traditional route structure. The database also provides descriptions of pilots experiencing trouble with GPS receivers when using a different manufacturer's GPS receiver other than the one to which they are accustomed.

Human factors problems with GPS have been experienced in maritime applications as well. The Royal Majesty incident that occurred off the coast of Massachusetts in June 1995 very likely epitomizes the role of several prominent human factors elements. These include: lack of adequate training, over-reliance on a single navigation system, failure to recognize that the primary (GPS) system was not working properly, system design deficiencies, and failure to check information by using any one of several working supplemental systems. The incident also is representative of many maritime adverse events in that while there was relatively little physical risk to the humans involved, there did result substantial inconvenience and financial cost [35].

There are other examples, including thousands of receivers in Japanese car navigation systems that failed because they were not designed properly to ignore ephemeris data from satellites broadcasting non-standard code. In many cases, a flaw in a casual user's receiver will be compounded by their lack of knowledge of GPS principles.

Human factors may represent the single largest risk to GPS use from a multi-modal perspective. The unfortunate motorist who followed his car navigation system instructions faithfully and drove into a river is another example. There is a need for training to recognize non-standard GPS performance, and to be able to initiate backup procedures.

Human factors in the GPS system operation, GPS equipment design, and among GPS users also could threaten safety. A mistake in uploading data to the satellites apparently has a very low probability, given the excellent record of the GPS Operational Control Segment[9], but it is a remote possibility. Bad satellite orbit positions would result in bad receiver positions unless differential corrections are applied. Satellite design flaws also are possible but will probably continue to be a rarity. A satellite design flaw has been documented in the block IIR satellites that cause the ranging code to be interrupted for a few seconds when new data are uploaded.

See Appendix A for more human factors detail.

3.2 GPS VULNERABILITIES TO INTENTIONAL DISRUPTION

The accelerating military dependence on GPS worldwide makes mechanisms to disrupt the signals potent weapons that many militarily sophisticated countries are actively developing. The U.S. and its allies can use the encrypted P(Y) code for better accuracy and integrity, but to acquire that code, most military receivers still must track the C/A code first [36]. Potential adversaries and the global civil community have access only to the C/A code. Y-code jammers typically would also be effective against C/A code.

The U.S. military has a policy to deny foreign adversaries the use of GPS and its augmentations in a conflict while preserving its utility to U.S. forces, and without unduly disrupting or degrading civilian uses outside the area of conflict. The effort to develop GPS disruption systems for this purpose, and to protect allied forces from GPS disruption is called NAVWAR [7]. Since P(Y) code is encrypted, potential adversaries will be using the C/A code, making it a target for localized disruption. Other countries are reported to be developing similar capabilities. NAVWAR testing may impact civil use of GPS in the U.S., but DoD and DOT have developed mechanisms to coordinate times and places for testing, and will notify users in advance [7].

Some jamming devices/techniques are available on the Internet and proliferation will continue, because a single device that could disrupt military and civil operations worldwide would be attractive to malicious governments and groups. Civil GPS applications may be either innocent bystanders or the intended target. In either case, the mechanisms, potential effects, detection observables, and available mitigation equipment and techniques must be completely known to the civilian community, so that vital and safety-of-life applications can be prepared properly. Most if not all of the severe consequences of deliberate disruption of the GPS service can be offset by judicious planning. This will include use of backup systems and/or procedures in critical applications. User training also will be important.

In addition, unintentional or natural disruptions such as produced by the ionosphere or unintentional RF interference could be used by saboteurs to disguise their intentional disruption efforts, at least to delay government response and warning. In fact, users warned of the

[9] As of this writing, such an error apparently has never happened.

likelihood of imminent natural disruptions would be more likely to dismiss observed anomalies as harmless when they may not be harmless.

3.2.1 SHUTDOWN

The Rumsfeld report publicly recognizes the potential for a significant attack against the U.S. military technology infrastructure in space, that includes intelligence, communications, and GPS navigation satellites ([2], page 23). The heightened awareness of this type of threat may help to ensure that future planning addresses the potential, however unlikely it seems today, "..for the GPS system to experience widespread failure or disruption [2]." The report states that "An attack on elements of U.S. space systems during a crisis or conflict should not be considered an improbable act. ... National leaders must assure that the vulnerability of the United States is reduced and that the consequences of a surprise attack on U.S. space assets are limited in their effect."

This type of attack could include the GPS system as a target. However, to have a significant effect on the GPS system performance many satellites must be damaged. The GPS satellites, furthermore, are at relatively high altitudes compared to some reconnaissance satellites, which would be easier targets. Also, any action to destroy U.S. satellites may be an act of war that would produce an aggressive U.S. response. Nevertheless, the potential exists for crippling many individual satellites and/or damaging the Operational Control Segment. Either action could cause a long-term outage of GPS that would significantly disrupt GPS service. The U.S. military, cognizant of the system limitations, is taking steps to harden its GPS dependent systems against the threat.

Although the likelihood that these events actually will occur is very small, the severe consequences merit an awareness of the potential threat. In addition, this threat will increase in importance over the next several years as critical modal applications such as aviation are expected to replace current navigation aids with augmented GPS as the primary navigation system [37]. This future critical role will add to the desirability of GPS as a target for hostile action.

3.2.2 JAMMING, SPOOFING, AND MEACONING

Jamming. Intentional interference or jamming of GPS is the emission of radio frequency energy of sufficient power and with the proper characteristics to prevent receivers in the target area from tracking the GPS signals.

It is well known within the military GPS community that the SPS can be jammed over a significant area by an airborne, low power jammer (1 watt). It is estimated that when airborne, such a jammer can deny GPS tracking to an already locked receiver at 10 km, and prevent it from acquiring lock at a range of 85 km [38,39]. It is estimated that a 1 watt spoofer could result in the loss of GPS signal acquisition for all satellites to the horizon (approximately 350 km) [39]. The exact distance and required jamming power depend on the type of jamming signal (CW, wideband, etc.), the altitude of the jammer, GPS antenna pattern, geometry between the GPS antenna and the jammer, body masking loss, and receiver design. It is very difficult to deny aircraft approaches over a large area with a single ground-based jammer because the

horizon/terrain blockage acts as a limiter. Multiple low-powered or airborne (balloon or aircraft) jammers can, however, be used to overcome this limitation.

If jammers are made with some sophistication, so that the jamming signal has the same type of spread spectrum as GPS, the same power results in a dramatically increased denial range. A one watt GPS-like signal can prevent C/A code acquisition to more than 620 miles (or as limited by the line-of-sight to the horizon). The jamming signals can be generated with relatively low cost equipment [40]. The vulnerability of the GPS system to this type of 'GPS-like' RFI can be a potentially serious threat. This type of interferer will deny the GPS spread spectrum de-spreading processing gain, and will be extremely difficult to detect by conventional methods such as spectrum analysis.

GPS jammers exist in a variety of sizes and output power levels. Small, lightweight, short-lived jammers with power from 1 to 100 watts can cost less than $1,000. These jammers can be built by people with basic technical competence from readily available commercial components and publicly available information.

Jammers borne by an SUV can emit between 100 and 1,000 watts and cost on the order of $100K. Airborne or truck borne, high-power jammers can produce jamming power in the range of 10 kW to more than 100 kW, but cost a million dollars or more. The high-end jammers can produce a variety of waveforms that enhance their effectiveness. The director of a U.S. military GPS testing program recently stated that there are many models of foreign military equipment that easily could be converted into megawatt GPS jammers.

At the other end of this threat spectrum is the potential for large numbers of mass-produced, low cost, and lower power jammers. Factories in foreign countries that are currently producing consumer products can easily be modified to produce thousands of jammers per day. Hundreds could be distributed in single area of GPS denial.

For a small noise jammer, the biggest limitation is power. Operation of a 1 watt GPS jammer for 12 hours would require about 2.1 lbs. of alkaline batteries or 1 lb. of lithium batteries. A ten watt jammer requires ten times more batteries by weight to operate for the same 12 hours. Some commercially available gasoline generators weighing about 30 pounds can operate an 80 watt jammer for five hours on one gallon of gas.

The most disturbing reports on the effect of jamming involve inaccurate position determination provided by receivers under jamming. Several tests of GPS receivers, aviation certified and uncertified, have shown that jamming can induce large range errors [41,42]. This range distortion usually occurs just before loss of lock, and the receiver tracking flag (if present) may not indicate a problem. Winer et al [41] give an example of a certified receiver tested in the lab with a CW jamming signal. As the interference level reached the receiver tracking threshold, the position error rose to 1,000 feet before the receiver lost lock and its tracking flag changed states. Ten seconds later, still under jamming, the tracking flag reverted to valid, and navigation solutions with a 2,000 foot error were output over approximately twenty seconds. These anomalies are not due to GPS deficiencies, but to receiver design limitations. The aviation

receivers tested by Winer et al [41] were operating in the en route and terminal modes. A 2,000 foot error is within the limits of these modes.

Other applications may have more stringent requirements. Moreover, Receiver Autonomous Integrity Monitoring (RAIM) used in aviation should be effective in detecting excessive position errors and should be considered for other applications. RAIM already is nearing implementation in maritime transportation, as the IEC is addressing both RAIM and GPS susceptibility to RFI in the maritime environment.

Once jamming stops, some receivers recover immediately. Others can take from a few seconds to two minutes to recover and begin generating good solutions. Some receivers do not recover until the power is cycled [43]. The variety in recovery behavior reflects the variety in receiver design. Immediate recovery is much more likely when using a well-designed, properly certified receiver.

These anomalous and non-uniform receiver responses increase the importance of testing GPS receivers for the critical applications, to determine their response to jamming as part of their certification. A standard flag indicating jamming conditions or loss of lock should be defined and required on all of these receivers. User displays also should provide for the indicator. Unless an unambiguous, high integrity jamming or lock indicator on the receiver is present in conjunction with training, backup procedures, and backup equipment, jamming could become an effective disruption.

Reasonable standardization is an important part of good system design. In aviation, for example, many pilots are qualified to fly different aircraft. In the manner that they expect the turn-and-bank indicator to have similar location, display, and functionality from one aircraft to another, so should they expect the same from other navigation display systems. This factor becomes more important during stressful situations such as troubleshooting failing GPS performance during a critical flight phase.

The military testing additionally indicated that jamming had greater systemic effects than would have been expected from just the loss of positioning. Unexpectedly, communications systems were shut down because they depend on GPS for timing. There also have been reports of commercial cellular networks being disabled by open air GPS jamming.

An important human factors result of U.S. Government tests was the observed responses of troops under jamming conditions. Some units turned off their receivers at the mere possibility of jamming, disregarding still valid navigation information. Even in the actual presence of jamming, techniques such as seeking terrain or vehicles to mask the jamming could have been used to get a valid position. GPS jamming significantly confused command and control functions, and complicated planning. Authoritative reports state that GPS disruption caused a convoy of helicopters to ignore obvious visual cues, and fly off in the direction indicated by an inaccurate GPS receiver. These actions by soldiers aware of possible GPS disruptions illustrate the importance of training to recognize jamming and to implement backup procedures immediately.

MDGPS, the maritime DGPS augmentation service in U. S. waterways uses radiobeacons to transmit differential correction signals. The radiobeacon broadcast frequency, power, and antenna sizes are expected to inhibit deliberate attempts to jam MDGPS differential correction signals. While there is no information on comprehensive GPS vulnerability tests or assessments of MDGPS, detailed analyses of the radiobeacon system [44] give confidence in its robustness to interference. Loss of the GPS satellite signal at the MDGPS facility will of course deny the benefits of MDGPS to the user, but the system also possesses adequate integrity monitoring to detect the signal loss. There should therefore be no serious consequence to the loss of GPS for mariners (or any other user) who have backup or supplemental navigation systems and are ready to use them.

Spoofing and Meaconing. Spoofing is a technique that has long been used to deceive a radar's target-ranging operation. In the case of GPS, the intent is to cause an active GPS receiver (whether or not presently tracking GPS signals) to lock onto legitimate-appearing false signals and then be slowly walked off the desired path such that sufficient time passes prior to the discovery of the deception, thereby precluding satisfactory corrective measures. Even if not fully successful, spoofing usually will inject hazardously misleading information (HMI), create significant PVT errors, and jam large areas effectively.

Spoofing can be more difficult to achieve than jamming, and it is less likely to be used as it is often targeted to an individual user. Spoofing, however, can achieve the widespread disruption of jamming, because, while a spoofer can inject misleading data within a localized area, the PRN signal will act as a highly effective jammer over large distances. A spoofer also can defeat nearly all anti-jamming equipment.

Meaconing is the reception, delay, and rebroadcast of radionavigation signals to confuse a navigation system or user.

The WAAS, LAAS, NDGPS, and MDGPS augmentations could theoretically be spoofed since their architecture is well known. For non-GPS links, more power may be required, but the signal structure is much simpler. Meaconing would not be needed against any of the DGPS correction links except WAAS, because these links are data messages and not ranging signals. The WAAS signal could be subject to meaconing because it is a data and ranging signal. The risk of proliferation of spoofing systems for non-GPS-type signals would seem to be lower than for a GPS spoofer because, unlike the GPS spoofer, they are not effective against world wide civil and military systems. A similar argument applies to the risk of development and proliferation of devices to spoof ground-based navigation aides such as VOR/DME.

Unfortunately, given the potential risk, little publicly available information or test results exist concerning the response of commercial receivers to spoofing. It is important to identify receiver observables that may indicate spoofing. Although some of the reported DoD test results indicate successful spoofing against some civil receivers, there is no information on the magnitude of the range error induced. There also is no open information on the capabilities of military spoofing systems or the expected capabilities of spoofing systems made from commercial components. Information on the capabilities, limitations, and operational procedures would help identify vulnerable areas and detection strategies. The DOT should coordinate with the DoD to ensure

that appropriate anti-spoofing technologies are available to civilian applications, should the need arise.

In the April 2000 *Journal of Electronic Defense* (On-Line), the Washington Report describes the GPS testing in early 1999 in the Atlantic off North Carolina. It indicates "a major purpose of the effort was to find ways to protect the GPS and evaluate the vulnerability of forces to spoofing and disruption of the satellite signal." Results from other tests indicate both jamming and spoofing disruption of commercial receivers. Information about the receiver responses or capabilities and limitations of such devices is not available.

There have been official reports of foreign awareness of spoofing technology and interest in developing actual devices. No devices are known to exist at this time, but C/A code spoofers would be desirable because hostile forces could use them against the military and civil infrastructures of countries that must utilize the C/A code. A major military use for C/A code is to acquire the P(Y) code [36].

Testing under FHWA sponsorship addressed vulnerabilities to MDGPS and NDGPS correction signals. The primary conclusion of this study [44] was that jamming disruption of the data link is possible, but relatively unlikely. Spoofing of the data link was felt to be more likely, especially if the power of the spoofing signal exceeds that of the true signal at the receiver antenna.

For the maritime community, spoofing does pose a potential concern: GPS signals to the reference stations conceivably could be spoofed, and a co-located MDGPS integrity monitor will be unable to detect the spoof.

4 GPS VULNERABILITY MITIGATION STRATEGIES

Techniques that would mitigate against the range of possible threats to the GPS system and signal cover a wide range of options. Methods likely to be effective against unintentional interference may be of limited value in combating intentional interference (jamming and/or spoofing). Moreover, the degree of protection required very often is application specific. Generally, mitigation strategies will be mode- and criticality-dependent, and will involve an appropriate mix of hardware upgrades, alternate operational procedures, and independent backup systems.

As an example, aviation mitigation techniques may involve high complexity and user costs. Two techniques suggested in the JHU GPS Risk Assessment Study [6] to suppress interference effects (nulling antenna technology, and IMU integration) could place a heavy cost burden on the aircraft operator (especially, in the latter case, if the aircraft doesn't normally carry an IMU). Although efforts are underway to lower the cost of these mitigation techniques and devices, it is unclear if and when much of the general aviation aircraft fleet will be able to install these recommended devices.

The approach taken in this report is to discuss mitigation within the context of the interference class (unintentional or intentional), followed by separate discussions of mitigation requirements on a mode-specific basis. Further information is provided in Appendix B. Mitigation strategies that involve operational procedures or (for aviation) ATC intervention are discussed in Chapter 6, as those are more pertinent to mitigating the impact of losses of GPS upon the transportation infrastructure, rather than mitigating the potential for disruption of the GPS system.

4.1 MITIGATION OF UNINTENTIONAL INTERFERENCE

4.1.1 SPECTRUM MANAGEMENT AND LEGAL ACTION

Effective spectrum management is the first line of defense against unintentional interference from man-made transmissions. In addition, strict enforcement of laws that prohibit interference with GPS will further deter the "casual" interferer.

4.1.2 DETECTION AND LOCATION CAPABILITY

Interference location equipment should be fielded that rapidly identifies and locates an interference source. This should be coupled with a prompt field response to silence the interferer as quickly as possible.

4.1.3 GPS MODERNIZATION

The GPS Modernization Program [45] is expected to provide a substantial reduction in the threat from unintentional interference. There also may be some degree of threat reduction from intentional interference. Higher GPS signal power, a C/A (or replacement civil, R/C) code on L2 and a more robust civil code on L5, all combine to reduce greatly the susceptibility of civil applications of GPS to unintentional interference. The L2 and L5 signals (1,227.6 and 1,176.45 MHz respectively) are sufficiently far removed from L1 (1,575.42 MHz) that it is extremely unlikely that an unintentional interfering source would jam all three frequencies simultaneously.

The second civil signal on L2 will begin implementation on a retrofitted Block IIR satellite scheduled to be launched in 2003. As of July 2001, it is expected that this new "L2c" signal will reach Initial Operating Capability (IOC) during 2007, and Final Operating Capability (FOC) during 2011.

The third civil signal on L5 will be implemented on the GPS III satellites along with the new military M-code. The specifications for GPS III are still be finalized as of July 2001 with the Preliminary Design Review (PDR) planned for 2004, and the Critical Design Review (CDR) in 2005. GPS III development and deployment are expected to start in 2007, and the L5 signal IOC is expected in 2012, while the FOC is planned for 2014. These schedules are subject to change depending on such factors as funding and the operating life of the satellites. However, it is clear that single-frequency C/A code use will dominate civil applications into the next decade, considering the launch schedule and the still-increasing number of deployed, single frequency receivers that will have to be replaced.

4.1.4 JAM-RESISTANT USER EQUIPMENT

Techniques to improve the jam resistance of GPS receivers may be broadly classified as precorrelation and postcorrelation methods. Precorrelation methods tend to be waveform specific and include spatial processing, temporal processing and spectral processing [46] Adaptive spatial processing (beam forming or null steering) using multi-element antennas can provide from 25 to 40 dB of anti-jam (AJ) protection, and is the only precorrelation method effective against broadband interference [46]. Multi-element antennas tend to be expensive and are more appropriate to military applications. One manufacturer has, however, developed a spatial filtering technique that uses polarization discrimination and requires only a single antenna aperture. This technique, as well as spectral and temporal filtering, can be applied ahead of an existing GPS receiver and at a relatively low cost.

Postcorrelation methods include (1) addition of other sensors and (2) enhanced signal processing. Inertial aiding is often used in military applications and permits the reduction of tracking loop bandwidths thereby improving AJ performance. Additionally, an integrated GPS/inertial system can slow the rate of navigation error growth when GPS is lost.

4.2 MITIGATION OF INTENTIONAL INTERFERENCE

4.2.1 JAMMING

Additional frequencies provided by GPS Modernization may be of some effectiveness against intentional jamming. The availability of GPS ranging signals on multiple frequencies will make jamming more difficult and costly. The new frequencies will not, however, pose an insurmountable problem. Jamming multiple GPS frequencies is simplified by the integer relationship among the three frequencies.

The signal characteristics of L5 make jamming it considerably more difficult (although still feasible). The 6 dB higher signal power is effective against all types of interferers and cuts the jamming distance in half. The higher chipping rate and longer code are effective against CW jammers, reducing susceptibility to them to be about the same as to wideband interference. As

much as 16 dB more jamming power would be needed to jam successfully a receiver using all three civil frequencies.

A second significant difference between unintentional interference and intentional jamming is that the latter may involve multiple sources. Temporal and spectral filtering can be effective against multiple narrowband jammers, but spatial filtering is the only precorrelation method effective against broadband jammers. Postcorrelation methods of dealing with wideband interference may have potential, but appear to be in the early stage of development.

Antenna Arrays. Adaptive antenna arrays (Controlled Radiation Pattern Antennas) are effective against broadband jammers. They are likely to be most suitable to high-end aviation applications because of their relatively high cost. A flight-qualified military CRPA of 5-7 elements with low-noise amplifiers now costs about $15,000. Spatial filtering is the only precorrelation method effective against broadband interference and can provide form 25 to 40 dB of AJ protection. CRPAs work by blocking all signal reception in areas in which it has detected strong interfering signals. This may result in satellite availability issues for high integrity applications, since the antenna blocks satellite signals as well as the jammer in the affected reception sector.

