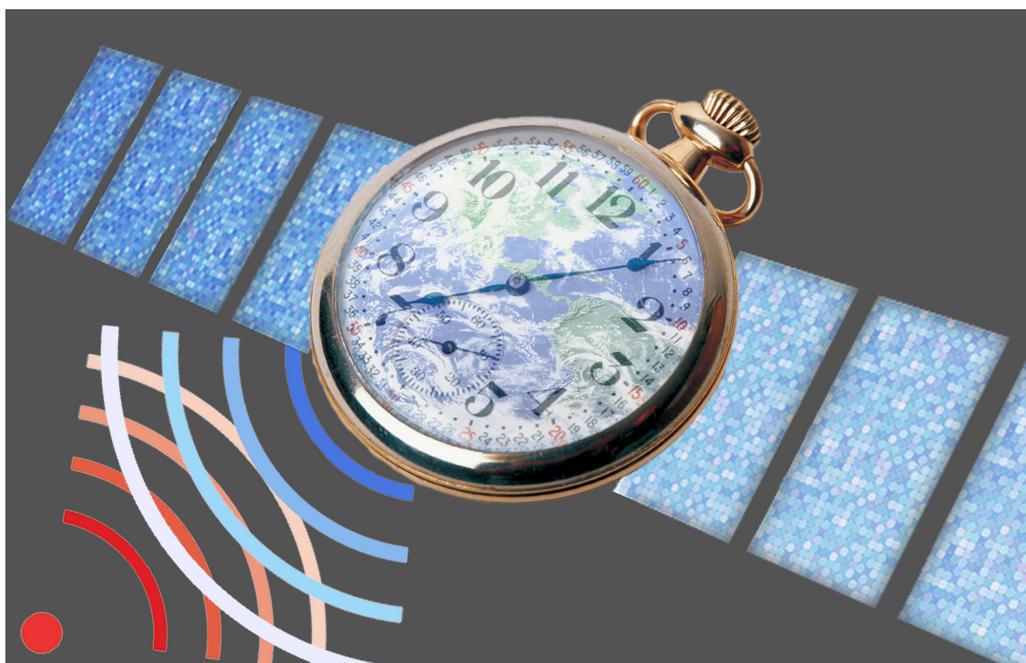




Radio Frequency Interference Impact Assessment on Global Navigation Satellite Systems

*Matthias Wildemeersch, Joaquim Fortuny-Guasch
EC Joint Research Centre, Security Technology Assessment Unit*

EUR 24242 EN - January 2010



The mission of the IPSC is to provide research results and to support EU policy-makers in their effort towards global security and towards protection of European citizens from accidents, deliberate attacks, fraud and illegal actions against EU policies

European Commission
Joint Research Centre
Institute for the Protection and Security of the Citizen

Contact information

Address: Centro Comune di Ricerca
Via E. Fermi 2749, 21027 Ispra (VA), Italy

E-mail: joaquim.fortuny@jrc.ec.europa.eu
Tel.: +39 0332 785104
Fax: +39 0332 785469

<http://www.jrc.ec.europa.eu>

Legal Notice

Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use which might be made of this publication.

Disclaimer

Certain commercial equipment and software are identified in this study to specify technical aspects of the reported results. In no case such identification does imply recommendation or endorsement by the European Commission Joint Research Centre, nor does imply that the equipment identified is necessarily the best available for the purpose.

Europe Direct is a service to help you find answers to your questions about the European Union

Freephone number (*): 00 800 6 7 8 9 10 11

(* Certain mobile telephone operators do not allow access to 00 800 numbers or these calls may be billed.)

A great deal of additional information on the European Union is available on the Internet. It can be accessed through the Europa server <http://europa.eu/>

JRC55767
EUR 24242 EN
ISSN 1018-5593
ISBN 978-92-79-14989-4
DOI 10.2788/6033

Luxembourg: Publications Office of the European Union
© European Union, 2010
Reproduction is authorised provided the source is acknowledged
Printed in Italy

Executive Summary

The Institute for the Protection and Security of the Citizen of the EC Joint Research Centre (IPSC-JRC) has been mandated, in the context of the AA for DG JLS, to perform a study on the Radio Frequency (RF) threat against telecommunications and ICT control systems. This study is divided into two parts. The first part concerns the assessment of high energy radio frequency (HERF) threats, where the focus is on the generation of electromagnetic pulses (EMP), the development of corresponding devices and the possible impact on ICT and power distribution systems. The second part of the study concerns radio frequency interference (RFI) with regard to global navigation satellite systems (GNSS). This document contributes to the analysis of RFI on GNSS and contains a detailed literature study disclosing the weaknesses of GNSS systems. Whereas the HERF analysis only concerns intentional interference issues, this study on GNSS also takes into account unintentional interference, enlarging the spectrum of plausible interference scenarios.

The relevance of this study reposes on three components.

- GNSS is applied in a large number of critical applications. In the field of aviation, GNSS is an aid in all phases of flight. In addition, emergency response operations and monitoring activities depend on GNSS. GNSS became also essential as a precise timing reference and for synchronization purposes in telecommunications networks.
- GNSS signal power levels are extremely low, due to the long satellite-receiver distance.
- RF interference is ubiquitous. The high occupancy of the spectrum around the GNSS frequency bands indicates the high probability of out-of-band emissions, harmonics or intermodulation products. Unintentional interference is mainly originating from satellite communications, TV broadcasting, radar applications and ultra wide-band (UWB) communications. The use of GNSS in military applications or critical infrastructures evidences the concerns around intentional interference, which attempts deliberately to disrupt nominal GNSS operation. In this context, attention should be raised about the spoofing threat, which can potentially be more damaging. Know-how about spoofing is summary and very recent.

Either coming from an intentional or unintentional source, the impact of the interference on the receiver and the corresponding robustness of the service has been determined. Wideband interference can be considered as additional noise and leads to a drop of the carrier power to noise density ratio. The impact of narrowband interference depends on the offset between interference frequency and the closest spectral line of the GNSS code. A maximum jammer-to-signal ratio can be deduced, still allowing nominal tracking. This ratio can be translated in an operating range of the GNSS receiver from the source of interference, given the effective radiated power (ERP) of the interferer.

It is important to have a sound methodology to evaluate the receiver environment

and detect the RF interference. Different methods can be used in successive parts of the receiver processing chain. Spectral analysis can be performed in the analog or digital domain. In the digital domain, detection methods comprise the monitoring of the automatic gain control (AGC) behavior, the monitoring of the acquisition and tracking loops and the estimation of the carrier power to noise density ratio.

Finally, the main purpose is to mitigate the interference. Mitigation techniques start with legal action (spectrum management) and signal design of the GNSS signals. It is very unlikely for unintentional interference to jam on different GNSS frequency bands. Further mitigation can be achieved by spatial or spectral techniques. Spatial mitigation techniques include beamforming techniques. Beamforming and nulling antennas are an efficient means to mitigate broadband interference, while angle-of-arrival discrimination is recommended to mitigate spoofing attacks. Spectral signal processing on the other hand consists of filtering, pulse blanking and techniques deduced from detection theory.

The range of interference scenarios is vast. In this report, the focus is on the unintentional interference originating from UWB transmissions. The main result of former studies is the definition of maximum allowable emission levels for a variety of UWB signals. Further study is still required to assess the impact of aggregate UWB interference, where the interference sources are spatially distributed with high density and in close proximity to the GNSS receiver.

Further activities at the JRC will consist of a robustness study of commercial and professional receivers. The performance of Galileo and GPS signals in the presence of continuous wave and pulsed interferers will be assessed. The vulnerability assessment of the receivers will be conducted using the different detection methodologies specified in this report.

Contents

1	Context	6
2	Introduction	8
3	General introduction to GPS	12
4	Interference outline	13
4.1	GPS vulnerabilities to intentional and unintentional disruption	13
4.2	Sources of unintentional interference	15
4.3	Spoofing of GNSS signals	16
5	Impact assessment of RFI	21
5.1	Impact of wideband and narrowband interference	21
5.2	Effect analysis of RF interference	22
5.3	Effects of interference on GPS C/A receiver	24
5.4	Signal degradation modeling	25
6	Interference detection	27
7	Interference mitigation	30
7.1	Mitigation strategies	30
7.2	Robust receiver design for interference mitigation	30
7.3	Spectral and spatial signal processing	31
7.4	Comparison of different interference mitigation techniques	35
8	Relevant interference scenarios	37
8.1	UWB interference on GPS	37
8.1.1	NTIA report on UWB/GPS compatibility	37
8.1.2	Potential interference to GPS from UWB transmitters	38
8.1.3	Theoretical approach for assessing UWB interference to GPS receivers	39
8.1.4	Co-locating UWB and GPS radios	42
8.1.5	SW approach to assess UWB interference on GPS receivers	43
8.2	TV/FM interference on GPS	43
9	Implemented HW for interference mitigation	46
10	Summary	49
	ANNEX A: Interference Detection	50
	ANNEX B: Detailed Literature on Interference Mitigation	54
	ANNEX C: Detailed Literature on UWB Interference on GNSS	58

1 Context

The JRC-IPSC has been mandated by the EC DG Justice, Freedom and Security to study the radio frequency threat against telecommunications and ICT control systems. The study is divided in three work packages:

WP1 - Study on European capabilities encompasses an inventory of existing European capabilities (theoretical and practical) for the analysis of RF threats in the EU Member States. This overview will cover EM immunity tests, simulation of jamming, current detection-, localization- and mitigation methods for threat agents.