A dual-aperture technique called amplitude/phase cancellation employs two antennas generally located on the top and bottom of an aircraft. Signals from the top and bottom antennas are combined to cancel the interfering signal. The technique can produce 20 to 30 dB suppression for both a single interference source, and for multiple sources around the horizon. It is effective against both wideband and narrowband interference sources. This technique requires the interference source to be under the aircraft.

Polarization Discrimination. One manufacturer has developed a single-aperture technique that exploits polarization discrimination to cancel the interfering signal. The technique operates at RF and uses a detection and tracking/control channel to identify and track the interfering signal and a hybrid junction to null the interference components of the composite signal. The cost is expected to be in the $200 to $250 range in quantities of 10,000 to 20,000 units.

It therefore appears that over half of the needed suppression specified in the JHU Report can be provided by a fairly inexpensive product that is effective against both wideband and narrowband interference without the need for multi-element antenna arrays. Moreover, according to the manufacturer [47], “Because it uses different operating mechanisms, it offers the potential for enhanced system anti-jam performance in a multi jammer scenario when combined with digital filters, and possibly even with null steering techniques.”

One should note, however, that at low elevation angles typical for a top-mounted antenna on an aircraft encountering a ground-based jammer, the aircraft’s skin acts as a ground plane causing the wave to be vertically polarized. Signals from low elevation satellites would be similarly effected leading to a reduced discrimination between the GPS and jamming signals. As a practical matter, the manufacturer claims that polarization discrimination works reasonably well on aircraft and that no one claims that it works as well as a CRPA. Nevertheless, it costs much less than a CRPA and takes up much less room on the aircraft skin.

Spatial-Temporal Filtering. One manufacturer is developing a low-cost AJ system for ground vehicle and helicopter applications. The program goals are to provide 30 dB of additional anti-jam protection for a mix of up to 3 wideband and up to 7 narrowband jammers.

Unlike aviation, where FAA certification of GPS receivers is required, certification requirements for maritime GPS receivers have not been implemented. This raises the issue of whether certification should be required and in particular, whether a RAIM algorithm should be required for certain maritime applications of GPS. RAIM has the potential to significantly lower the susceptibility of a GPS receiver to certain forms of spoofing. Similarly, requirements may be needed for jamming protection in a limited number of applications.

With the exception of the dual-aperture (top and bottom mounted antennas) technique called amplitude/phase cancellation, the jamming mitigation methods described above for aviation also apply to maritime operations. The shipboard siting of multi-element array antennas may, in some cases, present a problem due to the proximity of reflecting surfaces. Shipboard use of multi-element GPS arrays has not been widely reported in the open literature. If multi-element arrays do not lend themselves to shipboard applications (in some cases), a single aperture antenna with polarization discrimination may still allow for spatial filtering to combat wideband interference. Because some of the jamming mitigation techniques such as adaptive transversal filtering can be built into a receiver for a relatively low cost (less than $100), it seems that some minimal amount of anti-jam protection can be provided.

Because positive train control (PTC) systems have multiple means of determining train and maintenance-of-way vehicle location, only a minimal amount of enhanced anti-jam protection would be needed against the loss of GPS signals. An adaptive temporal filter could provide such protection. If spoofing were determined to be a significant hazard to rail applications of GPS, for example, spoofing of the NDGPS data link, most of the techniques applicable to an airborne platform would apply to rail applications as well.

Some ITS user services are vulnerable to interference, jamming, and spoofing. Most of these effects would be minor except for hazmat and emergency response.

Public transportation, travel management, and commercial fleets would be unlikely to bear the expense of special antennas for mitigating wideband jamming as the cost would be several times the cost of the GPS receivers in use. Polarization discrimination is a lower cost possibility, but it still doubles the system cost. In addition, because the users are on the ground it may be less effective against an RHCP jamming signal, since it may directly enter the antenna without having its polarization changed by refraction at the vehicle body.

For these user services, it is probably prudent that the first mitigation technique purchased be effective against CW and narrowband interference/jamming. These are the most common signal types that actually have been documented interfering with GPS. They are also dangerous, since CW can cause undetected navigation errors. Time Adaptive Filtering is the lowest-cost option.

Other user services prone to serious consequences if jammed, such as Emergency and Hazmat Response, should consider the commercial adaptive array antenna. Although rather costly, it provides protection against both wideband and narrowband jammers.

4.2.2 SPOOFING

Many techniques for identifying and ignoring a spoofer are known. Edwin L. Key discusses spoofing mitigation in rather complete detail [48]. He discusses the following techniques for countering spoofing:

- Amplitude Discrimination
- Time-of-Arrival Discrimination
- Consistency of Navigation IMU Cross Check
- Polarization Discrimination
- Angle-of-Arrival Discrimination
- Cryptographic Authentication

In his conclusions Key states, "There are many available techniques for identifying and ignoring a spoofer. The best anti-spoofing technique is probably the use of a multiple-element antenna to measure the angle-of-arrival of all received signals. Since it is very difficult if not impossible for a spoofer to match the angle-of-arrival of satellite signals, the spoofers are easily rejected." However, no method has been implemented, tested, or is commercially available.

Other techniques such as polarization or amplitude detection require new or modified receiver technologies, which are years away at best. The technique for discriminating a power jammer is not applicable to spoofing since the true and bogus signals have similar power. The sparse unclassified literature on anti-spoof simulation and testing indicates that much development and testing remains to be done, in order to determine the most effective anti-spoofing technique.

At present, there are no practical mitigation methods currently available for this class of GPS disruption, although a number of potentially effective techniques have been proposed. Many methods under consideration likely would be too expensive for some civil applications, for example ITS services.

(This page deliberately left blank)

5 ASSESSMENT OF TRANSPORTATION INFRASTRUCTURE VULNERABILITIES

This chapter presents an assessment of the transportation infrastructure vulnerabilities to a GPS outage and the risks to safety and operational continuity that result from those outages. As described in Chapters 3 and 4, natural and manmade mechanisms exist that may degrade or deny GPS data to the application. This chapter determines how such outages impact transportation.

The impacts of GPS disruption or outage can be measured as a **safety** impact or an **operational** impact. A safety impact involves potential environmental damage, property loss, injury or loss of life due to an accident or incident. An **operational** impact is one that results while operating the system safely but with reduced operational effectiveness. This might be the case if, for example, access to a specific airport was denied because of the outage of a needed navigation signal at that airport. The aircraft could proceed to an alternative airport safely, but with some economic impact upon the airline, the passengers, and commerce. A more severe operational impact might result if GPS service were denied over a wide area and all aircraft had to be vectored to airports where visual approaches might be made.

In this assessment, the distinction need not be made as to whether the GPS signal is degraded (for example, operating at less than the required navigation accuracy) or unavailable. If the GPS receiver can determine by some form of integrity and accuracy monitor whether it is being degraded or denied, and if the signal is declared as degraded, then it is effectively unavailable for its intended use. In some deliberate jamming situations, the jamming signal may reach the end GPS user, but not the monitoring station of a wide-area GPS augmentation such as WAAS, MSAS, EGNOS, or MDGPS. The affected users would then experience degraded performance, while the integrity monitors report no anomalies. RAIM users are not affected this way.

Factors that cannot be quantified in this assessment are the duration and geographic breadth of the expected disruption, or the probability of occurrence. However, for the purpose of this study, three situations are considered: (1) **Momentary Outage:** a single, very short term, limited breadth GPS outage (on the order of seconds or a minute, over a confined region); (2) **Serious Outage:** a single, moderate length, limited breadth GPS outage (on the order of minutes or hours, over a confined region); and (3) **Severe Outage:** a long term, wide breadth GPS outage (on the order of days over wide areas or a series of moderate length outages over a wide area).

A severe outage is considered to be an extremely unlikely event, probably only encountered in such situations as major military conflicts. A serious outage is less likely to occur than a momentary outage, but serious outages have occurred[10]. The duration of a serious outage makes it likely to involve many, if not most, of the safety impact situations. For example, aircraft in flight that are suddenly denied GPS have to be on the ground in less than a day at the most, due to fuel limitations. Other combinations of outage duration and breadth are possible, but these cases are adequate to assess qualitatively the potential disruption.

[10] The inadvertent jamming of a Continental Airlines aircraft over New York state recently is one example.

The following sections describe how each major user service responds to GPS disruption or outages. In all cases, no navigation system backup system is assumed, but there may be alternate procedures. The response to failure of GPS is to rely upon: (1) other non-navigational vehicle capabilities (for example, shipboard radars, odometers, or flight management systems); (2) visual navigation means; (3) ceasing operations where possible; (4) reliance on surveillance systems (for example, ground based radars to support air traffic controller vectoring); (5) operational procedures; or (6) combinations of these steps. A discussion of strategies to select and use backup systems is contained in Chapter 6.

Assessing the transportation risks was subjective, but used the conventional method to define risk, namely as a set of statements about the probability of an adverse event occurring and the consequences of such an occurrence. An unacceptable risk can arise from a very improbable event, if the consequences of such an event are large enough. The probability of an adverse event is, in turn, a function of the vulnerabilities of and the threats upon the transportation system. In this study, the vulnerabilities were examined, but not the threats.

It is recognized that determining the appropriate response of a system as complex as our national airspace system to the failure of a major subsystem such as GPS is an extremely difficult and complicated undertaking. This study should be considered as merely a first step in that determination. Operational procedures or methods that might be employed to respond to a major GPS outage probably are best left to each transportation mode to review, to determine the tradeoffs between operational procedures and backup systems. The FAA, for example, is planning a major simulation activity to determine how effectively air traffic controllers can respond to a GPS outage over a major piece of airspace (like an entire en route center). When the results of that study are available, a re-determination of the vulnerabilities and risks of the NAS can be made.

5.1 AVIATION VULNERABILITY

In 1998, the FAA funded a study by Johns Hopkins University [6] to determine whether GPS could be the only means air navigation system. The study identified ionospheric propagation effects and unintentional and intentional interference as risks to GPS signal reception. JHU concluded “unintentional interference is not a major risk factor.” Intentional interference was identified as the biggest risk area. The report stated “the impact of this risk was conservatively judged to be ‘hazardous’ because of the very widespread outage that can result and the potential impact on safety without appropriate air traffic control procedures.” The JHU study concluded that GPS and its augmentations could serve as “...the only navigation system installed in an aircraft and the only service provided by the FAA...” for operations anywhere in the National Airspace System (NAS) [6].

The findings in this report are generally consistent with the technical findings of the JHU report. There is agreement that unintentional interference is less of a concern, once managed, than intentional interference, and that the impact of intentional interference could be disruptive to normal operations. However, this report does not agree with the JHU conclusion that GPS and its augmentations could serve as the only navigation system for operations in the NAS. The implications of sudden loss of GPS over major population areas, possible long-term and widespread GPS outages, numerous reports of large undetected position errors due to jamming,

and the potential for a counterfeit signal to induce position errors are just too serious, both for safety and continuity of operations, to be able to make such a categorical statement. At a minimum, proven alternative procedures are necessary for all safety-of-life operations, as well as proper training and practice in recognizing GPS problems and using the alternative procedures. In some cases, independent backup systems are essential. This is consistent with comments made by FAA Administrator Garvey at an Air Traffic Controllers Association meeting in 1999 that aviation always will have a backup navigation system on the ground [11].

5.1.1 NAVIGATION (OCEANIC, EN ROUTE, TERMINAL, NPA, PA)

All aspects of navigation use of GPS are subject to Momentary, Serious, or Severe disruption resulting from degradation or loss of the GPS signal.

The impacts of **Momentary** outages would be minimal, assuming there is timely detection of the outages and alerting of the flight crew and air traffic controllers. However, this type of outage could result in missed approaches being required for aircraft on nonprecision or precision approaches, thus having an operational impact. When operating over certain terrain, the loss of missed approach guidance could be hazardous.

While the expected impact of most momentary outages probably can be controlled, especially from unintentional RFI, the potential chaos that may ensue from intermittent but frequent and randomly timed GPS outages caused by sophisticated intentional jamming. Without the ability to quickly detect, isolate, and react to GPS outages and transition to the use of backup systems or operational procedures, the air transportation system could effectively be shut down.

The impacts of **Serious** outages are more complicated. The duration of these GPS outages inevitably will require that an alternate procedure, possibly a backup system, be utilized, for any of the flight segments. The longer segments would generally not experience safety impacts, due to the relatively greater margins allowed. Depending on the specific situation, however, even the operational impacts could become costly. Safety impacts are possible, but probably not as likely. The aviation community should continue to develop an appropriate mix of proven backup systems and procedures to mitigate the Serious GPS outage.

For shorter flight segments, such as en route or terminal navigation, loss of GPS even for a short period of time could require extensive rerouting and vectoring of aircraft. Controller vectoring could probably maintain safety, but this assumption needs to be thoroughly validated before declaring all such operations safe. The FAA is planning a series of simulations to investigate the ability of ATC controllers to vector aircraft in the event of a widespread GPS outage, and a more complete assessment of these impacts can be made following those simulations.

Determining the impact of loss of GPS during nonprecision and precision approaches is rather complicated. It is extremely important that the pilot be alerted to the failure of GPS in a timely manner. Otherwise, the flight could continue using erroneous navigation signals with obvious safety implications. Assuming this timely notification, existing ATC procedures will handle almost all situations, whereby if navigation signals are lost, the aircraft executes a missed approach and either attempts the approach again, or proceeds to an alternative destination. The only situation that may require more study is the case where positive course guidance is required

(say in mountainous terrain) to execute the missed approach. If no other electronic navigation aid is available to provide this course guidance, some procedure or higher landing minima needs to be established to ensure safe missed approach operations.

The impacts of **Severe** outages also are pronounced. A safety impact might occur if extensive vectoring of aircraft to other airports results in excessive controller workload, considerable pilot confusion and additional workload, and possibly even fuel depletion if nearby airports were not available with weather conditions that would permit visual approaches and landings. As stated above, the FAA is planning a series of simulations to investigate this situation and a more complete assessment of these impacts can be made following those simulations. For a severe outage, aircraft would no longer be authorized to take off and conduct operations under Instrument Flight Rules. The economic impact of such a situation would be enormous. Retention of a sufficient backbone of ground-based navigation aids, acknowledged by the FAA to be consistent with its future navigation concept [7, 11], will be a very important mitigation to this type of threat.

5.1.2 AIR TRAFFIC CONTROL SURVEILLANCE

The use of GPS as part of an ADS-B or ADS-A surveillance system is subject to the same vulnerabilities as its use for navigation purposes. However, current FAA plans include provision of the full SSR system as a backup to ADS-B, should it be implemented, that should minimize either the safety or operational impacts of any ADS-B failure. Therefore, loss of GPS-based ADS-B would not significantly affect operations in any airspace where there was SSR coverage. For operations, however, in airspace where there is no SSR coverage, for example in oceanic, remote, and off-shore operations, users would have to revert back to procedural separation, with the attendant loss in efficiency and capacity of operations. If there is no non-GPS based navigation aid in those areas, failure of GPS would also restrict operations to visual flight rules.

5.1.3 AIRPORT SURFACE GUIDANCE AND SURVEILLANCE

Airport surface guidance and management based upon ADS-B is an emerging application. Impacts of the loss of GPS will only be felt after introduction of the services that depend upon GPS. If GPS is lost, and the flight crew requires it for safe and orderly navigation and guidance on the surface, then operations must cease, or revert back to perhaps less capable visual methods. As long as the crew receive accurate and timely notification of the failure of GPS, it is unlikely that a safety issue will arise from such a failure. However, some operational effectiveness will be lost. The situation with respect to surface management and air traffic control is similar. Both would have to revert back to visual or primary radar for aircraft surveillance.

5.1.4 COMMUNICATIONS SYSTEM TIMING

Several planned communications system improvements use GPS as a timing source and could be seriously impacted in the unlikely event that GPS timing signals are lost for an extended period of time. These include the NEXCOM digital air/ground communication system (using VDL Modes 3), VDL Mode 4 and UAT link systems[11]. These networks might utilize cesium clocks that can serve as a backup to GPS for a period of time. However, if synchronization of a network of communications facilities is required, a long-term outage of GPS can disrupt

[11] NEXCOM is using VDL Mode 3.

communications. Without mitigation strategies such as those proposed by NEXCOM, Serious or Severe GPS disruptions would have operational and possibly safety impacts for some operations.

5.2 MARITIME VULNERABILITY

Denial of GPS in the oceans and harbors, and DGPS in constricted waterways can lead to severe consequences when combined with another undesirable – and not always uncommon – event such as bad weather, loss of full control of the ship due to mechanical failure, or worse, a combination. The desire to exploit the full economic and safety benefits of GPS tends naturally to lead to extensive reliance on the system, and to a resultant inability to recover from some situations. This is particularly so in constricted waterways commonly encountered in HHA operations, where the off-course vessel, often as little as seconds away from a grounding or collision, can get into trouble quickly. Although only the rarest combination of unfavorable events could lead to loss of life following the failure of the GPS-based aids, major environmental and/or economic losses are more of a concern, and do occasionally happen.

In the case of Momentary outages, operational impacts would be felt, as users have to either revert to visual or radar navigation, or cease operations until visual conditions permit safe movement. In the cases of Serious or Severe outages, the longer term and wider coverage of the outage might result in unsafe operations.

GPS systems in the maritime environment are regularly affected by unintentional interference. Most events stem from other electronic devices now in regular and increasing use on the same vessel. New technology communications systems such as the MSS, LEO, GEO (for example, Inmarsat), and MEO options present the mariner with challenges to reliable reception of GPS signals. Shipboard radar can degrade GPS performance on a vessel. Mobile and fixed VHF transmitters have the potential to interfere with marine GPS receivers on inland waterways.

Ultra wideband (UWB) interference (see Section 3.1) can pose a threat to vessels using GPS that operate close enough to some UWB sources. The RTCA Special Committee SC-159 engaged a special working group (No. 6) to investigate GPS interference. This working group recently spent considerable time analyzing possible UWB effects. Though the work is not complete, there is some indication that UWB devices – which can perform many functions of great benefit to many people – may interfere sufficiently with GPS signals to warrant licensed (controlled) sales distribution. This possibility is strongly denied by many UWB manufacturers and vendors, and the FCC will make a decision within a few months on whether to grant UWB companies a waiver to sell devices at desired power levels without licenses, or whether they must negotiate power levels and use of spectrum with GPS stakeholders.

The USCG recently presented to Working Group 6 some maritime scenarios that may involve UWB interference with GPS. A GPS-equipped vessel passing under a bridge that has automated toll collection equipment for road vehicles may require more than 20 seconds to clear the area of possible UWB interference (the emissions can penetrate the road surface on the bridge and interfere with the vessel's GPS reception). If a vessel loses GPS for this length of time in such a restricted channel, there is a possibility of a collision or grounding in low visibility conditions.

Inertial systems commonly used would not be able to maintain course well enough, due to unacceptable drift rates, and radar tracking also could be inadequate.

In another area, many of the adverse events involving the use of GPS in the maritime application follow a similar pattern to those in the aviation application: a large percentage of these events reflect human factors considerations. This is discussed further in Appendix A.

The loss of GPS timing will impact current and future maritime communications networks. The emerging UAIS standards involve Self-Organizing TDMA (SOTDMA) data links that depend heavily on GPS for timing synchronization. Caution therefore must be employed to ensure that provision is made for the loss of GPS timing. It actually is easy to visualize the GPS dependence in the AIS and autopilot systems creating a serious vulnerability when the vessel is navigating a constricted channel in bad weather and GPS is lost. In this scenario, all vessels in the area will have much more difficulty locating each other and developing strategies for avoiding groundings or collisions. This is because AIS will provide the navigation, tracking and data communications capability, when vessels become fully equipped in a few years. The AIS architecture can allow for alternate systems, but many vessels may not equip for these. There is widespread use of GPS on ships today, as mentioned earlier, with varying degrees of operational robustness to loss of GPS. Crew training in proper use of GPS, and in switching to backup procedures or systems, also has achieved varying degrees of effectiveness.

5.3 SURFACE VULNERABILITY

The use of GPS in personal and commercial vehicles is growing rapidly and its utility is expanding. However, GPS is in limited use in critical surface transportation applications. In the following sections, certain critical surface transportation applications of GPS are assessed as to their vulnerability to GPS outages.

In assessing the potential effects of disrupted GPS service on surface communication links, any Serious or Severe GPS degradation has the potential to cause interconnected networks to become unsynchronized and fail. The actual effect will depend on the dependence of the local network architecture on GPS, and the degree and duration of the GPS disruption.