WP2 - Preliminary RF risk and threat assessment shall carry out a risk and threat assessment of some significant RF threats to telecommunications and ICT control systems. In this WP a methodological approach will be defined for future RF threat assessment. This comprises the identification of some RFI scenarios (e.g. harmful electromagnetic environments, attack means, etc.) In this WP distinction will be made between high and low energy RF threats.

- ☑ WP2.1 covers the first group of HERF threats. To this group belong the electromagnetic pulses (EMP), inducing physical damage to all types of conducting networks.
- ☑ WP2.2 will deal with low energy RF threats. Those threats do not cause any physical damage, but the performance of the victim system can be affected. WP2.2 will focus on a highly vulnerable electronic system, that is, GNSS receivers and the respective consequences of service disruption. Besides the use for navigation purposes, the GNSS signal is used in different critical infrastructures for the highly precise and stable time reference. In power supply networks as well as in telecommunication networks, the GNSS signal is used for time synchronization purposes. The study will elaborate on RF interference, intentional and unintentional, using commercially available sources. A summary of the detection techniques of RFI sources will be provided, as well as an overview of the current mitigation techniques to alleviate the GNSS vulnerabilities. This report covers WP2.2

WP3 - RF threat experimental work is the largest WP where theoretical development, simulation and experimental work will be combined, related to the RF threat on GNSS receivers. The following activities will be performed:

- ☑ Identification of the critical infrastructures relying on GNSS signals and the standards that can interfere with GPS/GALILEO. Distinction will be made between applications that use strictly the timing information and those used for navigation purposes. In the latter, higher accuracies can be reached by differential phase measurements.

- ☑ An emulator will be developed modeling a complete GNSS system. The emulator will comprise of a signal generator for the GNSS and interfering signals, a receiver front-end and a SW defined receiver, performing the signal demodulation and performance analysis. Mitigation algorithms will be implemented and tested.
- ☑ Finally tests will be performed (conducted and radiated) to validate the work performed.

2 Introduction

RF interference has the same effect as signal blockage, foliage attenuation, ionospheric scintillation and multipath, i.e. they all reduce the effective signal-to-noise ratio of the GPS signals. This report contains an overview of the RFI threats on GNSS systems and makes an inventory of different interference detection and mitigation techniques. In risk assessment there are two fundamental components to consider, i.e. the probability of occurrence and the potential loss due to the threat agent.

The probability of occurrence is related to the probability of the presence of an interferer, intentional or unintentional, and to the power ratio between interferer and the GNSS signal. The minimum GPS¹ signal power levels are specified and are approximately 10^{-16} W. Yet, the power level lies about 15dB below the RF background noise level of the receiver. Therefore, GPS signals are highly susceptible to tropospheric and ionospheric effects, multipath, blockage in urban canyon and interference originating from narrow- and wideband sources. The radio regulatory agencies protect the GNSS spectrum and limit the amount of energy that can be transmitted in the GNSS frequency bands. However, out-of-band emissions, harmonics and intermodulation products can harm the GNSS signal. The high occupancy of the RF spectrum around the GNSS bands gives a qualitative indication of the risk. The Volpe National National Transportation Systems Center published already a vulnerability assessment of GPS [1]. The report gives an overview of intentional and unintentional disruption of GPS service and discusses on high level for both cases the possible mitigation strategies.

The second component of a risk assessment concerns the potential loss caused by the interferer. The potential loss is related to the number of applications where GNSS is used. An overview is given in Table 1. The use of GNSS systems for navigation purposes is evident by its name. GNSS is for instance a key technology in aviation where it can be used in all phases of flight, this in contrast with the traditional phase-of-flight-specific traditional navigation solutions. The most demanding aviation objective is to support auto-landing, combining different requirements, ranging from accuracy to integrity and interference rejection in hostile jamming environments. Further, there are several ap-

¹We take the Global Positioning System (GPS) as an example of a GNSS system. In this report we will use the term GNSS as the generic name of all navigation satellite systems. When necessary this term will be specified.

Critical applications	
<i>Sector</i>	<i>Application</i>
aviation	precision and nonprecision approaches
marine	harbor, harbor approach and constricted waterways
surface	emergency response operations
communications	timing and synchronization

Table 1: Critical applications

plications related to health safety and emergency services. For ambulance services, standard arrival times are determined depending on the gravity of the situation. Other examples include police and fire services or search and rescue activities. The potential impact of loss of the navigation service depends on the reliance on GNSS. It should be noted that except for navigation purposes the GNSS signal is also used as a precise timing reference for power grids, for telecommunications networks, furthermore in astronomy and banking applications. UTC (Universal Time Coordinated) is based on International Atomic Time (TAI), which is derived from hundreds of Caesium clocks located in different standards laboratories. GPS system time is steered to UTC, from which it will not deviate by more than one microsecond. The exact difference is contained in the GPS navigation message, giving the time difference and rate of GPS time with respect to UTC. The frequency stability of GPS system time is about $2 * 10^{-14}$ and is used widely for network synchronization requiring an accuracy higher than 10^{-11} . The initial need of precise timing distribution over networks came from telecommunications industry. The signal of a single master clock is distributed to the network nodes at a different layer or stratum. A hierarchical structure with different performances on each stratum is constructed. There is a performance degradation due to the distribution through the levels. Note that there is few flexibility with respect to the number and the location of the nodes. The most obvious benefit of the use of GNSS is that a synchronization network with different layers and corresponding nodes is not longer necessary. All network nodes have direct access to the main synchronization signal. This evidences the benefits of the use of GNSS for applications with a need of a high level of synchronization over a wide geographical area. In what follows three examples are given of currently used synchronization applications.

GPS timing in electric power systems Timing systems are used to large extent in electric power supply networks. [2] describes how GPS time has become an important part in monitoring, control, maintenance and analysis tool. A short overview:

- ☑ *Generation control.* In electric power networks the generation and load must be in balance at all times. An automatic generation control system is employed to continuously adjust the generation. Errors in frequency or power measurement will become clear as system frequency offsets and unforeseen power exchange respectively. The need for an accurate frequency measurement is obvious.
- ☑ *System protection.* Protection equipment (relays, circuit breakers) detect power line faults and loss of synchronism. Some of this equipment is used very incidentally (once during its lifetime). This evidences why power systems are extensively monitored. Events are recorded and time stamped. A very accurate time synchronization is required to this purpose.
- ☑ *Fault location.* Current fault location techniques locate power line faults by comparing the arrival times of traveling waves on either side of the fault.

- ☑ *Phasor measurements.* A lot of applications benefits from phasor measurements. To maintain system integrity, stability control schemes are designed. State estimation is widely used to determine system stability from system voltage and phase angle.

GPS timing in telecommunications Precision timing is the cornerstone in telecommunications networks. The error-free transmission of information is only possible through precision synchronization [3]. Timing impairments or slips occur when the receiver clock runs slower or faster than the transmitter clock, leading to the repetition or deletion of data. Enhanced timing accuracy improves the service reliability and can increase the throughput of data. Timing inaccuracies on the other hand contributes to increased levels in voice applications or frequent retransmissions in data applications. High levels of synchronization are ensured by a highly stable frequency source and the distribution of that signal through the entire network. GPS has a lot of advantages with respect to other clock technologies. The current use of GPS is evidenced by the decreasing cost, the ubiquitous availability and the long term frequency accuracy. The need for quality synchronization is different for each telecommunications technology.

- ☑ In *PSTN* (Public Switched Telephone Network) the motivation for network synchronization is due to digital switching via time slot interchange. Time slots are often created in one office and switched at another one. In a complex network of digital switches it is clear that synchronization is needed to prevent impairments (e.g. slip). Degradation of the synchronization can cause jitter, wander or phase transients. Slip buffers are used to overcome the mentioned impairments. Over- or underflows of the buffer caused by too large phase offsets can induce slip: a complete frame of data is repeated or deleted.
- ☑ In *SONET* (Synchronous Optical Networks) frequency differences between network elements are accommodated by pointer processors. Excessive pointer adjustments can lead to payload errors.
- ☑ *CDMA* requires a timing reference as well as a frequency reference.
- ☑ *GSM/TDMA* requires only a stable frequency reference.

All discussed technologies have in common that they need a means for synchronization. The most common method to date has been a master slave arrangement. This solution employs caesium technology to provide the required frequency stability. Master clocks distribute timing throughout a transmission network. More recently the cost-attractive alternative is a GPS-based overlay synchronization network. With regard to Caesium technology, this technique gives rise to a considerable cost reduction, but is subject to radio interference. Moreover, GPS integrity can be affected by common factors as signal masking. A solution can be provided by a combination of GNSS and caesium timing sources. In this setup, the caesium clocks are the primary reference source and GNSS the slaved source.