5.3.1 RAIL ASSESSMENT

At present, railroads are using GPS primarily for non-safety-critical activities: mapping of facilities, travelers' advisory systems, locomotive fleet tracking, and shipment tracking systems. The loss of GPS would temporarily affect the ability of railroads and the FRA to determine the precise location of track geometry and rail integrity anomalies. The positive train control (PTC) systems under development, which employ GPS and NDGPS, may require special attention to make certain that they do not become vulnerable to the loss of GPS.

PTC systems user multiple sources to provide location and speed information: GPS, NDGPS, calibrated tachometers, digital maps in on-board and control center computers, wayside interface units that provide switch position indication, and sometimes, inertial sensors. A railroad is essentially one-dimensional with branches. When a train is on a track, it moves longitudinally along the track. A train can leave one track and move to another only at a switch that can have only two states, "through" and "diverging". GPS/NDGPS places a train on a given track that is

defined on a digital map in the on-board and control center computers. The tachometer, calibrated by GPS/NDGPS to correct for wheel slip and wheel wear, determines the longitudinal location of the train along the track. A wayside interface unit at a switch informs the PTC system of the switch position, and the optional inertial sensor can confirm the passage of the train through the switch.

In the event of a Severe GPS outage, PTC systems and train operations will continue, using the remaining sources of location and speed information. Efficiency may be reduced as trains are forced to reduce speed or even stop. It appears, however, that safety is not likely to be compromised by the loss of GPS. This conjecture cannot be justified fully until such time as the proposed PTC applications are better defined and operational experience has been achieved.

5.3.2 ITS ASSESSMENT

Presently, the effect of GPS disruption on ITS user services would be limited to autonomous travel management, public transportation, commercial fleets, emergency response, and advanced vehicle control and safety systems applications. The relatively slow moving ground vehicles of ITS probably could not drive out of the disruption area. Nevertheless, most of these effects would be minor except for hazmat and emergency response. Other user services have not been widely deployed yet. However, as traffic worsens they will become more essential, and those implementing these services should be cognizant of the susceptibility of their systems to GPS disruption in terms of both position and system timing.

For hazardous materials and emergency response, degradation of GPS positioning accuracy or loss of GPS service may affect response times. In emergencies, position errors can cause the incident positions to be mapped to the wrong road or to the wrong direction on a divided road, resulting in a potentially hazardous effect. For hazardous materials incidences, delay or confusion due to incorrect road matching may be catastrophic. Incorrect routing of general emergency responses due to incorrect road matching may have a hazardous effect. These incidents were judged to have an operational impact in the case of Serious outages and a safety impact in the case of Severe outages.

In this user service group, the potential effect of GPS disruption on the communication links in these life-sustaining applications may be serious. Local wireless service could possibly be affected. If the wireless links are lost, the emergency notification, coordinated response, and best route services cannot function. Loss of the best route and emergency notification could be hazardous effects. Loss of coordinated response could be a catastrophic effect. These incidents were judged to have an operational impact in the case of Serious outages and a safety impact in the case of Severe outages.

5.4 SUMMARY OF APPLICATION VULNERABILITIES

Table 5-1 summaries the vulnerability assessment of each of the major GPS applications considered for aviation, maritime, and surface users. The green-colored boxes indicate that safety and continuity of operations can be maintained in the presence of various levels of outages. A yellow box indicates a safe, but operationally inefficient level of operation. A red box indicates potentially hazardous or unsafe operations that might result from GPS outages.

Table 5-1. Application Vulnerability and Risk Summary

Mode	Application	Impact of GPS Disruption		
			Serious	**Severe**
Aviation	Oceanic Navigation	Minimal	Operational	Operational
	En Route Navigation	Minimal	Operational[1]	Operational[1]
	Terminal Navigation	Minimal	Operational[1]	Operational[1]
	Nonprecision Approaches	Operational[2]	Safety[3]	Safety[3]
	Precision Approaches	Operational[2]	Safety[3]	Safety[3]
	ADS Surveillance	Minimal	Minimal[4]	Operational
	Airport Surface Operations	Minimal	Minimal	Operational
	Timing (Communications)	Minimal	Operational	Operational
Maritime	Ocean	Minimal	Operational	Operational
	Coastal	Minimal	Operational	Operational
	HHA/Waterways	Operational	Safety[3]	Operational
	VTS Surveillance	Minimal	Minimal	Operational
	Timing (Communications)	Minimal	Minimal	Operational
Surface	Rail PTC	Minimal	Minimal	Operational
	ITS Hazmat/Emergency Response	Minimal	Operational	Safety[3]
	Timing (Communications)	Minimal	Operational	Safety[3]

[1] This assumes that upcoming FAA simulations demonstrate that controllers can safely respond to Serious and Severe GPS outages.
[2] This assumes missed approach course guidance is not required. If course guidance is required, the disruption could have a safety impact.
[3] This safety risk occurs not because the operations are inherently dangerous without GPS, but rather because possible circumstances combined with loss of GPS may result in a safety or large economic or environmental risk.
[4] This assessment is only for areas covered by SSR. For areas not covered by SSR, the impact would be Operational for Serious outages.

This report focuses on critical transportation applications identified in chapter 2: aviation precision approach and nonprecision approach, ships navigating in constricted channels, ITS use in some hazmat or emergency response situations, and some critical timing applications. These are the applications that may involve safety impacts if GPS service is lost (as shown in the table). The other applications shown in the table are felt to be less critical - that is, able in general to withstand GPS loss with less damage or economic loss. These applications did not, for the most part, receive the scrutiny applied to the critical applications.

The difference between a serious and a severe outage is in the duration and extent (area) of the outage. Since a serious outage can last several hours, the operator under a limited-breadth outage must exercise an alternate strategy while the outage is serious. A mariner in this situation will have avoided difficulty, and then "dropped anchor" until conditions improve (or GPS recovers). Thus, there would be no safety impact for any plausible marine application during a severe outage. In aviation, on the other hand, a severe GPS outage, because it covers a wide area, can make the pilot-controller workload a possible safety issue in executing alternate procedures. These scenarios have low likelihood of occurring, but must be a planning factor.

6 TRANSPORTATION INFRASTRUCTURE RISK MITIGATION STRATEGIES

An important finding of this study is that backup systems or appropriate operational procedures, integrated with a more robust GPS, will play a critical role for the indefinite future in mitigating the vulnerabilities of civil GPS users to loss of the GPS signal. A more robust GPS can be achieved through implementation of techniques described in Chapter 4.

The alternative backup systems analyzed were on-board systems (for example, inertial navigation systems), other satellite navigation systems, and ground-based air radionavigation aids (VOR/DME, DME/DME, ILS, and Loran-C). The strategy selected depends upon the public purpose of the GPS backup. If it is only to preserve safety of operations during GPS outages, then the strategy is called a **safety** backup strategy. If the intention is to preserve the operational effectiveness of the transportation mode, even in the light of a denial of GPS service, it is called an **operational** backup strategy, for one is trying to preserve the full transportation system capability, to the extent possible. For those operations for which there is currently no effective alternative navigation service (for example, off shore, oceanic, parts of Alaska), operations may simply revert back to those that existed prior to the introduction of GPS. As long as this reversion can be performed safely, the primary impact will be reduced operational efficiencies.

Using signals from other satellite navigation systems along with GPS for navigation applications offers the potential to enhance integrity, availability, and to some extent accuracy for civilian users. Of particular benefit will be mitigation of the consequences of a major GPS system disruption or satellite problem. Galileo, the proposed European Union navigation satellite system now in its planning phase, could provide effective mitigation to civilian GPS users, as long as sufficient interoperability between the Galileo and GPS architectures can be developed and U.S. concerns regarding direct user fees and trade issues are satisfactorily resolved[12]. It is important to note that the Galileo system has the same vulnerabilities to deliberate jamming that GPS has, because of the weak signal. Since the civil Galileo broadcast frequencies will not be any of the GPS bands, unintentional RFI can be mitigated for dual-system users. Intentional RFI impacts can be reduced, due to the greater required jamming power and the added complexity required to jam GPS and Galileo simultaneously. Another benefit of dual satnav use may be against the loss of GPS due to crippling of the GPS satellites or Operational Control Segment.

Table 6-1 summarizes the alternative strategies identified and described in subsequent sections. Other combinations of backup systems are undoubtedly possible, but these are meant to be indicative of the approach to assessing those strategies. A full analysis, with costs, performance, and benefits of each strategy was not possible within the scope and time available for this study. However, one of the recommendations of this study is that such a full analysis be performed to support policy decisions on the proper risk mitigation strategy to pursue.

[12] The Russian GLONASS system cannot be considered as a viable backup system to GPS, at this time or in the foreseeable future.

6.1 BACKUP STRATEGIES

A number of alternative systems are identified in Table 6-1. These, combined with effective procedures and user training, as appropriate, represent the candidate backup strategy. The provision of a backup system is primarily an economic decision, rather than a safety one. The tradeoffs involved in deciding whether or not one is warranted, and which one it would be, are very complex and specific to the mode of transport and operational concepts. In all cases, the backup system does not provide a service equal to GPS, so there will be some loss of operational effectiveness in the event of a GPS outage. Each strategy has particular advantages and attendant user and government costs, that will require more detailed analysis of the threat, its impact upon GPS, the impact of GPS outage upon the transportation mode, and the costs involved to select the most promising and practical strategy.

Table 6-1. Alternative Backup Strategies

Strategy	Applicability to Mode			Comments
	Aviation	Maritime	Surface	
Other Satellite Systems	X	X	X	Will mitigate but not eliminate GPS outage risks.
VOR/DME/DME	X			A reduced network may not fully satisfy current and future needs.
Inertial	X			Limited applicability to Maritime and Surface modes in critical applications.
ILS	X			A reduced number of ILS may not fully satisfy current and future needs.
Loran-C	X	X	X	Will not satisfy precision approach or airport surface requirements.
Timing Backups	X	X	X	Backups needed only for GPS-dependent communications systems.

Each of the aviation alternatives below provides en route and terminal navigation and the potential for adequate nonprecision approach capabilities.

- Full VOR/DME network capability
- Other Satellite Navigation Systems (Galileo)
- Loran-C

New procedures will have to be developed to ensure that transitions to the backup capability are conducted safely and the ability to transition back to GPS preserved. The existing SSR surveillance system is required to provide a backup to ADS-B in most airspace.

For maritime and surface applications, either other satellite navigation systems, Loran-C, or a combination may be required. Low cost inertial navigation systems may play a role, but long term drift will require some form of radionavigation system or position reference to update the inertial system.

The backup strategy for all modes should include a strategy for providing a precision timing backup to systems that rely on GPS for time synchronization. If Loran-C is selected as a navigation system alternative, it can provide such a suitable backup.

There are uncertainties with each backup strategy. The FAA is considering a reduced VOR/DME network as a backup to GPS, but the size and airspace coverage of the network has yet to be determined. A DME/DME combined with Loran-C is being studied that might permit further reductions in the VOR network, but may not provide the requisite number of nonprecision approaches to support operational needs. The Loran-C system may be capable of providing guidance through nonprecision approach, but requires the development of aviation certifiable receivers, P-static antennas, and equipage by IFR aircraft, a substantial user investment.

6.2 BACKUP NAVIGATION SYSTEMS

This section will discuss briefly each candidate backup navigation system.

6.2.1 LORAN-C

Loran-C can provide two-dimensional area navigation over the CONUS and is an accurate source of time synchronization. Loran-C operates in the 90 kHz to110 kHz band, far from the microwave L band used by GPS. Virtually any interference to GPS will have no effect on Loran. Moreover, although GPS operates at a very low power level, Loran-C is a very high-power system. Radiated power levels range from 0.325 to 1.6 MW, making it very difficult to jam Loran-C. Loran-C ground stations are somewhat vulnerable to hostile physical damage or power interruption, but the impact of these can be mitigated by new receiver designs. These planned Loran-C receiver designs allow “all-in-view” tracking of all Loran-C signals received, so they can continue to work properly even if one or more stations in view are not operating.

In order to maintain the current capabilities of Loran-C until a decision is made about its long-term future, the USCG has been funded through the FAA and is authorized to make certain modernizations to ensure its reliable and economic operation. These improvements include installing new cesium clocks at the transmitter sites, replacing all of the old vacuum tube transmitters with newer solid state transmitters, automating monitoring and control of transmitter operation, developing new data messaging capability, enabling user end improvements such as digital receivers and reduction in static interference, and implementing certain physical improvements to the transmitter buildings and antennas.

A Draper Laboratory Study [49] analyzed Loran-C as a supplement to GPS for aviation. It concluded that Loran-C has the capability to provide a backup for GPS for en route, terminal, and nonprecision approach operations. Loran-C is not expected to make any significant contribution as a backup for precision approaches, either with its current capability or with future improvements. In order for Loran-C to effectively serve as a backup for airborne operations, the ground Loran-C infrastructure must be upgraded and operated to support airborne requirements. Airborne equipment must be developed with a demonstrated ability to meet airborne requirements including reduced susceptibility to interference from precipitation and lightning-induced static. For nonprecision approach, it may be necessary to apply additional secondary phase factor (ASF) corrections that are updated roughly every two months, and are airport-specific.

In 1999, Booze-Allen & Hamilton (BAH) performed a second Loran-C study [50] to analyze Loran-C to determine its optimized configuration and how an optimized system could be

integrated into the NAS. BAH analyzed a baseline which consisted of the current full VOR/DME network and two Loran-C configurations as shown in Table 6-2.

"Current Loran" includes the capabilities in effect at the time of their study plus full deployment of automatic blink and the re-capitalization initiatives identified by the Coast Guard. Moreover, it also includes installation of an H-field antenna and associated static control measures.

Table 6-2. Backup System Configurations [50]

Configuration	Backup Navigation Source	Additional Systems
Baseline	VOR/DME (full network)	
Loran-Configuration I	Current Loran	Reduced VOR/DME (222 stations)
Loran-Configuration II	Enhanced Loran	Minimal VOR/DME (20-40 stations)

"Enhanced Loran" includes: precise timing for multi-chain operations, transmitter improvements to increase signal stability, receiver enhancements for greater range, and an Uninterruptible Power Source (UPS).

"Loran-Configuration I" builds on the baseline configuration but adds Loran-C with planned upgrades to improve maintainability and the lifetime of current deployments. With the addition of Loran-C as an adjunct to existing navigation sensors as well as GPS, the opportunity to leverage Loran-C and decommission elements of the existing VOR/DME infrastructure is introduced.

"Loran-Configuration II" offers the additional navigation opportunities through the increased availability, accuracy, and robustness of the Loran-C system. These additional capabilities and performance allow the VOR/DME infrastructure to be reduced even further as the enhanced Loran-C system is introduced. Paramount among the enhanced Loran-C features is the improvement of availability by an order of magnitude.

Loran-Configuration II includes the GPS baseline components and the existing Loran-C system, plus the following enhancements:

- Revising operational and maintenance procedures
- Including Uninterruptible Power Source (UPS)
- Incorporating improvements in Loran-C receiver technology

Loran-C may have the capability to provide an alternate or backup source of GPS augmentation in some critical transportation applications. Modulation of the Loran-C signal pulse has achieved data transmission rates that could meet WAAS correction data requirements, while retaining the stability of the Loran-C navigation signal. Applicability of this technology has been demonstrated. Loran-C may be able to meet augmentation requirements in areas where providing space-based correction signals would be cost-prohibitive, or it could function as a "background" source of correction and integrity data, able to assume the primary data reception role in an integrated GPS/Loran-C receiver.

6.2.2 OTHER SATELLITE NAVIGATION SYSTEMS

Galileo is a proposed European Global Navigation Satellite System (GNSS) which is now in the definition phase. According to a recent paper [51], if the EU maintains its current schedule, nominal operations will begin in 2008. Galileo therefore will not be able to supplement GPS operations for several more years. Galileo will be designed to complement GPS, in order to enhance signal availability [51]. The open Galileo service will provide performance comparable to dual-frequency GPS.

Various satellite configurations have been under consideration. According to [52], the Galileo constellation plans to consist of 30 medium earth orbit (MEO) satellites, 27 of which will be in a 3-plane symmetrical Walker configuration with 3 on-orbit spare satellites.

While the frequency plan for Galileo has not yet been determined, frequencies close to the GPS L1 and L5, known as E1, E2 and E5, were being considered [51]. Should these frequencies be chosen, it would appear that interference/jamming of GPS might well affect Galileo as well, thereby greatly reducing its ability to serve as a backup to GPS. In addition, Galileo's satellite signals will be about as powerful as GPS, making them also easy to jam. The effectiveness of other satellite navigation systems in mitigating vulnerabilities to GPS users will be enhanced if there is a high degree of interoperability of the systems (although using dissimilar broadcast bands is desirable for overall robustness), if user fee and trade issues are resolved accordingly.

6.2.3 LORAN-C/INERTIAL SYSTEMS

In 1998, Galaxy Scientific Corporation conducted a study [53] for the FAA to assess the feasibility and performance impacts of the use of Loran-C in aiding and augmenting GPS and INS during GPS outages occurring during the approach and landing phases of flight. The two types of outages examined were: combined GPS and Loran-C outages, and GPS only outages.

According to the Galaxy report, the use of INS and/or Loran-C during GPS outages has the greatest positive impact on nonprecision approaches. This results from the calibration of Loran-C and INS errors with GPS prior to its loss.

Galaxy notes that for GPS/INS systems, the quality of the inertial system is the significant driver for overall system accuracy. The GPS/INS systems support nonprecision landings for all GPS and INS combinations when GPS outages are less than 120 seconds.

6.2.4 GPS/INERTIAL SYSTEMS

GPS and inertial systems have complementary error sources. GPS provides excellent long-term stability whereas inertial sensors have good short-term stability, but drift without limit over time. Moreover, because inertial sensors are self-contained, they are immune to radiofrequency (RF) interference. Integration of inertial sensors with GPS reduces system vulnerability to interference in two ways.

GPS integration with inertial sensors effectively removes platform dynamics from the problem. Estimation of platform dynamics is usually a function of the carrier tracking loop which is typically the weak link in a GPS receiver. Use of an inertial sensor allows the system designer to

reduce the bandwidth of the carrier and code tracking loops, thereby reducing their sensitivity to noise and interference.

The second benefit of GPS/INS integration is that if the interference is sufficiently strong to cause the GPS receiver to lose lock, the availability of an inertial navigation system (INS) permits the user to coast for a short period. The duration of the coasting period depends on a number of factors. These include: (1) the required position and velocity accuracy requirements of the mission; (2) the drift rate of the INS; and (3) the degree to which the INS errors have been calibrated by GPS during the time when GPS was available.

Triply redundant inertial navigation systems (INS) are certified for primary means aviation navigation in oceanic airspace. The high cost of several tens of thousands of dollars for a single INS (not a triply redundant system) makes these systems applicable only to air carrier or military aircraft. The cost of an INS depends heavily on the quality of the system which can be loosely characterized by the system drift rate. Navigation grade systems have drift rates of better than one nautical mile per hour or equivalently 0.015°/hr (1-σ). This corresponds to the aviation requirement of 2 nm/hr (95%). Lower quality systems may however, provide short-term backup to GPS. Such systems are considerably less expensive than navigation grade systems and can employ low-cost fiber optic gyro (FOG) or microelectromechanical system (MEMS) technology.

Current FOG drift rates range from several tens of degrees per hour to 0.01 degrees per hour (short term). Single unit costs range from $1,000 to $2,000 for the lower performance units to $15,000 to $18,000 for navigation grade gyros.

Current MEMS gyros have achieved drift rates of about 3°/hr in the laboratory over a limited temperature range. Expectations are that a gyro bias stability of 1°/hr is achievable. It is anticipated that the cost of this class of MEMS gyro might get down to $250 per axis including electronics in quantities that might be supported by the aviation market. Unfortunately, the technology needed for this more demanding drift rate requirement does not lend itself to integration with the gyro electronics on a single chip. Long-term expectations for MEMS seem to vary somewhat. Some researchers are predicting that MEMS silicon gyros will be able to achieve a drift rate of 0.01°/hr. Others suggest that a stability in the 0.1°/hr to 0.03°/hr range is more likely. High accuracy MEMS gyro technology is still in the research and development state; its potential use in aviation and other transportation applications has yet to be determined.

6.2.5 VOR/DME

VOR/DME currently provides navigation for domestic en route, terminal and nonprecision approach. While VOR/DME is a suitable backup to GPS for aviation, it cannot serve as a backup for non-aviation modes of transportation because of its line-of-sight coverage limitation. If the FAA implements its plans to reduce VOR/DME services based upon the anticipated use of GPS for en route navigation and instrument approaches, VOR/DME can serve as a safety backup to GPS but could not provide the full coverage required to maintain operational effectiveness of the undamaged GPS.