GPS timing in financial and banking applications The banking and financial community does not have stringent requirements on timing and synchronization. Yet, a time reference is widely used for event logging, security purposes and document timestamping. Log entries refer very often to the internal clock for setting a timestamp. The implementation of a global time reference could improve network security. In order to protect high-value information, a two-factor authentication is required. Time synchronous authentication covers the concept of a password only valid for a precise moment in time.

In [4] an overview is given of the reliance on GNSS of different services and the impact of the loss of GNSS on those services is assessed. In telecommunications networks there is a high dependency on a hierarchy of timing sources. Primary time references are usually based on caesium clocks and GNSS based sources are increasingly used elsewhere in the network. Loss of synchronization due to the lack of a GNSS signal, would occur in days for systems reliant on GNSS conditioned high quality quartz clocks, and would begin to occur in a week to a month for systems based on GNSS conditioned rubidium sources. These times depend on the precision requirements of the service in question. A persisting loss of GNSS would lead to a decreasing network performance, depending on the stability of the backup time source. Therefore, for telecommunications networks, the short term loss less than one week of GNSS would be an inconvenience, however on the longer term greater than one week, the loss could be critical. For broadcast systems as Digital Audio Broadcasting (DAB), the loss of GNSS would cause a gradual decrease of reception quality. The impact analysis has been repeated for other user groups. Different industries have been considered, as road, rail, aviation, maritime, search and rescue, finance, etc. The dependency on GNSS for many user groups has grown and will grow to a critical need, although low received power levels and satellite visibility. Some of the communities account for these issues while others do not.

This introduction makes clear that there are three main incentives to analyze the threat of RF interference. First, the GNSS power level is inherently low. Further, RF interference is ubiquitous. The origin of the interference can range from out-of-band emissions, harmonics, intermodulation products and channel effects. Finally, a big variety of critical infrastructures makes use of GNSS for synchronization purposes. Those three arguments underline the relevance of a sound threat analysis related to GNSS. This report starts with an effect analysis of RF interference on the signal quality. Different metrics are introduced that quantify the degradation of proper operation. Further, an overview of the interference detection techniques is given and different mitigation techniques are introduced. They alleviate the RFI threat in different parts of the processing chain. Finally, special attention is given to the specific scenario of UWB interference.

	GPS	GALILEO
<i>Frequencies/Bandwidth(MHz)</i>		
Galileo E5a		1176.45/27.795
GPS L5	1176.45/27.795	
Galileo E5b		1207.14/23.205
GPS L2	1227.6/22	
Galileo E6		1278.75/40
GPS L1	1575.42/24	
Galileo L1		1575.42/32
<i>Power level (dBm)</i>		
Galileo E5a		-125
GPS L5	-127.9	
Galileo E5b		-125
GPS L2	-130	
Galileo E6		-125
GPS L1	-128.5	
Galileo L1		-127

Table 2: GNSS system parameters

3 General introduction to GPS

A thorough introduction and more detailed information can be found in [5, 6, 7, 8, 9]. The GPS system consists of three segments: the space segment, the user segment and the control segment. The control segment tracks all satellites and uploads periodically clock time corrections and predictions of the satellite trajectories. The power level of the signal is only -160 dBW. The highest power density of the spread spectrum signal is -220 dBW/Hz where the nominal background noise level is approximately -205 dBW/Hz, i.e. the signal strength lies 15 dB beneath the background noise level.

We would like to draw attention on the frequency assignment of different GNSS systems: GPS and GALILEO. The choice of frequencies is a complex combination of many technical and nontechnical parameters. Regarding the technical properties, propagation capabilities through the terrestrial atmosphere of good quality are required. Essentially this involves frequencies above 1 GHz. With regard to the GPS C/A code, a degradation of the SNR of a few decibels is already sufficient to prevent signal acquisition. The assignment of frequencies is achieved under the coordination of the ITU. The major system parameters of GPS and GALILEO (frequencies, bandwidth and power levels) are summarized in table 2.

4 Interference outline

The GPS signal level lies approximately 15 dB under the background noise level. The spread spectrum processing gain is about 60 dB. By consequence, if an interfering signal is introduced in the receiver location with power 45 dB higher than the noise floor, then the receiver is completely jammed. Interference signals can be classified as follows.

- ☑ *Narrowband interference* can be modeled as a continuous wave at a specified frequency.
- ☑ *Broadband interference* has a flat power spectral density over a wide range of frequencies. This type of interference can be modeled as additive white gaussian noise.
- ☑ *Pulsed interference* can be characterized by a pulse duty cycle.

The most efficient jamming technique makes use of the spread spectrum GPS codes and the GPS code-chipping rate. With this approach the power spectrum of the jammer matches perfectly the power spectrum of the GPS satellite signals. Operation of a receiver in the proximity of ground-based transmitters will result to a considerable extent in the jamming of GPS satellite signals. The intentional transmission of false, but stronger signals is able to capture a GPS receiver: this is called spoofing. The military antispoofing Y-code uses encryption and thus, minimizes the spoofing risk. In this chapter, an overview shall be given of (un)intentional interference and spoofing. In the rest of the document, focus will be on unintentional interference.

4.1 GPS vulnerabilities to intentional and unintentional disruption

Civilian use of GNSS services grow rapidly because of the quality, the ease of use and the low cost of the service. Existing and planned uses of GPS are widespread. It has even been stated that GPS has the capability to serve as the only navigation system in the United States. At that point the limitations and vulnerabilities of the system should be made evident. The Volpe report identified some critical applications that are illustrated in table 1 on page 8. Distinction is made between intentional and unintentional disruptions. *Unintentional interference* includes ionospheric effects, RFI, signal blockage and multipath. Intentional disruption include jamming, spoofing, meaconing and deliberate attempts to shut down GPS operations. For unintentional interference the current services of concern comprise broadcast television, VHF interference, personal electronic devices (PEDs), mobile satellite service (MSS) and UWB radar and communications. The emissions of MSS communications systems are regulated such that a single device can not raise the noise level of the GPS receiver causing disruption. Handheld MSS Mobile Earth Stations transmit in the 1610-1660.5 MHz band. The effect of a cluster of MSS devices is however not studied. The spurious and harmonic emissions of geostationary satellites (1525-1559 MHz band) are also a potential source of RF interference. UWB interference

will be discussed in a following section. *Intentional interference* can be jamming, spoofing and meaconing. Jamming concerns the emission of RF energy of sufficient power to prevent signal acquisition. Low power airborne jammers (1 watt) can already cause loss-of-lock at 10km distance and prevent acquiring lock at a range of 100 km. Jammers which have the same type of spread spectrum as GPS have an even more dramatic effect. Spoofing is the transmission of legitimate-appearing false signals while meaconing is the reception, delay and rebroadcast of radionavigation signals.

The literature around interference issues for the Global Positioning System is vast. [10] gives a good introduction in the field. The low power level of the GPS signals explains the susceptibility for interference. A 1W noise signal is sufficient to prevent a receiver to perform C/A signal acquisition up to a distance of 100km. Even though the P(Y) signal can theoretically directly be acquired, the processing is extremely slow due to the 1-week-long chip duration of the P(Y) pseudonoise. A military receiver will acquire first the C/A signal to obtain the accurate system time. In other words, also for the military receiver the 1W jammer at a distance of hundred kilometers can compromise the signal acquisition. In fact, it is not surprising that most military platforms have a redundant inertial navigation system, complementary during GPS outages.

Accuracy is a key feature for GPS performance. The measures to improve GPS performance are numerous. On the *signal level* different actions can be taken. First the signal power level can be increased. To this purpose also spot beams and pseudolites can be considered. Then the signal structure can be altered to enhance processing gain and improve antijam capability. Currently, the C/A signal accessible to the civil community is limited to the L1 frequency band. As a consequence corrections for ionospheric delay can not be obtained by the civilian GPS receiver. Military receivers on the other hand use both L1 and L2 frequencies. Future policy foresees C/A code on frequency L2 and moreover a third frequency L5. Concerning the *user equipment*, performance can be enhanced by using different antenna topologies. Beamforming techniques and adaptive signal processing cause the interfering signals to cancel and combine coherently the satellite signals, providing therefore antenna gain in the direction of the satellites. The use of massive correlators improves the robustness of the signal processing. Finally the *jammer sources* can also be addressed directly.

The GPS satellite navigation system is designed to serve both commercial and military applications. It is obvious that the use in military systems necessitates a high level of robustness and a significant tolerance to interference and jamming. This requirement was an important consideration in the design of the signal structure. The GPS C/A and P(Y) signals are both spread spectrum signals and are as such less susceptible to narrow-band interference. Moreover, the GPS frequency bands are licensed by international frequency assignments. With respect to intentional and unintentional interference, GPS can be characterized by a higher level of robustness with regard to conventional narrowband signals. The most important advantages are:

- Spread spectrum signals can tolerate significantly larger amounts of co-channel of

adjacent channel interference than narrowband signals.