6.2.6 INSTRUMENT LANDING SYSTEM (ILS)

ILS is an international standard aviation system for performing precision approaches. Approximately 1,000 systems are installed in the U.S., each serving one end of a runway. Most commercial air carriers have ILS avionics, as do many business and general aviation aircraft. ILS has no utility to other transportation modes. Current FAA plans are, following full deployment of WAAS and LAAS, to retain a limited number of ILS installations as a backup to GPS for precision approach services. This strategy will not provide full operational capability in the event of a widespread GPS outage

6.3 BACKUP SURVEILLANCE SYSTEMS

6.3.1 LORAN-C BASED ADS

If a GPS-based ADS system is implemented, it must be determined how the ADS surveillance function will be performed if GPS fails. There are several alternatives, including using Loran-C.

For aviation, surface, and coastal maritime operations, Loran-C offers an alternative to GPS as a navigation input to an ADS system. All of the cost, performance, and operational issues associated with Loran-C as a replacement navigation system apply here as well. This ADS could replace the airborne ADS-B for transmission to nearby aircraft for situational awareness but is not sufficiently accurate to serve as an ADS-B on the airport surface.

6.3.2 MULTILATERATION

Multilateration is a promising surveillance system concept to replace ADS-B based ground surveillance in several applications. Its use as a full replacement for the SSR network or GPS ADS-B has not been seriously considered, but its use in limited applications is being evaluated. These applications include airport surface surveillance, parallel runway approach surveillance, and surveillance in the Gulf of Mexico.

Beacon multilateration is the determination, on the ground, of the horizontal position of the aircraft based on the reception of 1090 MHz transmissions from the aircraft transponder at multiple ground sites. ATCRBS (Modes A and C), Mode S (short and extended length), and ADS-B formats are all utilized. No changes to current aircraft transponders (ATCRBS or Mode S) are needed.

Three or more ground stations measure the time-of-arrival (TOA) of the same transponder message. Aircraft horizontal position is determined by joint processing of the TOA measurements at a central location (for example, on-shore at an ATC facility). Only one transponder message need be received to accurately determine aircraft position (i.e., operation is “monopulse” in the literal sense (one pulse)). Aircraft identity (beacon code) and barometric altitude are determined by decoding the information in transponder messages. Some designs of multilateration systems use GPS as a timing reference, so some provision needs to be made in such systems to guard against loss of GPS timing.

For Mode S equipped aircraft, the DF11 short squitter - emitted once per second (without being elicited), in order to announce the presence of an aircraft to nearby TCAS equipped aircraft - is the principal signal source for multilateration. Mode S aircraft are also interrogated

approximately once each 12 seconds, to determine their altitude. ATCRBS equipped aircraft are interrogated to obtain messages for multilateration (rate is to be determined). ATCRBS aircraft responses to nearby TCAS aircraft interrogations are also used for surveillance.

6.4 BACKUP TIMING AND CONTROL

As described in Section 2.2.4, GPS is becoming a primary source of precision timing in a wide variety of communications systems. These systems may need Stratum 1 (highest accuracy) clocks for the necessary precision to maintain required synchronization. Stratum 1 level timing can be provided by GPS, Loran-C, or cesium clocks (see Table 2-10). Loran or cesium therefore can backup GPS to maintain long-term, precision timing. This option may be appropriate for some critical uses. Short-term precision following loss of GPS usually can be maintained for at least two or three weeks. In just about any scenario for GPS loss that is likely to occur, this duration will be adequate to forestall severe consequences. If lower stratum clocks such as rubidium or quartz are available, they can substitute, albeit with some loss of precision.

Unacceptable consequences may arise if Stratum 1 networks have no GPS backup and if the GPS system suffers a severe (long-term) outage. However, this scenario is highly unlikely, especially since only one GPS satellite is needed to provide a timing reference. Jamming can disrupt GPS timing receivers, and this would deny access to *all* GPS satellites until the jamming ceases. But again, long-term successful jamming is very unlikely. The risk of unacceptable synchronization loss can very likely be mitigated via a combination of utilizing backup devices, protecting the timing receiver antennas from possible jamming sources, and providing the network with access to several timing receivers, separated if possible by a large distance. The appropriate mix, as usual, depends on balancing cost versus avoided undesirable consequences for each application. Some action will be needed, however, for critical timing systems that may now rely only on GPS.

The FAA's NEXCOM (using VDL Mode 3) may rely upon GPS timing at various sites to synchronize its ground stations, each of which will have a high stability clock. It should be noted that NEXCOM planners are considering backup strategies in the event of GPS failure, including obtaining precise time from Loran-C, WWV[13], or landline signaling. Similarly, VDL modes and UAT air-ground data links rely on GPS timing. The Coast Guard's UAIS system will rely on GPS timing for its SOTDMA data link.

In addition, the loss of GPS timing would greatly impact conventional communication networks such as high capacity fiber and cellular phone networks. It is clear that some form of backup to GPS timing is required to ensure long-term operations of our national communications networks, wherever high precision, long term timekeeping is required. Backup systems can range from a short-term backup such as crystal or rubidium clocks to long-term backups based on Loran-C or cesium timing. Loran-C was previously the principal source of precise timing for many applications, and if available, it could serve as a backup to GPS as a timing reference.

[13] WWV is a federal radio station that broadcasts time and frequency information at all times of day, on broadcast frequencies of 2, 5, 10, 15, and 20 MHz from Fort Collins, CO. A similar station, WWVH, is located in Hawaii.

7 FINDINGS AND RECOMMENDATIONS

Three sets of findings and recommendations are made relative to:

- Overarching issues related to GPS vulnerabilities
- Mitigating the vulnerabilities of the GPS signal to disruption or loss
- Mitigating the vulnerabilities of the transportation system resulting from disruption or loss of the GPS signal

OVERARCHING ISSUES RELATED TO GPS VULNERABILITY

Findings

- There is growing awareness within the transportation community of the risks associated with the GPS system being the only means for position determination and precision timing. The risks are a function of the probability of intentional and unintentional interference and the transportation-related consequences of loss of the GPS signal. The probability of interference is, in turn, a function of the vulnerabilities of the GPS system to disruption and the threats that could be made against the GPS system.

- Like any radionavigation system, GPS is vulnerable to interference that can be reduced but not eliminated. Because of the increasing reliance of transportation upon GPS, the consequences of loss of the GPS signal can be severe (depending upon its application), both in terms of safety and environmental and economic damage to the nation, unless the threats are mitigated.

- There are many augmentations to GPS (for example, the aviation Local Area Augmentation System - LAAS) that improve the basic GPS accuracy, reliability, availability, and integrity. However, even with these augmentations, use of GPS still can be disrupted and transportation services thus impaired. These impairments could range from mere inconvenience to major disruption of the national transportation infrastructure. The more serious consequences are very unlikely to occur, and can be avoided by awareness, planning, and supplementing GPS with a backup system or operational procedures when it is used in critical applications (applications in which the consequences of GPS loss could be catastrophic without ensuring that mitigating options are available).

- As GPS further penetrates into the civil infrastructure, it becomes a tempting target that could be exploited by individuals, groups or countries hostile to the United States. The potential for denying GPS service by jamming exists. The potential for inducing a GPS receiver to produce misleading information exists. Loss of GPS satellites or the Operational Control Segment could also impact GPS service, but attacking these elements can be more challenging and likely would produce a more aggressive U.S. Government response than jamming GPS users.

Recommendations

- Public policy must ensure, primarily, that safety is maintained even in the event of loss of GPS. This may not necessarily require a backup navigation system for every application. Of secondary but immediate importance is the need to blunt adverse environmental or economic impacts. The focus should not be on determining the nature of the backup systems and procedures, but on which critical applications require protection.

- Because requiring a GPS backup will involve considerable government and user expense, it is recommended that the transportation community determine the level of risk each critical application is exposed to, what level of risk each application can accept, the costs associated with lowering the risk to this level, and how such costs are to be funded.

MITIGATING THE VULNERABILITIES OF THE GPS SIGNAL TO DISRUPTION OR LOSS

Unintentional Disruption

Findings

- The GPS service is susceptible to unintentional disruptions from ionospheric effects, blockage from buildings, and interference from narrow and wideband sources. Some natural phenomena such as ionospheric distortions and scintillation can be predicted. These disruptions are most noticeable for users of single-frequency (L1) receivers.

- GPS-based timing synchronization is being used both for transportation-related digital communication links and other applications such as telecommunications, banking, commerce, and the Internet. Critical communications systems such as the FAA NEXCOM digital air/ground communication system rely on timing synchronization between ground sites. Other aviation data links rely directly upon GPS for timing synchronization. This is recognized within the FAA, which is planning the system to mitigate the consequences of loss of timing synchronization. A possible synchronization source is the GPS signal.

Recommendations

- Continuation of on-going GPS modernization programs involving higher GPS broadcast signal power and the eventual availability of three civil frequencies should be encouraged.

- The Federal Communications Commission (FCC), FAA Office of Spectrum Policy and Management, National Telecommunications and Information Administration (NTIA), the Departments of State and Defense, and other agencies should continue to vigorously support and protect the spectrum for GPS and its applications.

- GPS receivers involved in critical maritime and surface applications should be certified by the appropriate regulatory authorities. These authorities should recommend receiver performance standards in non-critical applications.

- Efforts must be taken to create and heighten awareness among the aviation, maritime, and surface user communities of the need for mitigation to degradation or loss of the GPS signal through unintended interference from such sources as VHF signals, mobile satellite services, ultra wideband communications, and broadcast television.

- Systems and procedures to monitor, report, and locate unintentional interference should be implemented or utilized in any application for which loss of GPS is not tolerable. Mitigation of signal blockage impacts should be addressed as much as possible in the GPS application system design process. RFI incidents that affect critical transportation applications should be reported to users as potential hazards to navigation, and users need to be trained in recognizing degradation or loss of the GPS signal, how to switch to an alternate navigation system or procedure if called for, and how to switch back to GPS when it recovers performance.

Intentional Disruption

Findings

- The GPS signal is subject to degradation and loss through attacks by hostile interests. Potential attacks cover the range from jamming and spoofing of GPS signals to disruption of GPS ground stations and satellites.

Recommendations

- Continuing assessments should be made of the applicability of military anti-jam technology, including receiver and antennas, to the civil sector. U.S. government agencies should be encouraged to identify the more promising anti-jam technologies, and to work with industry to make them affordable and suitable for civilian applications.

- The DOT should coordinate with the DoD to ensure that appropriate anti-spoofing technologies are available to civilian applications, should the need arise. It is important to identify observables that may indicate spoofing in civil safety-critical receivers. In addition, DOT should develop independent information to determine the validity and extent of possible civil spoofing threats.

- Within the limits of security requirements, the civil sector transportation community should be apprised of on-going threats and take effective countermeasures to those threats. Civil users should be encouraged to report GPS outages.

MITIGATING THE VULNERABILITIES OF THE TRANSPORTATION SYSTEM TO LOSS OR DEGRADATION OF THE GPS SIGNAL

Findings

- As with any radionavigation system, the vulnerability of the transportation system to unintentional and intentional GPS disruption can be reduced, but not eliminated. There is a growing awareness within the transportation community that the safety and economic risks associated with loss or degradation of the GPS signal have been underestimated. The GPS system cannot serve as a sole source for position location or precision timing for certain critical applications. Public policy must ensure that safety is maintained, even in the event of loss of GPS. Utilization of backup systems and procedures to GPS in applications where the consequences of losing GPS are unacceptable will ensure optimum safety.

- Backups for positioning and precision timing are necessary for all GPS applications involving the potential for life-threatening situations or major economic or environmental impacts. The backup options involve some combination of: (1) terrestrial or space-based navigation and precision timing systems; (2) on-board vehicle/vessel systems; and (3) operating procedures. Precision timing backups include cesium clocks or Loran-C for long-term equivalent performance, or rubidium or quartz clocks. The appropriate mix for a given application will result from careful analysis of benefits, costs, and risk acceptance.

Recommendations

- Create awareness among members of the domestic and global transportation community of the need for GPS backup systems or operational procedures, and of the need for operator and user training in transitions from primary to backup systems, and in incident reporting, so that safety can be maintained in the event of loss of GPS, in applications that cannot tolerate that loss.

- Encourage all the transportation modes to give attention to autonomous integrity monitoring of GPS signals, as is being done in the aviation and maritime modes (Receiver Autonomous Integrity Monitoring, RAIM).

- In an effort to provide the greatest benefit to the users, encourage the development of affordable vehicle-based backups such as GPS/inertial receivers, and, in the event Loran-C becomes a viable backup to GPS, aviation certifiable Loran-C receivers, and GPS/Loran-C receivers. All GPS receivers in critical applications must provide a timely warning when GPS positioning and timing signals are degraded or lost. Conditions for setting the warning indicator in the receiver, and for displaying it to users, should be standardized within each mode.

- Conduct a comprehensive analysis of GPS backup navigation and precise timing options including VOR/DME, ILS, Loran-C, inertial navigation systems, and operating procedures. Consideration must be given to: (1) the cost of equipage for both general and commercial

users – national and international in aviation uses; (2) navigation and precision timing system capital and operating costs; and (3) operating procedures and training costs associated with the need for situation awareness when the GPS signals are degraded or lost.

- Continue the Loran-C modernization program of the FAA and USCG, until it is determined whether Loran-C has a role as a GPS backup system. If it is determined that Loran-C has a role in the future navigation mix, DOT should promptly announce this to encourage the electronics manufacturing community to develop new Loran-C technologies.

- DOT should take an active role in developing a roadmap for the future navigation infrastructure that will be clearly stated in the Federal Radionavigation Plan, and will be followed by the DOT modes and navigation user communities in their navigation activities.

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.

(This page deliberately left blank)

APPENDIX A. GPS VULNERABILITIES

A.1 CAUSES OF THE VULNERABILITIES

This section discusses the aspects of the GPS architecture that make it vulnerable, and provides an overview of disruption mechanisms and the effects they can potentially cause.

The primary signal characteristic that makes GPS exceptionally vulnerable is the low power of the signal. Some GPS receivers can lose lock on a satellite due to an interference signal that is stronger than the GPS signal by about 30 to 35 dB [38,41]. A receiver attempting to acquire lock on a GPS signal requires 6 to 10 dB more carrier-to-noise (C/N_o) margin than is required for tracking [27]. C/N_o is the spread spectrum equivalent to signal-to-noise ratio; until de-spread with the code, the GPS signal is below the noise.

The low power signal problem is worsened because the receiver gain is limited by the bandwidth (BW) of the carrier-tracking loop, which must be wide enough to track platform dynamics (without external aiding). The code-tracking loop BW is much smaller, to minimize measurement noise, but that can introduce other problems. A typical code loop BW is 0.1 Hz, which means that it takes approximately 10 seconds (1/0.1 Hz) to get an independent measurement [54,55] depending on the robustness of the receiver design. This data latency may delay the recognition by the receiver of a loss of lock, resulting in corrupting measurements entering the navigation filter (processing algorithms), and the position-velocity-time solution.

The civil C/A code characteristics also contribute to the vulnerability problem. The C/A codes are Gold codes that repeat every millisecond. Instead of a continuous spectrum, this short code has a discrete line spectrum with lines separated by 1 kHz (inverse of the code period). This allows a Continuous Wave (CW) interference signal, which has a line spectrum, to mix with strong C/A code lines and leak through the correlator. The result can be undetected false signal lock. In addition, CW interference power that is attenuated to the noise floor using mitigation techniques may still leak through due to this effect. This code artifact will cause more problems during code search than tracking. There are, however, various methods to detect false lock. Ward [38] gives one example of a CW jamming detector which can be used to set a warning flag for false lock. Moreover, the parity check decoding algorithm can serve as an indication that false lock may have occurred. Longer ranging codes such as the one proposed for the new civil L5 signal do not produce the strong spectral cross-correlation lines exhibited by the C/A code.

The well known signal structure for the civil SPS is both a benefit and a weakness. The largely open architecture and intense scientific research into its characteristics has allowed a widespread commercial boom in GPS equipment, applications, and techniques. However, because the SPS signal is well defined and because of its mass-market success, it can be generated from widely available, relatively inexpensive equipment. Depending on the quality of the generated signal, it can be used as an enhanced jammer or as a true spoof signal that could be used to mislead a GPS receiver. The military PPS is much harder to spoof because of the encrypted P(Y) code.

The polarization of the GPS signal does provide benefits. Many unintentional interference sources generate linear polarized signals. GPS antennas are usually designed to be nominally Right Hand Circular Polarized (RHCP). Because a polarization mismatch between the signal and antenna attenuates the power passed to the receiver, interference signals not matching the GPS antenna polarization are reduced in strength according to the degree of mismatch. This attenuation, of course, also would apply to a jamming signal that was not polarized to match GPS. Note, however, that at low elevation angles typical for a top-mounted antenna on an aircraft encountering a ground-based jammer, the aircraft's skin acts as a ground plane, causing the jamming wave to be vertically polarized. Signals from low elevation satellites would be similarly affected, leading to a reduced discrimination between the GPS and jamming signals.

RAIM is the best receiver technique for detecting most integrity problems, especially in critical aviation flight segments. Receivers certified under FAA TSO C-129 [56] should be effective in detecting excessive position errors that result from jamming. The IMO is developing a marine RAIM standard, and the other modes also should look at this technique. A certified, quality receiver should recover immediately from RFI, although most apparently can recover within one or two minutes.

A.2 GPS DISRUPTION MECHANISMS

GPS is susceptible to disruption by both unintentional and intentional mechanisms. Unintentional mechanisms include ionospheric effects, interference from other RF emitters, and signal blockage. Human error also can disrupt GPS services. Intentional disruption mechanisms include jamming, spoofing, and meaconing[14]. Disruption and damage that results in severe (long term) GPS outages could be caused by hostile actions far less overt than full scale war. Although the likelihood of intended or unintentional damage to the GPS Operational Control Segment is very small, the consequences of such damage would be severe, since the satellites require regular upload information for nominal operation. The subsections below discuss disruption mechanisms.

A.2.1 UNINTENTIONAL DISRUPTION MECHANISMS

Ionospheric Interference

Mechanism Description. The ionosphere surrounding the earth at approximately 350 km altitude (F layer) can refract the L band signals of GPS. If the ionosphere contains small-scale electron density fluctuations, they can form a grating that diffracts the signal into a pattern of amplitude and phase variations that moves across the surface of the earth. This effect is called scintillation.

Total Electron Content (TEC) fluctuations are caused by the sun. Even during times of solar quiescence, the density of the electrons in the ionosphere varies geographically, and with time. This variation reduces the accuracy of single frequency/non-DGPS positioning. However, scintillation, which has the most effect on GPS, rarely causes problems except during the years around the maximum of the solar cycle. The most variability (and resulting scintillation) is seen along two bands at ±15° latitudes, and in the auroral regions that are between the ±65° latitudes and the poles. The bands on each side of the equator have maximum scintillation during the

[14] Meaconing is the reception, delay, and rebroadcast of radionavigation signals to confuse a navigation system or user. It is discussed further Section A1.2.2, under the heading "Spoofing and Meaconing."

hours just before midnight as the electrons stripped by solar energy rapidly, but not homogeneously, recombine with ions after sundown. In addition, the equatorial scintillation has a seasonal variability, with occurrence more likely during September to March [57].

The auroral regions' electron variability and resulting scintillation is due to energized particles captured by the magnetic field of the earth causing ionization in the ionosphere over the poles. The scintillations at the poles are not as strong as in the equatorial regions but they can occur at any time of the day, and last for days. This activity is related to the sun spot cycle and high geomagnetic activity [58].

The sun exhibits an eleven year cycle of sunspot and solar storm activity. There are several types of solar events that are of concern for GPS users. The largest geomagnetic storms are started by Coronal Mass Ejections (CMEs), large amounts of solar material shot toward earth during severe solar events. The solar material also can endanger satellites but the GPS constellation was undamaged by a recent large CME. CMEs lead the cycle sunspot peak so they are expected to be most numerous in 2001 and 2002 of the current cycle [59]. During that period, 25 major storm days can be expected each year and each storm may last for days.

After the CMEs diminish at sun spot peak, the maximum number of storms is expected to occur around 2005, but most of these will be minor. Caused by coronal holes, they will usually occur in phase with the 27 day synodic period of the sun [59]. In addition, short lived Solar Proton Events shower the earth with energetic particles that penetrate into the atmosphere and cause ionization. The particles also can cause Single Event Upsets (SEU) on GPS satellites. During Cycle 22, a proton event caused a large increase in GPS SEU. However, the satellites have been further hardened since that event in 1989. It is expected that there will be about a dozen proton events each year from now until after the peak (2002 - 2003) [59]. Lastly, solar X-ray flares can cause rapid changes in the TEC for the dayside ionosphere. This activity is expected to be most prominent between 2000 - 2002, with a large decrease after 2003. Each event will last only 30 to 60 minutes, but 450 - 550 major flares can be expected during each peak year.