- The GPS signal sources are located on satellites. As a consequence they are not easily disturbed by natural disasters. With respect to that, ground-based transmitters are much more vulnerable. Furthermore, generally the number of available satellite signals is bigger than the required number for position calculation. In other words, the position determination problem in many cases overdetermined and therefore robust.
- Receivers can be equipped with detection mechanisms for interference. If detected, corrective actions can be taken by a wide variety of mitigation strategies.

It is however obvious that any radionavigation system can be disrupted by an interference source of sufficiently high power. In such situation, the receiver can be designed to switch over to a redundant navigation system based on other sensors, such as inertial measurement units (IMU).

4.2 Sources of unintentional interference

The possible sources of unintentional interference can be summed up as follows:

- Pulsed interference from radar signals in nearby frequency bands that are inadequately filtered
- Accidental transmission in the wrong frequency band
- Out-of-band interference caused by nearby transmitters. This can be solved by adequate filtering in the GNSS receiver
- Harmonics and intermodulation products of various ground and airborne transmitters. Those transmitters should be sufficiently filtered to avoid interference in the GPS frequency band. The harmonics and intermodulation products can also originate from the oscillators or transmitters on the same platform as the GPS receiver. Measures should be taken to prevent radiation coupling into the GPS receiver.

The frequency bands assigned for satellite navigation systems (GPS and Galileo) are summarized in table 2. The nearby frequency bands used for satellite communications are listed in table 3. Just underneath the GPS L1 band there is a satellite-to-ground link. The expected power levels received on earth are low. However, the 1610-1626 MHz frequency band is a licensed uplink band for satellite-based cellular phones. It is obvious that the close proximity of this uplink at only 24.58MHz above the upper edge of the GPS spectrum requires adequate filtering for the a GPS receiver. The same comments hold for the aeronautical satellite communications uplink. Moreover, if the transmitter is on the same platform as the GPS receiver, there should be enough antenna separation and isolation to prevent overload the GPS low noise amplifier (LNA). Finally, attention is drawn to the harmonics of improperly filtered TV channels. They can be a potential source of interference in the vicinity of a TV transmission tower.

<i>Frequency (MHz)</i>	<i>Bandwidth (MHz)</i>	<i>usage</i>
525		UHF television at 1/3 GPS L1
782-788	51	UHF television at 1/2 GPS L1
1535-1559	24	space-to-ground: several bands for satellite downlinks to mobile, marine and aeronautical users
1610-1626.5	16.5	earth-to-space uplink and satellite based cellular
1626.5-1660.5	34	Aeronautical satellite communications uplinks (possible intermodulation products)

Table 3: Frequency bands assigned for mobile satellite communications

4.3 Spoofing of GNSS signals

While interference issues and jamming are extensively studied in literature, the potentially more damaging spoofing has been given little attention. In the publicly available sources, only a limited number of publications could be found [11, 12, 13, 14, 15, 16, 17, 18]. During a jamming attack, the victim receiver loses position lock, but is aware of this event. A spoofing attack on the other hand, is surreptitious in the sense that the victim is not aware of the attack. The victim receiver is fed with corrupted information and continues calculating counterfeit position, velocity and time (PVT). Concerns about the authenticity of the signals is usually related to military applications. At present, two GPS signals are broadcasted: a civilian unencrypted signal and a military encrypted signal. The civilian signal was never intended for critical or security applications, but unfortunately, this is how the civilian signal is often used. Critical infrastructures rely heavily on civil GPS for navigation and timing in the field of telecommunications, banking and finance, power supply control systems, aircraft guidance, public transport, tracking of dangerous goods, electronic toll collection etc. GNSS is gaining as well importance in law enforcement. In fisheries for instance, ships have onboard vessel monitoring systems (VMS), that report real-time position to monitor compliance with regulations. Spoofers can allow those vessels to hide their actual location. As the number of civil safety- and security-related applications based on GPS is growing, it becomes a tempting target for spoofing.

The issue of intentional interference is of growing concern throughout the world. The 2001 Volpe Report, Vulnerability Assessment of the Transportation Infrastructure Relying on GPS [1], stated clearly that the anti-spoofing techniques for civilian applications should be made available and observables identifying spoofing should be provided. The study recommended studies to characterize the spoofing threat in order to identify vulnerable areas and detection strategies. At the moment of this writing, civil GPS receivers are as vulnerable as before to this threat. In [16], the authors did an informal survey in which

several manufacturers of high quality GPS receivers revealed to be aware of the spoofing vulnerability, but at the same time very skeptical about the spoofing threat. They did not implement any spoofing countermeasures. The Volpe report also cites an internal memorandum [19] in which several techniques to counter spoofing are presented.