Expected Effects. For the contiguous 48 states (CONUS), the largest effect of the solar maximum will be on the accuracy obtainable by single frequency users not employing differential techniques. The large solar flares will cause fluctuating range errors at a rate of less than 20 cm/min [60], with a total error on the order of 8 – 20 meters [61]. Also, some wide area differential systems located near the Gulf of Mexico or at Canadian latitudes will see some degradation in their ionospheric correction accuracy due to the variability in the TEC density over their service area.

The worst signal fading and phase scintillation will occur for satellites located near the poles and equatorial zones. The worst effects in the southern latitudes will occur in the evening hours before midnight. Severe scintillation that can cause brief signal fading by as much as 20 dB may cause some poorly designed L1-only receivers to lose lock on satellites in these affected zones, as was reported during a storm in 1992 [58]. Recent testing and simulation of scintillation indicates, however, that most L1 receivers will not be significantly affected, except perhaps during acquisition and tracking of low elevation satellites [57,62]. This fading usually lasts only

a few seconds, but it can cause cycle slips and measurement accuracy deterioration due to low C/N_o.

The greatest scintillation effect will be on codeless and semi-codeless tracking of L2 in the affected zones. This type of L2 tracking is primarily used in surveying and DGPS applications such as WAAS, LAAS, MDGPS, and NDGPS, to measure the ionospheric error. The most recent simulations and data from the National Satellite Test Bed indicate that phase fluctuation, which may vary as much as ±1 radian, does not fade, but causes loss of lock on L2 [57,58,60,62]. The tight BW (0.1 Hz) in the L2 code loop cannot track this rate of change. Although the worst scintillation may only last for ten seconds, it can take several minutes to reacquire the satellite. Receivers in CONUS may only lose the satellites over the susceptible zones (poles and equatorial belts), which would result in minor availability problems. Receivers within the susceptible zones may, however, lose L2 track on satellites in all line-of-sight directions [58]. Since the ionosphere is the largest error source in GPS, this can lead to significant degradation of the accuracy of DGPS corrections, mostly for small systems within a limited area near these susceptible zones.

Unintentional Radio Frequency (RF) Interference

There are concerns about interference from other RF transmitters that may produce harmonics in the L1 band. The systems of concern appear to have been distilled down to mobile and fixed VHF, television channels 23, 66, and 67, Over-the-Horizon (OTH) military radar, and possibly the Mobile Satellite Service (MSS).

L2 is even more vulnerable to interference because the frequency is not in an ARNS protected band. Codeless and semi-codeless tracking of L2 is more tenuous than direct code tracking because of processing losses and the weaker signal level. Many DGPS and survey-quality systems rely on the L2 measurement to determine the ionospheric delay correction. Despite this, L2 interference has not been studied as much as L1 interference. Newer receivers that track L2, however, have much greater protection from loss of that signal.

The proposed new L5 civil signal at 1176.45 MHz, allocated to Aeronautical Radionavigation Service (ARNS), partially overlaps the frequency band allocated to the military Joint Tactical Information Distribution System (JTIDS) and the Multi-Functional Information Distribution System (MIDS). JTIDS/MIDS and L5 have co-primary allocation. L5will be 6 dB stronger than L1 (1575.42 MHz), which is allocated to the ARNS and the Radionavigation Satellite Service (RNSS) band.

Broadcast Television. Interference from TV signals has been observed in at least one case [28]. In that case, however, the interference signal did not enter the antenna; it entered the power connection for the active antenna Low Noise Amplifier (LNA). The connection was designed to block signals at L band, but not the 525.25 MHz video carrier for channel 23. This high power signal caused harmonic distortion in the LNA that resulted in an average 5 dB decrease in C/N_o.

The best option for minimizing occurrences would appear to be through tightened FCC harmonic limits, education of TV engineers to maximize voluntary compliance, and enhanced enforcement. Also, all users should be urged and instructed how to report interference incidents.

These efforts should start now, since most stations presently are not transmitting at the maximum harmonic power levels. That may change with the arrival of widespread DTV, which employs an entirely different signal. Even if these steps were taken, it would be difficult to correct a malfunctioning transmitter within the initial two hours of disruption. More study is therefore required to identify critical applications and determine appropriate mitigation strategies.

VHF Interference. A study conducted by JHU [6] indicated that mobile and fixed VHF transmitters might interfere with GPS receivers at ground level as far away as 3.5 and 5.5 nautical miles, respectively.

Although there have been reports of interfering signals that have not been identified, there are no confirmed reports of VHF interference from ground-based transmitters to be found in the literature despite the use of VHF transmitters and GPS for a decade. This observation does not apply to on-board aircraft equipment. Transmissions from on-board VHF communications equipment have caused significant interference with GPS signal reception [29]. Technical and operational solutions are, however, available. Moreover, VHF transmitters usually do not emit the maximum allowable harmonic power. Also, the band allocated to VHF is not rich in harmonics that affect L1.

More study and testing of land and marine applications that may operate near VHF transmitters should be considered. The lack of reports of interference could be due to the transient nature of mobile interference. All users should be encouraged and instructed on how to report interference incidents.

Over-the-Horizon Radar. The JHU study also suggested that more study be done on OTH radar because of the limited public information on such systems. They suggest the threat is minimal due to the small number of these radar and their small beam widths. There is agreement with the JHU recommendation for more study because these radars often are used to scan over the North Pole for hostile forces and in Central America for drug smugglers. These areas also are most susceptible to GPS ionospheric degradation.

Mobile Satellite Service (MSS). The recent proposal to place MSS in the 1559-1567 MHz band adjacent to L1 presented a potential serious threat to GPS integrity. Nearby hand-held satellite transmitters could jam GPS receivers on highways, ships, and railroads. Satellite emissions could interfere with the WAAS geostationary satellite signal that has a lower power and different navigation (NAV) code format. L2 codeless and semi-codeless tracking would be severely affected [27]. Fortunately for the GPS community, this proposal was defeated at the June 2000 World Radiocommunication Conference (WRC).

Simulations performed recently indicate a 95% probability that the C/N_o degradation would be 1.2 dB for acquisition and about 1 dB for tracking at L1, perhaps affecting low elevation satellite acquisition and tracking. Despite the WRC decision, L2 codeless and semi-codeless tracking could be degraded by 2dB, which is serious due to the inherent losses in this tracking mode and the weaker L2 signal [63].

Ultra Wideband Radar and Communications. Ultra wideband (UWB) radar and communications systems generate extremely short pulses of energy that produces a very wide,

low power spectrum. The spectrum spreading can be done with or without a pseudo-random code. For normal narrowband systems, the average amount of power in their spectrum from a wideband system is negligible, which is why ultra wideband is used for Low Probability of Intercept (LPI) applications such as Special Forces communications. However, all UWB signals will have a central spectral pulse that stands well above the rest of the signal spectrum. In an environment with multiple systems, these peak pulses could be all over the spectrum with some overlapping to increase the instantaneous peak power. In addition, a wideband signal like GPS, generated with pseudorandom noise codes (PRN), may result in enough cross-correlation to produce interference. All ultra wideband signals that overlap the GPS frequencies will raise the noise level over the GPS band, but the effect on GPS tracking is extremely difficult to quantify due to many different kinds of UWB pulses having different characteristics (duration, rise time, harmonic modulation components, etc.) produced by different electronic designs and antennas [31].

The FAA Associate Administrator for Regulation and Certification (AVR) is reviewing the interference potential of wideband radar in the aviation application [64]. Also, RTCA Special Committee SC-159 is developing a report on the possible impacts on modal transportation users of GPS that may arise from UWB interference.

Human Factors in GPS Disruption

The human factors impact on the GPS system, GPS equipment design, and among GPS users also could threaten safety. Although in most cases a person in the loop is an additional safety factor, human factors can contribute to a problem if there is a lack of user understanding of the limitations and vulnerabilities of GPS navigation. The U.S. government test that recently achieved successful spoofing of some civil receivers shows that even users expecting GPS problems can put too much (or too little) faith in the receiver solution.

It appears that most of the accidents to date involving use of GPS actually have been the result of human factors issues. The National Transportation Safety Board (NTSB) has reported use of non-differential GPS for altitude information resulting in pilots crashing into terrain, pilots programming handheld receivers in flight resulting in accidents, and loss of battery power on handheld GPS receivers also causing accidents [32].

In a study conducted by the Australian Bureau of Air Safety Investigation (BASI) [65] of 367 pilots who use GPS, the results demonstrated that 7.9% used GPS in instrument meteorological conditions (IMC) before it was legal to do so in Australia. Pilots in Australia are required to take training on the use of GPS, however the study indicated that 21% of the pilots were using GPS before completing the training. Of the pilots who did take the training, 22% indicated they felt it had inadequately prepared them for the use of GPS.

A recent paper presented by NASA at the Ohio State Symposium on Aviation Psychology [33] suggested that pilots are more likely to take greater risks during flight regarding the weather when the airplane is equipped with a GPS than when only older navigational instruments (i.e., VOR, ADF) are available.

The NASA Aviation Safety Reporting System (ASRS) database [34] also provides numerous accounts of pilots traveling into restricted airspace while using GPS since it gives them the

flexibility to not have to fly the traditional route structure. The database also provides descriptions of pilots experiencing trouble with GPS receivers when using a different manufacturer's GPS receiver other than the one to which they are accustomed.

Human factors problems with GPS have been experienced in maritime applications as well. The Royal Majesty incident that occurred off the coast of Massachusetts in June 1995 very likely epitomizes the role of several prominent human factors elements. These include: lack of adequate training, over-reliance on a single navigation system, failure to recognize that the primary (GPS) system was not working properly, system design deficiencies, and failure to check information by using any one of several working supplemental systems. The incident also is representative of many maritime adverse events in that while there was relatively little physical risk to the humans involved, there did result substantial inconvenience and financial cost. The following detail is derived largely from the NTSB Abstract of Final Report on the incident [35].

The Royal Majesty, en route from Bermuda to Boston, grounded on June 10 1995 about 10 miles east of Nantucket Island, Massachusetts, with 1,509 people on board. Because of unfavorable tide conditions and developing poor weather, the vessel could not be freed, nor passengers evacuated, until the following day. Damage to the vessel and lost revenue were estimated to cost about $7 million. This figure does not include the economic impact to passengers. NTSB determined that *the probable cause of the grounding of the Royal Majesty was the watch officers' over-reliance on the automated features of the integrated bridge system; the company's failure to ensure that its officers were adequately trained…; the deficiencies in the [system] design and implementation, and the procedures for its operation…; and the second officer's failure to take corrective action after several clues indicating that the vessel was off course.*

Contributing factors were inadequate international training standards for such equipment and inadequate international standards for the design, installation, and testing of integrated bridge systems aboard vessels. The integrated bridge system on the Royal Majesty included GPS. The vessel also had a fully functioning Loran-C system on-board that inexplicably was not turned on.

The incident precipitated when the GPS antenna cable, mounted in an area exposed to traffic, disconnected from the receiver. This caused the GPS to switch to a dead-reckoning mode; however, the autopilot was not programmed to detect the mode change, and thus did not correct for the effects of wind, current, or sea conditions. Also, the fathometer alarm was not set to 3 meters, which on sounding may have provided the crew 40 minutes for course correction, and the weather at the time was clear enough to visually sight the Nantucket lighthouse. This aid would not have been visible if the ship were on course. The only mechanical problem lay in the GPS receiver. The unfortunate German couple who followed the rental car navigation system instructions faithfully and drove into a river is another example. This incident emphasizes the need for training to recognize and react to the loss of GPS.

Human factors problems also can occur with the GPS Operational Control Segment. A mistake in uploading data to the satellites apparently has a very low probability given the excellent record of the GPS Control Segment, but it is a possibility. Bad satellite orbit positions would result in

bad receiver positions unless differential corrections are applied. More likely are satellite and receiver design flaws - these have happened in the past.

The GPS Operational Control Segment and the satellites have various ways to indicate a failure or problem to users. These methods, detailed in ICD-GPS-200C, include setting health bits in the NAV message, generating a non-standard preamble in the navigation (NAV) message, switching an unhealthy satellite to the reserved PRN 37 code, and generating a non-standard code of alternating 1s and 0s (Block IIR only) [36]. There have been several occurrences of satellite anomalies that caused a satellite to generate non-standard C/A code. Stanford and the National Satellite Test Bed (NSTB) staff independently reported seeing a recurring, undetected, frequency anomaly, but the satellite gave proper warning of a problem. The problem was that processing algorithms used by Stanford University and NSTB researchers were using codeless cross correlation of the L1 and L2 carriers. They therefore never detected the non-standard code and continued to use the unhealthy satellite.

During extensive initial testing of a satellite launched in October 1997, the health bits were set to unhealthy so it would not be used. A receiver used in thousands of car navigation systems in the Far East was not designed correctly resulting in complete failure of all those receivers during the five days of satellite testing. Although the receiver did not use the unhealthy satellite in the navigation solution, it used some of its out of range NAV data in ephemeris calculations [36].

During 37% of the navigation uploads to Block II satellites, an anomaly occurs due to a satellite design flaw that causes the satellite to go unhealthy and broadcast non-standard code for a minimum of six seconds [36]. Several commercial receivers being monitored for their response to this anomaly stopped tracking the satellite, and it took between 18 and 53 seconds for most to reacquire after the anomaly ceased. One took over two minutes to start tracking again. This reduces availability and can delay signal lock. Another receiver exhibited large code range and phase jump at the onset of the anomaly, which is an integrity problem [66]. That receiver manufacturer is making changes for future models, but the older models are still in use.

A.2.2 INTENTIONAL DISRUPTION MECHANISMS

Although the GPS C/A code is referred to as a civil code, for many foreign armed forces it is a military code. Potential adversaries and the civil community have access only to the C/A code. The accelerating worldwide military dependence on GPS makes mechanisms to disrupt the signals potent weapons that many militarily sophisticated countries are actively developing. Though problematic and a possible act of war, it is possible that adversaries could create the capability to deny the GPS signal to civil applications over wide geographic areas and for long periods of time. This might be through widespread jamming, disabling numerous GPS satellites, or disruption of the Operational Control Segment, including backup facilities.

The U.S. military has a policy to deny foreign adversaries the use of GPS and its augmentations in a conflict while preserving its utility to U.S. forces, and without unduly disrupting or degrading civilian uses outside the area of conflict. The effort to develop GPS disruption systems for this purpose, and to protect allied forces from GPS disruption is called NAVWAR [7]. Since P(Y) code is encrypted, potential adversaries will be using the C/A code, making it a target for disruption. Other countries are reported to be developing similar capabilities.

NAVWAR testing may impact civil use of GPS in the U.S., but DoD and DOT have developed mechanisms to coordinate times and places for testing, and will notify users in advance [7]

Some jamming devices/techniques are available on the Internet and proliferation will continue, because a single device that could disrupt military and civil operations in any region worldwide would be attractive to malicious governments and groups. Civil GPS applications may be either innocent bystanders or the intended target. In either case, the mechanisms, potential effects, detection observables, and available mitigation equipment and techniques must be completely known to the civilian community, so that vital and safety-of-life applications can be prepared properly.

Jamming

Mechanism Description. Intentional interference or jamming of GPS is the emission of radio frequency energy of sufficient power and with the proper characteristics to prevent receivers in the target area from tracking the GPS signals. Low C/No causes loss of lock or inability to lock. That results in increased thermal noise jitter in the carrier-tracking loop until it exceeds the tracking threshold. Code tracking can be maintained only with external aiding when carrier tracking is lost.

Typically, the jamming signal power must exceed the signal power by 30 - 40 dB to jam an already locked receiver, but one tested receiver had a margin as low as 20 dB [41]. The jamming signal can be CW, broadband, narrowband, Gaussian, or a GPS-type modulation. Narrowband interference is about 3 dB more effective than broadband interference against GPS. Narrowband (less than 500 kHz BW) can, however, be removed with signal processing techniques. A signal modulated to look like GPS is effective at preventing satellite acquisition at very long ranges with considerably less power than other types of jammers would require. A pulsed jamming signal has advantages against some mitigation techniques.

It is well known in the military GPS community that the SPS can be jammed over a significant area by an airborne, low power jammer (1 watt). It is estimated that when airborne, such a jammer can deny GPS tracking to an already locked receiver at 10 km, and prevent it from acquiring lock at a range of 85 km [38,39]. It is estimated that a 1 watt spoofer could result in the loss of GPS signal acquisition for all satellites to the horizon (approximately 350 km) [39]. The exact distance and required jamming power depends on the type of jamming signal (CW, wideband, etc.), GPS antenna gain, body masking loss, and receiver design. One should point out that it is very difficult to deny aircraft approaches over a large area with a single ground-based jammer because the horizon/terrain blockage acts as a limiter. Multiple low-powered or airborne (balloon or aircraft) jammers can, however, be used to overcome this limitation.

If jammers are made with some sophistication, so that the jamming signal has the same type of spread spectrum as GPS, the same power results in a dramatically increased denial range. In line-of-sight conditions, a one watt GPS-like signal can prevent C/A code acquisition to more than 620 miles (or as limited by the line-of-sight to the horizon). The jamming signals can be generated with relatively low cost equipment [40]. The vulnerability of the GPS system to this type of ‘GPS-like’ RFI can be a potentially serious threat. This type of interferer will deny the

GPS spread spectrum de-spreading processing gain, and will be extremely difficult to detect by conventional methods such as spectrum analysis.

One other complication related to GPS C/A code jamming is that CW jamming can cause problems even if mitigation techniques reduce the jamming power to the receiver noise level. As mentioned at the beginning of this appendix, the line spectrum of the CW jamming signal can leak through the receiver correlators because it mimics the C/A code line spectrum. Because the C/A code repeats every millisecond, the C/A code has a line spectrum with lines separated by 1 kHz. Small fluctuations in the autocorrelation function of the C/A codes lead to deviations from a sin(x)/x amplitude spectrum. Every C/A code has a few "strong" lines above the sin(x)/x envelope. These lines are vulnerable to continuous wave (CW) interference at this line frequency. The correlation process between a CW interferer and a PRN code normally spreads the CW line. Unfortunately, the mixing process at some "strong" C/A code lines results in the interfering CW line being suppressed less than at other frequencies [67]. This effectively reduces the tracking loop gain by several dB (depending on the receiver design) and can cause false lock incidents. The problem will be worse for receivers with wider front-end bandwidths [38,55].

If the motive is intentional injection of misleading information by creating false lock, the mechanism is referred to as deceptive jamming. A recent study conducted at one of the U.S. military colleges demonstrated the effect of correlator leak-through on a modern commercial C/A code GPS receiver. Both CW and swept CW jamming signals were combined with live satellite signals to study the sensitivity of an SPS receiver to jamming. According to the study, "By tailoring the jamming signals to match with the Doppler shifted satellite frequencies and offsetting the jamming to a maximum spectral line, it was shown that individual Navstar XR5-M receiver channels for specific satellites could be selectively jammed/spoofed." The report noted "Swept CW jamming resulted in pulling the XR-5M receiver tracking channels off frequency by up to 20 Kilohertz but resulted in a maximum position error of only 220 meters. The CW jamming of at least one of the XR-5M receiver channels resulted in position errors in the receiver in excess of 12 kilometers." It should be pointed out that large navigation errors were encountered before the receiver flagged the position as invalid.

This CW effect apparently can be produced unintentionally as well. One type of commercial receiver in the National Satellite Test Bed (NSTB) reference stations experienced numerous cases of false lock on different receivers, at different reference stations, and at different times. All the reference stations were adjacent to airports, so it could have been caused by VHF communications. The effect appeared very similar to what has been reported from CW interference with the C/A code line spectrum. Other types of receivers in the same stations were not affected. The affected receivers' figure-of-merit indicated a good signal that could be used in the navigation solution. The NSTB reported the problem to the manufacturer.

GPS jammers exist in a variety of sizes and output power levels. Small, lightweight, short-lived jammers with power from 1 to 100 watts could cost less than $1,000. These jammers can be built by people with basic technical competence from readily available commercial components and publicly available information.

Jammers borne by Scout-sized vehicles emit between 100 and 1000 watts and cost on the order of $100K. Airborne or truck borne, high-power jammers can produce jamming power in the range of 10 kW to more than 100 kW, but cost a million dollars or more. The high-end jammers can produce a variety of waveforms that enhance their effectiveness. The director of a military GPS testing program recently stated that there are over 70 models of foreign military equipment that could easily be converted to megawatt level GPS jammers.

At the other end of this threat spectrum is the concern about the potential for large numbers of mass-produced, low cost, and lower power jammers. There are foreign factories currently making consumer products that easily could be modified to produce thousands of GPS jammers a day. Hundreds could be distributed in single area of GPS denial.

For a small noise jammer, the biggest limitation is power. Operation of a 1 watt GPS jammer for 12 hours would require about 2.1 lbs. of alkaline batteries or 1 lb. of lithium batteries. A 10 watt jammer requires 10 times more batteries by weight to operate for the same 12 hours. Some commercially available gasoline generators weighing about 30 pounds can operate an 80 watt jammer for five hours on one gallon of gas.

It also should be noted that GPS augmentation systems could be jammed as well. These include WAAS, LAAS, MDGPS, and NDGPS. The WAAS correction signal is a GPS L1 C/A code signal with a different NAV message format. Its signal is one dB weaker than L1 C/A code signals. Other non-GPS communication links in DGPS systems can be jammed but generally require more power than GPS jamming.

Expected Effects. The primary effect of jamming is the prevention of satellite acquisition and, at a closer range, the loss of GPS tracking. Estimates of jamming effectiveness as a function of power, range, and receiver type are useful. The true effectiveness, however, will vary significantly within those areas, especially for ground applications. In safety critical applications, it is imperative to test the susceptibility to jamming on the actual vehicle under realistic conditions, because the results depend heavily on the environment.

Spoofing and Meaconing

Mechanism Description. Spoofing, the injection of misleading information into a navigation system, is a technique that has long been used against targeting radar. There are several common techniques, including range gate pull-off and range gate pull-in. Range gate pull-off as applied to radar is a defensive technique. The deception system determines the time of arrival of the targeting radar pulses. Then the system emits a false pulse that is delayed from the real reflected pulse by a gradually increasing amount of time. Radar determines range from the travel time of pulses reflected off the target. Delaying those pulses injects a range error.

Radar uses early and late gates to keep the pulse centered in the correlator by sliding (in time) toward the gate with the most signal power until they are balanced. The power of the pulse train from the deception system is stronger than the real reflection so as it is swept across the range cell (time delay) where the two gates are centered, it captures them. Then the gates are slowly (electronically speaking) pulled away from the true range. U.S. pilots in Iraq and recently in Yugoslavia depend on similar techniques to confuse radar-guided, surface-to-air missiles. The technique also can be applied to GPS, as it is a ranging system that uses early-late gate tracking

of code pulses. Figure A-1 is an illustration of range gate capture as it might be applied to a GPS tracking channel. Note there are three gates in most GPS receivers - early, prompt, and late. At first, the spoof pulse train would appear to the receiver as an interfering signal or a minor correlation peak caused by the C/A code line spectrum. After capture, the real signal could

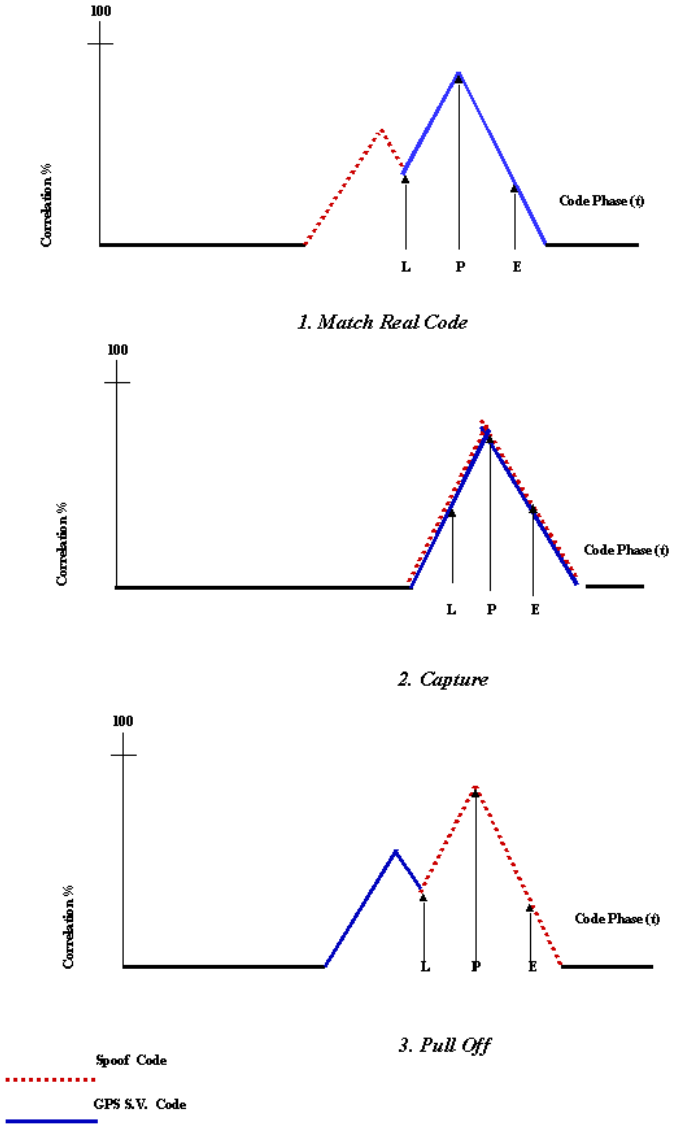

Figure A-1. Illustration of a Range Gate Capture Technique

appear to be multipath until the correlators are pulled completely away, depending on whether the range was shortened or lengthened.

The spoof signal can be generated from knowledge of the true signal or the true signal itself can be manipulated and rebroadcast. In order to minimize a sudden unreasonable change in GPS

position readout, and avoid potential detection by integrity monitoring such as RAIM, information on the actual position of the targeted receiver relative to the spoofer is required. A spoofer must be able to predict the next code pulse to shorten the measured range. The anti-spoofing encryption of the very long P(Y) code makes it difficult to spoof because the deceptive jammer does not know what code chip comes next. The C/A code, however, is well known and is relatively easy to generate. Less information on the relative position is required to capture the range gate if spoofing is preceded by jamming, which could cause the receiver to lose lock prior to acquiring the spoof signal.

Spoofing is more difficult to achieve than jamming, and it is less likely to be used, since it is usually targeted to an individual user. Spoofing does not normally achieve the widespread disruption of standard jamming, but its PRN signal actually can jam at very long distances.

Meaconing is the reception, delay, and rebroadcast of radionavigation signals to confuse a navigation system or user. Even if the ranging code was unknown and unpredictable, and could not therefore be generated, meaconing could produce a genuine-appearing signal. Meaconing may be easier than generating spoof signals because when generating a signal, NAV data and satellite positions must be created or copied. Since meaconing involves the delay of a navigation signal, in the case of unpredictable codes, it would seem to require that the meaconing system be closer to the satellites (airborne) than the target when the range gates are captured, if it is to be undetected. Depending on receiver response to time shifts, a C/A code meaconing system may not be bound by these restrictions because the code repeats every millisecond. More independent testing is needed to determine receiver response and operational restrictions. The existence of meaconing as a *possible* disruption agent argues against using authentication bits as a mitigation approach. It should be noted that other communication links in DGPS systems could be spoofed.

The WAAS, LAAS, NDGPS, and Coast Guard radiobeacon transmissions could theoretically be spoofed since they are well known. For non-GPS type links more power may be required, but the signal structure is much simpler. Meaconing would not be needed against any of the DGPS correction links except WAAS because they are data messages and not ranging signals. The WAAS signal could be subject to meaconing because it is a data and ranging signal. Demand for these spoofing systems would seem lower than for a GPS spoofer because of their limited uses, unlike a GPS spoofer which has worldwide civil and military applications. A similar argument applies to the demand for devices to spoof ground-based aircraft navigation aides. Components required for generating a deceptive C/A code signal are commercially available.

A GPS meaconing system would probably be made of components used in deceptive radar jammers, GPS receivers, and GPS translators. A key component is probably a commercially available high speed, Digital Radio Frequency Memory (DRFM). DRFM is used in EA systems to record and variably delay a radar signal before it is transmitted back to the radar. This gets around the problem of predicting the pulse repetition rate (or code) of the true signal when generating a spoofing signal. GPS translators or the front end of a GPS receiver can be used to receive and down-convert the GPS signal to a lower frequency that can be digitally sampled. Once the GPS signal is down-converted and sampled, the samples are stored and delayed in a DRFM, then up-converted to the original frequency and rebroadcast at a higher power. A

directional antenna would allow the effect to be contained, and could reduce interference with the meaconing system receiver that originates from its transmitter.

Although there are many operational considerations, the technology appears to be available. An advertisement for a DRFM on the commercial market in early 1998 offers a 500 MHz BW card, with a variable delay in 2 nanosecond increments (60 centimeter range resolution for GPS), phase synchronization input, variable Doppler shift, and independent adjustment of amplitude and phase.

An even less complicated implementation was proposed by the instructor of a 1999 Association of Old Crows unclassified course on Expendable Jammers. The implementation would simply replace the DRFM with an optical fiber communications link. The delay through the optical link would be even less than through the DRFM, providing enhanced ability to get inside the receiver range gate by presenting a signal even closer to the true signal phase. A combination of the two delay methods (DRFM and fiber) might make an even more effective device.

It is often thought that someone attempting to spoof a receiver must have very accurate knowledge of the target position in order to match the code phase well enough to get within the receiver range gate. However, a typical GPS receiver range gates have three correlators, early, prompt, and late that are spaced ½ code chip apart. The total span of that gate is at least a code chip, which for C/A code is 300 meters. Therefore, a spoofer can have a relatively large error in target position and still be able to sweep the signal phase across the expected position to capture the range gate - if 1-chip correlator spacing and spoofer/target receiver time synchronization are assumed. Doppler offsets can be generated for a trajectory automatically with a signal generator or calculated in advance. Jamming prior to spoofing could cause receivers to lose lock, making knowledge of the target's position less important.

In addition, transportation mode vehicles frequently are restricted to well-known and often repeated paths. These well-known paths include airport approach patterns, constricted shipping channels, railroad tracks, and roads. Simple trial and error at these constricted points probably could yield success. Such a crude approach would be unlikely to capture the gates seamlessly but given the current lack of knowledge, vigilance, and receiver indicators, it could be successful.

Potential Effects. The minimum spoofing effect would be to jam the receiver. Without further independent testing, it is impossible to judge how effective these devices are in misleading a receiver. It seems possible, however, to inject significant range errors in a receiver. Determining whether an autonomous receiver can detect spoofing would require more independent testing.

Contrary to some opinions, the effects of spoofing will be experienced over large areas. The largest affected area would experience the enhanced jamming effect caused by saturating the receivers with plausible but false signals, which will be especially disabling during satellite acquisition; an ongoing process in all receivers as satellites set and rise. The next smaller area would be close enough to the target area that the spoof signal would sweep - at least momentarily - across some receivers' range gates, causing range errors similar to bad multipath. Receivers in the smallest area near the target may lock on to the strong spoof signal, causing erroneous

position and timing solutions. The perpetrator can greatly enlarge the size of the area in which receivers lock on to the spoof signal by preceding the spoofing with jamming until the receivers lose lock. The receivers would no longer know their positions and would likely lock to the strongest signals present. This eliminates any need to know even the approximate positions of the targets.

Given the possibility of injecting significant errors, it is not hard to envision nightmare scenarios for GPS-dependent transportation modes. In critical applications such as marine narrow channel navigation, a ten meter error could cause ships to collide or run ground and perhaps leak their hazardous cargo. A small increase in error during bad weather could drive a barge into a highway bridge at rush hour. Pilots in the Panama Canal and in many other waterways use a DGPS system for navigation.

There is almost no information and no test results concerning the response of commercial receivers to spoofing. It is important to identify receiver observables that may indicate spoofing. Although some of the available results of DoD tests indicate successful spoofing against some civil receivers, there is no public information on the magnitude of the range error induced. There also is no open information on the capabilities of military spoofing systems or the expected capabilities of spoofing systems made from commercial components. Information on the capabilities, limitations, and operational procedures would help identify vulnerable areas and detection strategies. Since the theoretical effects of spoofing could be disastrous, it is essential that DOT develop independent information to determine the validity and extent of the threat.

A.3 FURTHER DETAILS OF GPS VULNERABILITY

The L1 signal (Figure A-2) at 1.575 GHz carrier is Binary Phase Shift Key (BPSK) modulated by the combination of three binary data streams: the navigation message at a bit rate of 50 Hz, the 1023 bit C/A code at a code chip rate of 1.023 MHz, and the long, encrypted P(Y) code at a chip rate of 10.23 MHz. The resulting GPS signal is spread spectrum (similar to a *sin(x)/x* pattern) with nulls spaced in the spectrum corresponding to twice the code chipping rates. The GPS signal is nominally Right Hand Circular Polarized (RHCP) which indicates that the signal electric field has nearly equal vertical and horizontal magnitudes. Right hand indicates the direction of field rotation during propagation.

The C/A signal at the surface of the earth has a minimum specified power of -160 dBW (1×10^{-16} watt), which is on the order of 20 dB below a receiver thermal noise level. This level of signal power has been compared to the energy received from a 25 watt light bulb at a distance of 11,000 miles [68]. Only by correlating this very weak signal with a local replica of the C/A code is the civil GPS receiver able to pull the signal out of the noise to decode the navigation (NAV) message (satellite positions, health, time) and measure the signal travel time from the satellite. The P(Y) code power level on L1 is -163 dBW.

The L2 signal at 1.227 GHz structure is similar to L1 but presently does not have the C/A code because originally it was to be a military frequency only. The C/A code will be added to L2 over the next decade as a co-primary allocation in this band. However, prior to the decision to add C/A code to L2, civil receiver designers developed “codeless and semi-codeless” methods to track the frequency even without correlating with the encrypted P(Y) code. This allows direct

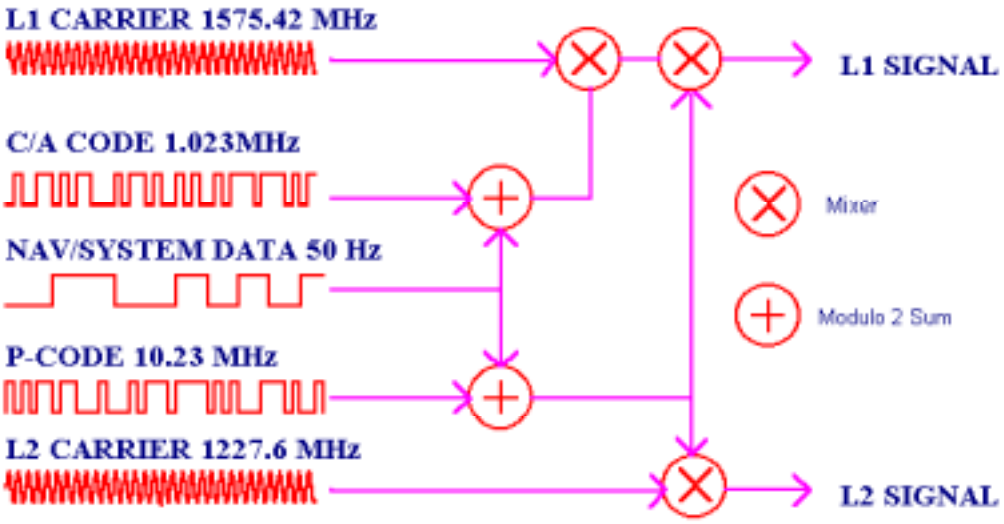

Figure A-2. GPS Signal Structure

measurement of the frequency dependant, ionospheric delay error, and its removal from the Position, Velocity, and Time (PVT) solution.

The minimum specified Y L2 signal level at the surface of the earth is -166 dBW, 6dB below the L1 C/A signal level. That power difference plus additional processing losses in the codeless/semi-codeless tracking techniques results in between 3 - 12 dB more susceptibility to interference and jamming than L1 C/A tracking. The exact level of increased susceptibility depends on the specific receiver and antenna design, as well as the incident signal strength. Another problem with using L2 is that it is presently not allocated to ARNS, as is L1. Figure A-2 shows the GPS signal structure for the L1 and L2 bands.

APPENDIX B. GPS VULNERABILITY MITIGATION STRATEGIES

Mitigation techniques cover a wide range of options. Methods likely to be effective against unintentional interference may be of limited value in combating intentional interference (jamming and/or spoofing). Moreover, the degree of protection required can be expected to be application specific.

As an example, aviation mitigation techniques often involve what may be unacceptable complexity and high user costs. The three techniques suggested in the JHU GPS Risk Assessment Study [6] to suppress interference effects (aircraft body shading, nulling antenna technology, and IMU integration) appear to place a heavy cost burden on the aircraft operator. Although efforts are underway to lower the cost of these mitigation techniques and devices, it is unclear if and when much of the general aviation aircraft fleet will be able to install these recommended devices.

Also, some of the improvements that were stated in the JHU report [6] as necessary for integrity and robustness may not be implemented for some time, when at least 24 Block IIF SVs that can broadcast the second and third civil frequencies will be deployed. This implies that ground-based navigation aids ought to operate during the transition period. Users will face a dilemma of when to equip.

The approach taken here is to discuss mitigation within the context of the interference class (unintentional or intentional), followed by separate discussions of mitigation requirements on a mode specific basis.

B.1 MITIGATION OF UNINTENTIONAL INTERFERENCE

Although a threat assessment is not within the scope of this project, unintentional interference may well be the most likely source of interference to GPS. To date, this appears to be the case for the aeronautical community, based upon the experience of the FAA. Perhaps the most significant difference between unintentional interference and intentional jamming is the likelihood that under the latter, multiple GPS frequencies (L1, L2, and L5) will be jammed simultaneously.

GPS Modernization

The GPS Modernization Program [45] should provide a substantial reduction in the threat from unintentional interference. Higher GPS signal power, a C/A code on L2 and a more robust civil code on L5, all combine to greatly reduce the susceptibility of civil applications of GPS to unintentional interference. The L2 and L5 signals (1,227.6 and 1,176.45 MHz respectively) are sufficiently far removed from L1 (1,575.42 MHz) that it is extremely unlikely that an unintentional interferer would jam all three frequencies simultaneously.

GPS modernization will mitigate the loss of GPS across all applications due to unintentional interference. However, it should be noted that the L2 frequency is not in an ARNS band that is protected for aeronautical navigation. Primary civil uses of L2 are for direct measurement of

ionospheric delay and integer ambiguity resolution for high precision applications. Consequently, while L2 may serve as a backup in certain applications, it is not likely to be accepted by the FAA as a backup frequency.

Implementation of the second civil signal is to begin on a retrofitted Block IIR satellite projected to be launched in 2003. The third civil signal on L5 is to be implemented on the Block IIF satellites with the first launch projected for 2005. At the current launch rates for planned GPS Block IIR and IIF spacecraft, the new modernized capabilities will be available in the 2010 to 2015 time frame. There is interest in accelerating this schedule and in increasing the GPS constellation. According to McDonald [45], "Investigations accomplished for the FAA and others indicate that 30 to 36 spacecraft may be necessary to meet integrity and safety-of-life requirements."

Increased satellite signal power, coupled with the more robust L5 code, increases the protection still further. It therefore appears that in the long term, GPS modernization will for most, if not all applications, greatly minimize the problem of unintentional interference. The key phrase is, of course, "long term."

Jam-Resistant User Equipment

Techniques to improve the jam resistance of GPS receivers may be broadly classified as precorrelation and postcorrelation methods. Precorrelation methods tend to be waveform specific and include spatial processing, temporal processing and spectral processing [46] Adaptive spatial processing (beam forming or null steering) using multi-element antennas can provide from 25 to 40 dB of anti-jam (AJ) protection and is the only precorrelation method effective against broadband interference [46]. Multi-element antennas tend to be expensive and are more appropriate to military applications. One manufacturer has, however, developed a spatial filtering technique that uses polarization discrimination and requires only a single antenna aperture. This technique, as well as spectral and temporal filtering, can be applied ahead of an existing GPS receiver and at a relatively low cost.

Each of these methods has limitations. Adaptive spatial antennas are less effective against pulsed jammers because they need a continuous signal for assigning nulls. Multiple jammers can overwhelm them since they can accommodate only one less jammer than antenna elements. For some modes, satellite availability could be an issue when portions of the sky are nulled out. The polarization discrimination technique is only effective against a non-RHCP signal at the antenna. Assuming that the jammer uses a properly polarized antenna, the polarization change has to be induced by the refraction of the signal at the body of the vehicle. If the jammer is above the antenna as is possible for some modes, its polarization will be unaffected by the vehicle or vessel body. Neither adaptive spatial antennas nor polarization discrimination is effective against a jamming signal that has the spread spectrum characteristics of GPS signals (pseudorandom noise code modulation), unless the signal is so powerful that it is significantly above the noise floor.

Adaptive temporal processing methods include blanking and clipping of short duty cycle, high power signals. Transversal filtering and amplitude domain processing methods provide from 15 to 45 dB AJ improvement [46]. Adaptive spectral processing methods include digital excision

and spectral amplitude domain filtering. These methods provide 25 to 30 dB of AJ improvement against a variety of narrowband interference sources [46]. They operate because a narrowband interfering signal must be above the noise level to be effective and is therefore subject to detection and mitigation. See Chapter 6 of [67] for a comprehensive discussion of the effects of interference on GPS receivers.

According to Gustafson et al. [46], "The performance of postcorrelation methods tends to be waveform independent and offers the possibility of enhanced AJ capability against broadband Gaussian jammers. Postcorrelation methods include (1) addition of other sensors and (2) enhanced signal processing." Inertial aiding is often used in military applications and permits the reduction of tracking loop bandwidths thereby improving AJ performance. Additionally, an integrated GPS/inertial system can slow the rate of navigation error growth when GPS is lost. Additional information on inertial systems and sensors is included in Section 6.1.2.

Signal processing techniques include bandwidth reduction [69] and "data wiping," that is, increasing the coherent processing time beyond 20 milliseconds [70]. Sennott [71] has proposed a method that accounts for the position and velocity error correlation among the satellites. These techniques are receiver-specific, requiring new receiver design and development.

Gustafson et al. [46] have proposed another signal processing technique that is claimed to operate independent of the ones described above and to offer significant AJ improvement. According to the authors, because it is independent of the other signal processing methods, it can be cascaded with any of the above methods thereby enhancing the total AJ capability. They state, "In summary, the hardware-in-the-loop demonstration results indicate an improvement in code tracking of 15 to 20 dB in wideband AJ capability for the proposed deeply integrated INS/GPS system relative to traditional tightly coupled designs." Deep integration is said to apply to GPS-only navigation as well as integration with other sensors such as the inertial sensor said to be representative of current microelectromechanical system (MEMS) sensor technology. However, deeply integrated systems like these combine their GPS and IMU observables so tightly that they may not be able to determine when the GPS is giving good data in the presence of jamming.

The use of a ferrite based power limiter has been suggested [72] for the suppression of both wideband and narrowband jammers. The power selective limiter (PSL) operates in the power domain and takes advantage of the nonlinear property of YIG ferrite material. The insertion loss of the device described is about 5 dB for power levels below the threshold (currently about -24 dBm) and is proportional to the signal level for signals above the threshold. The current threshold is considered too high and the author claims that the next generation limiter will have a threshold around -65 dBm. According to the author, since the device operates at the molecular magnetic dipole level it has an extremely fast response time. A small external magnet maintains dipole alignment. The author concludes that the PSL "provides significant jammer suppression, at very low cost, and since it operates at RF is easy to retrofit (can be inserted between the antenna and receiver of an existing system). It has small size, and requires no prime power."

While the PSL appears attractive, further development is required. The PSL would be ineffective against a jamming signal that has the spread spectrum characteristics of GPS signals

(pseudorandom noise code modulation), unless the signal is so powerful that it is significantly above the noise floor.

B.2 MITIGATION OF INTENTIONAL JAMMING AND SPOOFING

Jamming

The term intentional jamming as used here refers to the use of RF interference to cause a GPS receiver to fail to acquire or to break lock and no longer provide a useful navigation solution. This is distinguished from the term deceptive jamming where an interfering CW signal at a selected Doppler offset has been shown to be able to "capture" a tracking loop causing it to provide false information for a limited period of time before the receiver becomes aware of the problem.

Additional frequencies provided by GPS Modernization offers promise of effectiveness against intentional jamming. The availability of GPS ranging signals on multiple frequencies will make the problem for the jammer difficult and costly. The signal characteristics of L5 make jamming it considerably more difficult. The 6 dB higher signal power is effective against all types of interferers and cuts the jamming distance in half. The higher chipping rate and longer code are effective against CW jammers, reducing susceptibility to them to be about the same as to wideband interference. As much as 16 dB more jamming power would be needed to jam successfully a receiver using all three civil frequencies.

Additional civil frequencies will not, however, pose an insurmountable problem to organizations of enemy states. Jamming multiple civil GPS frequencies is simplified by the integer relationship among the three frequencies that soon will be available (one of these, L1, is available now). All three are integer multiples of the same basic GPS frequency of 10.23 MHz. The likelihood that multiple GPS frequencies will be jammed simultaneously may constitute a significant difference between unintentional interference and intentional jamming.

A second significant difference between unintentional interference and intentional jamming is that the latter may involve multiple sources. Temporal and spectral filtering can be effective against multiple narrowband jammers, but spatial filtering is the only precorrelation method effective against broadband jammers. Postcorrelation methods of dealing with wideband interference may have potential, but appear to be in the early stage of development.

The mitigation methods for unintentional interference may also apply to intentional jamming. Because the mix of threats is likely to be different, a combination of techniques likely to be adequate for unintentional interference may not provide sufficient protection against intentional interference. The choice of mitigation methods will depend on the specific application and the perceived threat to that application and is beyond the scope of this report. Non-critical uses may require only a modest amount of jamming suppression, whereas safety-critical applications may have very stringent requirements. For example, the Johns Hopkins University (JHU) report [6] claims that, "Techniques that can add 40 to 50 dB of additional rejection are possible; inclusion of such capabilities would virtually defeat the jamming threat considered in this study."

C/A code receivers are subject to a phenomenon known as correlator leak-through. A strong CW signal can cause a receiver to lock to this signal as if it were a real satellite. This can result in

range errors on the order of hundreds of meters, which may be detectable using RAIM depending on the number of receiver channels in false lock. Deceptive jamming is not always intentional as electronic systems sometimes produce RF interference with line spectra that correspond to the vulnerable C/A code spectral lines. This process is discussed more fully in Chapter 4 of [67].

Fortunately, narrowband jamming such as this can be mitigated using adaptive temporal filtering, a relatively low-cost receiver augmentation available now. Locating the emitter and adding filtering at the source also can mitigate unintentional interference from immobile sources. Spatial adaptive filtering (null steering antenna) also is effective, but it is presently more expensive than temporal filtering. The additional civil frequencies planned would help mitigate this threat by providing for more robust RAIM performance to the point of completely mitigating unintentional CW jamming.

Spoofing

Much of the following material comes from the work of Key [48].

In the context of GPS countermeasures, spoofing is defined to be the transmission of GPS-like signals that are bogus. These bogus signals are intended either to produce erroneous navigation solutions or saturate the processor of the victim receiver, effectively jamming it.

Spoofing has certain advantages over jamming as a GPS countermeasure. In most applications, spoofing requires substantially less power because it benefits from the full coherent processing gain of the GPS signal. For the C/A code this gain is between 30 and 43 dB, and P(Y) code provides an additional 10 dB. Spoofing in its simpler form may deny navigation by saturating the receiver with credible but bogus signals. Sophisticated spoofing also can create false navigation solutions, and it is possible that the victim will not realize that this has happened.

On the other hand, spoofing signals may have characteristics that will someday allow the user to detect and ignore them. Unlike random noise, it employs a known signal that is very structured. If the intended victim recognizes the presence of a spoofing signal, it may be completely ignored, or eliminated by processing. The spoofing signal will as a rule differ in some respect from the true GPS signal. It can differ in time of arrival, Doppler shift, amplitude, polarization, or angle of arrival. These differences, if exploited, can be used to ignore the spoofers and concentrate on the valid GPS signals. Unfortunately, no commercial systems are currently available to detect these spoof signal characteristics.

Many techniques for identifying and ignoring a spoofer are known. Spoofing mitigation is discussed in rather complete detail in a paper by Edwin L. Key [48]. Key notes that, “Although the emphasis is on airborne platforms, most of the treatment is applicable to problems faced by ground forces as well.” He discusses the following techniques for countering spoofing:

- Amplitude Discrimination
- Time-of-Arrival Discrimination
- Consistency of Navigation IMU Cross Check
- Polarization Discrimination
- Angle-of-Arrival Discrimination
- Cryptographic Authentication

In his conclusions Key states, "The best anti-spoofing technique is probably the use of a multiple-element antenna to measure the angle-of-arrival of all received signals. Since it is very difficult if not impossible for a spoofer to match the angle-of-arrival of satellite signals, the spoof signal can be detected if its incident angle is different enough from the real signal's incident angle and the receiver has received or can receive valid GPS satellite navigation messages telling where the satellites can be found." However, no anti-spoofing technique has been implemented, tested, or become commercially available yet.

There are issues concerning the implementation of this technique that need to be addressed via further testing. The accuracy of the angle to the satellite determined by interferometry depends on the length of the baseline between the receiving antenna elements [73]. Most multi-element antennas have baselines on the order of a few centimeters that under normal conditions might yield an angular accuracy of tens of degrees. To be effective, multi-*antenna* systems that allow baselines on the order of meters may be required. Carrier phase interferometry is very susceptible to multipath errors, so antenna placement is key [74]. In addition, the attitude of the vehicle must be known in order to check for proper satellite angles relative to the reference plane of the vehicle. In addition, as mentioned above, some means of validating newly received NAV messages (almanac and ephemeris data) may be required.

A search of the literature reveals only two papers from officers at the Air Force Institute of Technology that discuss techniques that at a minimum have been simulated to estimate their effectiveness. The techniques discussed, Multiple Model Adaptive Estimation (MMAE [75]) and Parallel Kalman Filter Estimation [76], involve the use of complex multiple Kalman filters to detect, estimate, and correct the induced range offset of a spoofer. An INS is required for both techniques. Both papers indicated their methods showed promise but needed further development and testing.

Other techniques such as polarization or amplitude detection require new or modified receiver technology, which is years away at best. (The technique for discriminating a power jammer discussed above is not applicable to spoofing since the true and bogus signals have similar power.) The sparse literature on anti-spoof simulation and testing indicate that much development and testing remains to be done to determine the most effective anti-spoofing technique.

B.3 MITIGATION STRATEGIES BY MODE

Mitigation for Aviation Applications

RF interference can be mitigated if it is detected, if the source is located, and if the interfering signals are neutralized or turned off. The FAA currently is addressing this issue. In addition, receiver designs that mitigate the risk can be implemented at modest cost.

Antenna Arrays

Adaptive antenna arrays (often called a Controlled Radiation Pattern Antennas or CRPA) are effective against broadband jammers. They are likely to be most suitable to high-end aviation applications because of their relatively high cost. A flight-qualified CRPA of five to seven

elements with low-noise amplifiers now costs about $15,000. Spatial filtering is the only precorrelation method effective against broadband interference and can provide form 25 to 40 dB of anti-jamming protection. A lower cost approach using polarization discrimination is more likely to meet the needs of general aviation.

Generally speaking, multi-element antenna arrays are needed to combat wideband jammers and an N-element array is needed to place nulls on (N-1) jammers. Note that N elements are not always effective against N-1 jammers, since multipath restrictions of each jammer's signal can reduce the number of degrees of freedom. A two-element array should be able to suppress a single source of broadband interference. In practice, a minimum of three or more elements might be desirable. Low cost multi-element antennas may soon become commercially available. Such antennas do not need to meet the stringent phase/amplitude specifications required to form the deep nulls required by the military, nor are they required to have a low radar cross section as is often required for military applications. According to one manufacturer, multi-element patch antennas for commercial applications might be produced at a cost of a few hundred dollars per element. Another manufacturer said that a flight qualified flat array of 5-7 elements might cost from $2,000 to $3,000 in quantities of hundreds of units.

A dual-aperture technique called amplitude/phase cancellation employs two antennas generally located on the top and bottom of an aircraft. Signals from the top and bottom antennas are combined to cancel the interfering signal. The technique can produce 20 to 30 dB suppression for both a single interference source, and for multiple sources around the horizon. It is effective against both wideband and narrowband interference sources. This technique requires the interference source to be under the aircraft.

It is unlikely that more than a single unintentional interferer will be encountered. In the case of intentional interference, it is difficult to speculate on the number and kind of jammers that might be encountered. This is best left to other agencies which deal with threat assessment. The FAA Office of Civil Aviation Security Intelligence has already funded such a study.

Polarization Discrimination

One manufacturer has developed a single-aperture technique that exploits polarization discrimination to cancel the interfering signal. Various packaging options are available including the Interference Suppression Unit (ISU) LRU, module and chip set form and a Miniature AJ Engine (1.4×2.4×0.16 inches). The technique operates at RF and uses a detection and tracking/control channel to identify and track the interfering signal and a hybrid junction to null the interference components of the composite signal. According to the manufacturer, the COTS product provides greater than 25 dB suppression of wideband interference and greater than 35 dB of suppression of narrowband interference. The AJ Engine operates with any single-aperture antenna which has a two-port feed. The cost is expected to be in the $200-$250 range in quantities of 10,000 to 20,000 units.

It therefore appears that over half of the needed suppression specified in the JHU Report can be provided by a fairly inexpensive product that is effective against both wideband and narrowband

interference without the need for multi-element antenna arrays. Moreover, according to the manufacturer [47], "Because it uses different operating mechanisms, it offers the potential for enhanced system anti-jam performance in a multi jammer scenario when combined with digital filters, and possibly even with null steering techniques."

Spatial-Temporal Filtering

An example of spatial and temporal filtering is provided by Mayflower Communications Co. Mayflower has developed anti-jam hardware modules that can be placed ahead of a GPS receiver to minimize the effects of interference. The AIC-2000 employs temporal filtering and up to 35 dB suppression of pulsed, CW and narrowband interference [77].

The AIC-2000 is an Adaptive Transversal Filter (ATF) which works with a Fixed Radiation Pattern Antenna (FRPA) and provides up to 35 dB of jammer power suppression for pulsed, CW and narrowband jammers. A second generation device, the AIC-2100 can suppress up to 50 dB of interference from as many as 10 simultaneous pulsed, CW or narrowband interferers. It is capable of operating on either the L1 or L2 frequencies. Because the ATF works at baseband, embedded chip set versions of the AIC-2000 and AIC-2100 do not require the relatively expensive RF downconversion/upconversion process needed in the stand-alone version.

Mayflower has combined the AIC 2100 digital ATF technology with adaptive array antenna processing in order to suppress both wideband and narrowband interference. The performance goal is to provide up to 30 dB jammer suppression against ten jammers (3 wideband and 7 narrowband). The antenna array measures 8.6 inches by 9.4 inches and is 0.6 inches high. The array consists of four active L1/L2 antenna elements each integrated with a low-noise amplifier.

It should be pointed out that there are several other programs that deal with wideband jamming. See for example [78,79]. Also, the FAA initiated several years ago a still-active program to locate, identify, and stop jamming interference in real time.

Frequency domain filtering has been used to reject out-of-band as well as in-band interference. Multi-pole ceramic or helical resonators will provide selectivity to the desired signal against out-of-band interference sources. Also, custom designed SAW (surface acoustic wave) filters achieve good selectivity with a very high rejection ratio [80]. According to [80], when the interference is within the signal passband it is very difficult to separate the desired signal from the interference on a spectral basis. Spectral notch filters for GPS applications have not been found to be cost effective when compared with other approaches such as temporal filters. Upton et al. [80] note that, "The principal use of spectral filtering continues to be to insure that the GPS front-end only has to handle the GPS signal and none of the other 'neighboring' users".

Spoofing. As mentioned by Key [48] above, most of the techniques for identifying and ignoring a spoofer have focused on aviation applications.

Mitigation for Maritime Applications

Spoofing and unintentional jamming represent the greatest threats to maritime use of GPS, but the extent of these threats still must be determined. The mitigation methods described above for aviation also apply to maritime applications. In December 2000, the Maritime Safety Committee adopted SOLAS V (Safety Of Life At Sea), a standard that requires "GNSS" (GPS) receivers to be of a type approved by Administrations (cognizant authorities in each IMO nation; for example, the U.S. Coast Guard). Each Administration must establish a quality assurance program in its receiver certification process. The USCG is working on implementing these SOLAS provisions.

The International Electrotechnical Commission (IEC) is investigating both RAIM and GPS susceptibility to unintentional RFI. The IEC is not known at present to be investigating specifically maritime vulnerability to intentional RFI. The IEC also is developing integrated navigation system (INS) standards, which can aid greatly in mitigating some of the vulnerabilities. RAIM has the potential to significantly lower the susceptibility of a GPS receiver to certain forms of spoofing, and maritime RAIM standards are under development. Similarly, requirements, ideally developed by a body such as the IEC, may be needed for jamming protection in a limited number of applications. Such questions are not within the scope of this study. Nevertheless, it is important to point out what mitigation methods apply to maritime operations.

Jamming. With the exception of the dual-aperture (top and bottom mounted antennas) technique called amplitude/phase cancellation, the jamming mitigation methods described above for aviation apply to maritime operations. The shipboard siting of multi-element array antennas may, in some cases, present a problem due to the proximity of reflecting surfaces. Shipboard use of multi-element GPS arrays has not been widely reported in the open literature. If multi-element arrays do not lend themselves to shipboard applications (in some cases), a single aperture antenna with polarization discrimination may still allow for spatial filtering to combat wideband interference. Because some of the jamming mitigation techniques such as adaptive transversal filtering can be built into a receiver for a relatively low cost (less than $100 for the AIC-2000 mentioned above), it seems that some minimal amount of anti-jam protection can be provided.

Spoofing. As mentioned by Key [48] above, most of the techniques used to counter spoofing on an airborne platform apply to a ground based platform as well.

Mitigation for Surface Applications

Positive Train Control

The PTC systems under development are being designed with GPS/NDGPS in mind. In order to obtain FRA approval for implementation of a PTC system, the developer and its client railroad must demonstrate that the PTC system can safely handle a loss of GPS and NDGPS signals. In the event of the loss of GPS the primary impact would be a loss of efficiency rather than reduced safety. In such a situation, a minimal amount of enhanced anti-jam protection would most likely be adequate. An adaptive temporal filter could provide such protection. If spoofing is

determined to be a significant hazard to rail applications of GPS, for example spoofing of the NDGPS data link, most of the techniques applicable to an airborne platform would apply to rail applications as well.

ITS

Some ITS user services are vulnerable to interference, jamming, and spoofing. The effects would primarily be limited to autonomous travel management, mass transit, commercial fleets, and emergency response. Most of these effects would be minor except for hazmat and emergency response. Other user services have not been widely deployed yet. Unfortunately, most of the ITS user services could not afford the high cost mitigation techniques such as multi-element arrays and inertial aiding.

Jamming. Mass transit, travel management, and commercial fleets would be unlikely to bear the expense of special antennas for mitigating wideband jamming as the cost would be several times the cost of the GPS receivers in use. Polarization discrimination is a lower cost possibility, but it still doubles the system cost. In addition, because the users are on the ground it may be less effective against an RHCP jamming signal, since it may directly enter the antenna without having its polarization changed by refraction at the vehicle body.

For these user services, it is probably prudent that the first mitigation technique purchased be effective against CW and narrowband interference/jamming. These are the most common signal types that actually have been documented interfering with GPS. They are also dangerous, since CW can cause undetected navigation errors. Time Adaptive Filtering is the lowest-cost option.

Other user services prone to serious consequences if jammed, such as Emergency and Hazmat Response, should consider the commercial AIC 2000 antenna. Although rather costly, it provides protection against both wideband and narrowband jammers.

The best jamming solution for ITS may possibly be an integrated GPS/Loran-C receiver. Loran-C is hard to jam and the user cost could be on the order of a stand-alone GPS receiver. Integrated GPS/ antennas are available today. It is likely that a mass-produced combination receiver could take advantage of digital processing and software radio technology to be competitive in cost with current GPS receivers. Loran-C enhancements may have to be implemented to deliver two-dimensional positioning accuracy comparable to GPS, but even the current system may be useful as an integrated GPS integrity monitor.

Depending on the course the technology takes, digital cellular 911 positioning possibly could be used as an integrated integrity monitor. However, if the 911 technology for determining user positions incorporates GPS as is now possible, this potentially low-cost approach would not be useful when the GPS signal is degraded or lost.

Spoofing. There are no practical mitigation methods currently available for this type of GPS disruption, although a number of potentially effective techniques have been proposed. Most methods theorized likely would be too expensive for most ITS services. These methods include

Multi-antenna or multi-element antenna systems for interferometry, specialized receiver electronics to detect polarization, amplitude, or Doppler, and methods involving use of an IMU.

The best spoofing solution for ITS may possibly be an integrated GPS/Loran-C receiver. Loran-C is hard to jam or spoof and the user cost could be on the order of a stand-alone GPS receiver. Integrity checking software (enhanced RAIM) could be used to detect out-of-bounds GPS solutions. Loran-C enhancements (see Section 6.2.1) may have to be implemented to deliver two-dimensional positioning accuracy comparable to GPS.

Until the technology is available to ITS users, training operators of critical ITS services about GPS disruption, detection, and alternative procedures is crucial. This will minimize the impact of GPS disruption. Furthermore, training in reporting degradation or loss of GPS signals can facilitate corrective actions.

ITS Communications Links - Interference, Jamming and Spoofing. Many ITS user services rely on wireless data links. Wireless links are the most susceptible to loss resulting from timing synchronization problems caused by GPS disruption. Providers and developers of these services should insure that they are equipped with an adequate secondary timing source to prevent service loss. Critical user services such as Emergency and Hazmat Response should confirm the integrity of their communication links if GPS is disrupted. Alternative communication methods should be developed if appropriate. Training in recognizing and reporting disruption problems, and in using alternative procedures should be performed for these critical services.

(This page deliberately left blank)

ACRONYM LIST

ACARS	Aircraft Communication and Reporting System
ADS	Automatic Dependent Surveillance
ADS-A	Automatic Dependent Surveillance – Addressed
ADS-B	Automatic Dependent Surveillance – Broadcast
AIS	Automatic Identification Systems
AJ	Anti Jam
ALERT	Advanced Law Enforcement and Response Technology
ANSI	American National Standards Institute
APV	Approach with Vertical Guidance
ARINC	Aeronautical Radio Incorporated
ARNS	Aeronautical Radionavigation Service
ASDE	Airport Surface Detection Equipment
ASF	Additional Secondary Phase Factor
A-SMGCS	Advanced Surface Movement Guidance and Control System
ATC	Air Traffic Control
	Automatic Train Control
ATCRBS	Air Traffic Control Radar Beacon System
ATF	Adaptive Transversal Filter
ATIDS	Airport Target Identification System
ATM	Air Traffic Management
ATON	Aid to Navigation
AVR	Associate Administrator for Regulation and Certification
BAH	Booz Allen Hamilton
BPSK	Binary Phase Shift Key
C/A	Coarse/Acquisition
CAT	Category
CDPD	Cellular Digital Packet Date
CDTI	Cockpit Display of Traffic Information
CME	Coronal Mass Ejection
CONUS	Continental United States
COTS	Commercial Off the Shelf
CNS	Communication, Navigation, and Surveillance
CPDLC	Controller Pilot Data Link Communications
CRPA	Controlled Radiation Pattern Antenna
CW	Continuous Wave
DB	Decibel
DGPS	Differential GPS
DME	Distance Measuring Equipment
DoD	Department of Defense
DOJ	Department of Justice
DOT	Department of Transportation
DRFM	Digital Radio Frequency Memory
DTV	Digital Television
FAA	Federal Aviation Administration

FCC	Federal Communication Commission
FDE	Fault Detection and Exclusion
FHWA	Federal Highway Administration
FOC	Full Operational Capability
FOG	Fiber Optic Gyroscope
FRA	Federal Railroad Administration
FRPA	Fixed Radiation Pattern Antenna
GEO	Geosynchronous Earth Orbit
GHz	Gigahertz
GMDSS	Global Marine Distress and Safety System
GPS	Global Positioning System
HDTV	High Definition Television
HHA	Harbor/Harbor Approach
HOW	Hand Over Word
HRI	Highway-Rail Intersection
ICAO	International Civil Aviation Organization
IEC	International Electrotechnical Commission
IGEB	Interagency GPS Executive Board
ILS	Instrument Landing System
IMU	Inertial Measurement Unit
INS	Inertial Navigation System
ISU	Interference Suppression Unit
ITS	Intelligent Transportation Systems
ITU	International Telecommunication Union
IFR	Instrument Flight Rules
JHU	Johns Hopkins University
JPALS	Joint Precision Approach and Landing System
JTIDS	Joint Tactical Information Distribution System
L2c	Planned second civil GPS signal
LAAS	Local Area Augmentation System
LDRCL	Low Density Radio Communications Link
LEO	Low Earth Orbit
LLWAS	Low Level Windshear Alert System
LORAN	Long Range Navigation
MASPS	Minimum Aviation System Performance Standard
MDGPS	Marine Differential GPS
MEO	Medium Earth Orbit
MEMS	Microelectromechanical System
MES	Mobile Earth Station
MHz	Megahertz
MIDS	Multi-functional Information Distribution System
MMAE	Model Adaptive Estimation
MSS	Mobile Satellite Service
MW	Megawatt
NAS	National Airspace System
NATO	North Atlantic Treaty Organization

NAV	Navigation
NAVWAR	Navigation Warfare
NDGPS	Nationwide Differential GPS
NEXCOM	Next Generation Communication
NMEA	National Marine Electronics Association
NPA	Nonprecision Approach
NSTB	National Satellite Test Bed
NTIA	National Telecommunications and Information Administration
NTSB	National Transportation Safety Board
OTH	Over the Horizon
PA	Precision Approach
PAWSS	Ports and Waterways Safety System
PPS	Precision Positioning Service
PRM	Parallel Runway Monitor
PRS	Primary Reference Source
PSL	Power Selective Limiter
PTC	Positive train control
PVT	Position, Velocity, Time
RAIM	Receiver Autonomous Integrity Monitoring
RF	Radio Frequency
RFI	Radio Frequency Interference
RHCP	Right Hand Circular Polarized
RNAV	Area Navigation
RTCM	Radio Technical Commission for Maritime affairs
SARPS	Standards and Recommended Practices
SDH	Synchronous Digital Hierarchy
SONET	Synchronous Optical Network
SOTDMA	Self-Organizing Time Division Multiple Access
SPS	Standard Positioning Service
SSR	Secondary Surveillance Radar
SUV	Sport Utility Vehicle
TCAS	Threat Alert and Collision Avoidance System
TEC	Total Electron Count
TIS	Traffic Information Service
TV	Television
UAIS	Universal Automatic Identification System
UAT	Universal Access Transponder
UHP	Ultra High Performance
UPS	Uninterruptible Power Source
UWB	Ultra Wideband
VDL	VHF Data link
VFR	Visual Flight Rules
VHF	Very High Frequency
VMC	Visual Meteorological Conditions
VOR	Very high frequency Omni Range

VTS	Vessel Traffic Service
USCG	United States Coast Guard
WAAS	Wide Area Augmentation System
WRC	World Radiocommunication Conference

REFERENCES

1. White Paper, "The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63," May 22, 1998.
2. Report of the Commission to Address United States National Security Space Management and Organization, January 11, 2001
3. Martin, K., "GPS Timing in Electric Power Systems," Proceedings of the 12th International Technical Meeting of the Satellite Division of the Institute of Navigation, GPS-99, Nashville, September 14-17, 1999, pp. 1057-1064.
4. Mann, P., and Butterline, E., "Global Positioning System Use in Telecommunications," Proceedings of the 10th International Technical Meeting of the Satellite Division of the Institute of Navigation, GPS-98, Nashville, Sept. 15-18, 1998, pp.1449-1454.
5. Butterline, E., and Frodge, S.L., "GPS: Synchronizing Our Telecommunications Networks," Proceedings of the 12th International Technical Meeting of the Satellite Division of the Institute of Navigation, GPS-99, Nashville, Sept. 14-17, 1999, pp.597-605.
6. Johns Hopkins University Applied Physics Laboratory, "GPS Risk Assessment Study - Final Report," January 1999.
7. U.S Department of Defense and U.S. Department of Transportation, "1999 Federal Radionavigation Plan," February 2000.
8. Federal Aviation Administration, "NAS Architecture Version 2.0," September 1998.
9. U.S Department of Defense and U.S. Department of Transportation, 1996 Federal Radionavigation Plan, July 1997.
10. Federal Aviation Administration, "NAS Architecture, Version 4.0," January 1999.
11. Garvey, J., Presentation to the 44th Air Traffic Control Association Annual Meeting, San Diego, CA, September 26-30, 1999.
12. Validated ICAO GNSS Standards and Recommended Practices (SARPS), November 2000.
13. Minimum Aviation Performance Standards for the Local Area Augmentation System (LAAS), RTCA DO-245, Sept. 28, 1998.
14. "Minimum Aviation Performance Standards for Automatic Dependent Surveillance Broadcast (ADS-B)," RTCA DO-242, Feb. 19, 1998.
15. "The Role of the Global Navigation Satellite System (GNSS) in Supporting Airport Surface Operations," RTCA DO-247, January 7, 1999.
16. Creamer, Paul M., D. H. Alsip and J. P. Radziszewski, "Performance Requirements for the Coast Guard's Differential GPS Service," *Navigation - Journal of the Institute of Navigation*, Vol. 4, No. 4, Winter, 1993-94.
17. "Minimum Operational Performance Standards for Airborne Supplemental Navigation Equipment using Global Positioning System (GPS)," Radio Technical Commission for Aeronautics, Document No. DO-208, July 12, 1991.
18. "Report of the Railroad Safety Advisory Committee to the Federal Railroad Administrator," *Implementation of Positive Train Control Systems*, September 8, 1999.
19. Federal Railroad Administration in cooperation with The Office of the Secretary of Transportation, The Federal Aviation Administration, the Federal Highway Administration,

and The United States Coast Guard, "The Department of Transportation on Civilian Use of the Global Positioning System (GPS): The Nationwide Differential Global Positioning System and Additional Civilian GPS Signals," Report to Congress July 1, 1999.

20. Molitoris, J., Letter on Positive Train Control to Class I Railroad CEOs, September 1998.
21. Johnson, C.M., and Birch, G. E., "Incorporating Standard GPS and Scaling the Precision in Tracking Railroad Assets," Proceedings of the 10th International Technical Meeting of the Satellite Division of the Institute of Navigation, GPS-97, Kansas City, September 16-19, 1997, pp. 1363-1367.
22. Webb, P., "On Track and On Time," *GPS World*, January 1999, pp. 20-26.
23. U.S. Department of Commerce, "A Technical Report to the Secretary of Transportation on a National Approach to Augmented GPS Services," NTIA Special Publication 94-30, December 1994, p.10.
24. Conley, R., "Results of the GPS JPO's GPS Performance Baseline Analysis: The GOSPAR Project," *Navigation - Journal of the Institute of Navigation* Vol. 45, No. 1 Spring 1998.
25. Grudinin, N., and Roytelmen, I., "Heading off Emergencies in Large Electric Grids," *IEEE Spectrum*, April 1997, pp.48-52.
26. GPS Standard Positioning Service Signal Specification, June 2, 1995.
27. Kalafus, R., "Interference to GPS Receivers from Mobile Satellite Emissions," Proceedings of the 11th International Technical Meeting of the Satellite Division of the Institute of Navigation GPS-98, Nashville, Sept. 15-18, 1998.
28. Buck, T, and Sellick, G., "GPS RF Interference via a TV Signal," Proceedings of the 10th International Technical Meeting of the Satellite Division of the Institute of Navigation GPS-97, Kansas City, Sept. 1997.
29. "VHF Transceiver Emissions in the GPS L1 Band," Volpe National Transportation Systems Center Report, February 27, 1995.
30. "Assessment of Radio Frequency Interference Relevant to the GNSS," RTCA DO-235, January 27, 1997.
31. Barrett, Terence, "History of Ultra Wideband Communications and Radar: Part 1, UWB Communications," *Microwave Journal*, Vol. 44 No. 1, January 2001.
32. National Transportation Safety Board Web site: http://www.ntsb.gov.
33. Henry, W., Ohio State Symposium on Aviation Psychology, May 2-6, 1999.
34. NASA Aviation Safety Reporting System Database.
35. "Marine Accident Report – Grounding of Panamanian Passenger Ship ROYAL MAJESTY near Nantucket Island, Massachusetts, June 10, 1995," abstract of Final Report, NTSB Public Meeting, March 12, 1997.
36. Barker, B. and Huser, S., "Protect Yourself! Navigation Payload Anomalies and the Importance of Adhering to ICD-GPS-200," Proceedings of the 11th International Technical Meeting of the Satellite Division of the Institute of Navigation, GPS-98, Nashville, Sept. 15-18, 1998, pp. 1843-1854.
37. Enge, P. and Misra, P., "Scanning the Issues/Technology," Proceedings of the IEEE, Special Issue on GPS, Vol. 87, No. 1, January 1999, pp. 11.

38. Ward, P., "GPS Receiver RF Interference Monitoring, Mitigation, and Analysis Techniques," *Navigation - Journal of the Institute of Navigation*, Vol. 41, No. 4, Winter 1994.
39. Gilmore, S. "The Impact of Jamming on GPS," Symposium on GPS Interference and Mitigation Techniques held at the Volpe National Transportation Systems Center, August 27, 1998.
40. Rodgers, C. "Development of a Low Cost PC Controlled GPS Satellite Signal Simulator," Proceedings of the 15th Biennial Guidance Test Symposium, Holloman AFB, New Mexico, 1991.
41. Winer, B., et al., "GPS Receiver Laboratory RFI Tests," Proceedings of the Institute of Navigation National Technical Meeting, Santa Monica, CA, January 22-24, 1996.
42. Wallis, S., "GPS Open Air Testing - Jamming at Woomera," Proceedings of 1999 Technical Meeting & 19th Biennial Guidance Test Symposium, San Diego, Jan. 25-27, 1999.
43. Colby, G., et al., "Test Results of the Joint FAA/DoD Investigation of GPS Interference," Proceedings of the 10th International Technical Meeting of the Satellite Division of the Institute of Navigation, GPS-97, Kansas City, Sept. 1997.
44. "The Vulnerability of the Differential Global Positioning Satellite (DGPS) Correction Signal Broadcast by Marine Radionavigation Beacons," prepared for the Federal Highway Administration, HSR-10, by ARINC, Inc., January 1997.
45. McDonald, K.D., "Performance Improvements to GPS in the Decade 2000-2010," Proceedings of the 55th Annual Meeting of the Institute of Navigation, Cambridge, MA, June 28-30, 1999
46. Gustafson, D., Dowdle, J., and Flueckiger, K., "A High Anti-Jam GPS-Based Navigator," Proceedings of the Institute of Navigation National Technical Meeting, Anaheim, CA, January 26-28. 2000, pp. 495-503.
47. Hiorth, D., "A New Approach for Suppressing RF Interference of GPS Satellite Signals – Test Results," Paper presented at the 23rd Joint Data Exchange Meeting, Orlando, FL, November 18-21, 1996.
48. Key, Edwin L., "Techniques to Counter GPS Spoofing," Internal Memorandum, MITRE Corporation, February 17, 1995.
49. "Final Report for Loran-C Backup Navigation System Analysis," The Charles Stark Draper Laboratory, Report No. R-2855, February 1999.
50. "Assessment of the Capability of Loran-C to Serve as an Alternative or Complementary System to GPS for En-Route Navigation and Non-precision Approach to Landing," Booz-Allen & Hamilton, Inc., Final Report, June 10, 1999.
51. Fromm, H.H., "Galileo: Responding to the European Infrastructure Needs," Proceedings of the Institute of Navigation National Technical Meeting, Long Beach, CA, January, 2001.
52. Salgado, G., Abbondanza, S., Blondel, R., and Lannelongue, S., "Constellation Availability Concepts for Galileo," Proceedings of the Institute of Navigation National Technical Meeting, Long Beach, CA, January, 2001.
53. "Feasibility Study of INS/GPS/Loran-C Systems for Precision Landings," Galaxy Scientific Corporation, December 30, 1998.
54. U.S. Coast Guard, "Navstar GPS User Equipment Introduction (Public Release Version)," Sept. 1996.

55. Owen, J., "A Review of the Interference Resistance of SPS GPS Receivers for Aviation," *Navigation - Journal of the Institute of Navigation*, Vol. 40, No. 3, Fall 1993.
56. Federal Aviation Administration, "TSO C-129a, Airborne Supplemental Navigation Equipment Using the Global Positioning System (GPS)," February 20, 1996.
57. Pullen, S., et al., "A Preliminary Study of the Effect of Ionospheric Scintillation on WAAS User Availability in Equatorial Regions," Proceedings of the 11th International Technical Meeting of the Satellite Division of the Institute of Navigation, GPS-98, Nashville, Sept. 15-18, 1998.
58. Nichols, J., et al., "High Latitude Measurements of Ionospheric Scintillation Using the NSTB," Proceedings of 1999 Technical Meeting & 19th Biennial Guidance Test Symposium, San Diego, Jan. 25-27, 1999.
59. Kunches, J., "Now It Gets Interesting: GPS and the Onset of Solar Cycle 23," GPS Interference Symposium - Volpe National Transportation Systems Center, Boston, Aug. 27, 1998.
60. Dougherty, P., et al., "The Spatial and Temporal Variations in Ionospheric Range Delay," Proceedings of the 10th International Technical Meeting of the Satellite Division of the Institute of Navigation, GPS-97, Kansas City, Sept. 1997.
61. Klobuchar, J., "Expected Ionospheric Effects On GPS During Years of High Solar Activity," GPS Interference Symposium - Volpe National Transportation Systems Center, Boston, Aug. 27, 1998.
62. Dehel, T., et al., "National Satellite Test Bed (NSTB) Observations of the Effects of Ionospheric Storms on a Prototype Wide Area Augmentation System," Proceedings of the 1999 Technical Meeting of the Institute of Navigation & 19th Biennial Guidance Test Symposium, San Diego, Jan. 25-27, 1999.
63. McGraw, G., and Erlandson, R., "Analysis of Interference to GPS/WAAS by Proposed MSS Spectrum Allocations," Proceedings of the 11th International Technical Meeting of the Satellite Division of the Institute of Navigation, GPS-98, Nashville, Sept. 15-18, 1998.
64. DeCleene, B., "GPS Risk Assessment - FAA Implementation," FAA SOIT, May 20, 1999.
65. "Regional Airline Safety Study," Australian Department of Transport and Regional Services Bureau of Air Safety Investigation.
66. Lavrakas, J. and Knezha, D., "GPS Receiver Responses to Satellite Anomalies," Proceedings of 1999 Technical Meeting of the Institute of Navigation & 19th Biennial Guidance Test Symposium, San Diego, Jan. 25-27, 1999.
67. Kaplan, E.D., (editor), "Understanding GPS: Principles and Applications," Artech House Publishers, 1996.
68. Bond, L, "Overview of GPS Interference Issues," GPS Interference Symposium - Volpe National Transportation Systems Center, Boston, Aug. 27, 1998
69. Bye, C.T., Hartmann, G.L., and Killen, A., "Development of a FOG-Based GPS/INS," Proc. IEEE PLANS, Palm Springs, CA, April 1998.
70. Landry, R., "New Technique to Improve GPS Receiver Performance by Acquisition and Tracking Thresholds Reduction," 6th St. Petersburg International Conference on Integrated Navigation Systems, St. Petersburg, Russia, May 1999.

71. Sennott, J. and Senffner, D., "A GPS Carrier Phase Processor for Real-Time High Dynamics Tracking," Proceedings of the 53rd Annual Meeting of the Institute of Navigation, Albuquerque, NM, June 30-July 2, 1997.
72. Littlepage, R.S., "The Impact of Interference on Civil GPS," Proceedings of the 55th Annual Meeting of the Institute of Navigation, Cambridge, MA, June 28-30, 1999, pp. 821-828.
73. Rodgers, C., et al., "Testing and Analysis of Baseline Length as a Performance Factor in GPS Attitude Determining Systems," Proceedings of the Institute of Navigation National Technical Meeting, San Diego, Jan. 24-26, 1994.
74. Rodgers, C. and Gardner, A. "Testing of Performance Factors in GPS Attitude Determining Systems (ADS)," Proceedings of the 22nd Joint Services Data Exchange for Guidance, Navigation, and Control, Scottsdale, AZ, Oct. 31- Nov. 3, 1994.
75. White, N, Maybeck, P, and DeVilbiss, S, "MMAE Detection of Interference/Jamming and Spoofing in a DGPS-Aided Inertial System," Proceedings of the 11th International Technical Meeting of the Satellite Division of the Institute of Navigation, GPS98, Nashville, TN, September 1998.
76. Vanek, B, Maybeck, P, and Raquet, J, "GPS Signal Offset Detection and Noise Strength Estimation in a Parallel Kalman Filter Algorithm," Proceedings of the 12th International Technical Meeting of the Satellite Division of the Institute of Navigation, GPS99, Nashville, TN, September 1999.
77. Falcone, K., Dimos, G., Yang, C., Nime, F., Wolf, S., Yam, D., Weinfeldt, J., and Olson. P., "Small Affordable Anti-Jam Antenna (SAAGA) Development," Proceedings of the 12th International Technical meeting of the Satellite Division of the Institute of Navigation, GPS-99, Nashville, Sept. 14-17, 1999, pp. 1149-1156.
78. Bazuin, B., Fassler, C., and Schwartz, R., "All-Digital, Spatial Anti-Jam GPS Receivers: Architecture, Implementation, and Initial Performance Results," paper presented at the 12th International Technical meeting of the Satellite Division of the Institute of Navigation, GPS-99, Nashville, Sept. 14-17, 1999.
79. Reynolds, D., Brown, A., Reynolds, A., "Miniaturized GPS Antenna Array Technology and Predicted Anti-Jam Performance," Proceedings of the 12th International Technical meeting of the Satellite Division of the Institute of Navigation, GPS-99, Nashville, Sept. 14-17, 1999, pp. 777-785.
80. Upton, D. M., Upadhyay, T.N., Marchese, J., Greskowiak, D., and Rash, G., "Commercial-Off-The-Shelf (COTS) GPS Interference Canceller and Test Results," Proceedings of the Institute of Navigation National Technical Meeting, Long Beach, CA, January 21-23, 1998, pp. 319-325.