1. Amplitude discrimination
2. Time-of-arrival discrimination
3. Consistency of navigation inertial measurement unit cross check
4. Polarization discrimination
5. Angle-of-arrival discrimination
6. Cryptographic authentication

Techniques 1 and 2 are easy to implement on a software-defined GPS receiver, but are only effective against simple spoofing attacks. Techniques 3 to 5 require additional hardware and as a consequence, those techniques are unlikely to find widespread adoption. The cryptographic authentication require a change of the civil GPS structure, which again, is very unlikely to happen. The research arm of the US Department of Homeland Security has also considered the threat of civil GPS spoofing [12]. Their shortlist of spoofing countermeasure is similar to the techniques proposed by Key [19], but more importantly, none of the proposed techniques would adequately defend against a sophisticated spoofing attack.

Spoofing scenarios can be divided among static and dynamic cases. In the static case a receiver is mounted with clear sky view on the top of a building. A possible example is a timing receiver, used to synchronize a communications network, for control of the power grid or for global trading synchronization. In [17, 18, 16], the authors divide the spectrum of spoofers along simplistic, intermediate and sophisticated. The simplistic attack is set up by means of a GPS signal generator, a power amplifier and an antenna. Every stand-alone civilian GPS receiver available today is vulnerable to such spoofing attack. Fortunately, attacks as discussed before are easy to detect. However, this fact does not result in higher security. The vulnerability remains until the implementation of rudimentary spoofing countermeasures in civilian GPS receivers. The intermediate attack is set up by means of a portable receiver-spoofers. The receiver component uses the genuine GPS signal to estimate its own position, velocity and time. The spoofer component further generates counterfeit signals, with the characteristic that at the phase center of the target antenna the counterfeit and genuine signals are aligned. Such attack could be difficult to detect, even for target receivers equipped with stable oscillators and a low-drift inertial measurement unit (IMU). The probability of an attack, orchestrated by such a device, is currently low, since receiver-spoofers are not readily available. Nonetheless, the emergence of software-defined receivers increases the likelihood of such attack. Finally, a sophisticated attack can be deployed by means of multiple

phase-locked portable receiver-spoofers. The angle-of-arrival detection countermeasure can be bypassed by means of a coordinated attack with as many receiver-spoofers as there are antennas on the target receiver. The only known defense against such attack is cryptographic authentication. The software-defined receiver-spoofers have been implemented at Cornell University. Spoofing attacks have been demonstrated inserting authentic GPS L1 C/A signals combined with counterfeit signals in a target receiver. The receiver-spoofers could accurately reproduce the code phase, frequency, data bit values and relative amplitudes of all visible satellites. The spoofing attack has been visualized using 81 correlator taps around the prompt tap, which is aligned with the incoming signal. The counterfeit signal aligns with the genuine signal, gradually increases its power and finally drags the tracking points away from the genuine signal. A representation of the baseband genuine and counterfeit signal as phasors in a complex plane indicates that a spoofing phasor could also be produced, suppressing the authentic phasor. Combined with data bit prediction, such an attack could be impossible to detect relying only on user-equipment-based defenses. As far as the authors are aware, it appears that nothing but cryptographic authentication can guard against such a sophisticated spoofing attack.

In [16], the authors explain how they implemented two software-defined user-equipment-based defenses. Although not spoof-proof, they are straightforward to implement and increase to high extent the difficulty to mount a spoofing attack. The first technique, the data bit latency defense, monitors continuously data bit sign changes. If a data bit sign change is detected unexpectedly, the target receiver raises a flag. The second method, the vestigial signal defense, is based on the complexity of suppressing the genuine signal after the tracking points have been pulled away by the counterfeit signal. The construction of an effective signal suppressor requires very precise knowledge of the carrier phase at the phase center of the target antenna, i.e. cm-level knowledge of the vector between the transmitter and receiver phase centers. This would be very challenging, except in static situations, in close proximity of the target receiver. If the authentic signal is not suppressed and the correlation points are monitored over a larger interval, a remainder of the genuine signal can still be distinguished. The authentic signal can be detected by subtracting the tracked, counterfeit signal from the incoming signal and performing acquisition on this data.

In [17, 18], the same authors demonstrate the use of a dual-antenna receiver applying an angle-of-arrival spoofing countermeasure. This technique is supposed to be effective against all but the most sophisticated spoofing attacks. The phase difference between the two antennas is monitored over time. It can be observed that the phase difference changes due to the satellite motion and the rate of phase difference is proportional to the baseline length. The expected carrier phase differences can be calculated and compared to the measured delta phases. During an indoor experiment, the authors were able to demonstrate the carrier phases did not change over time, indicating the presence of a malicious transmitter.

With the foreseen addition new GNSS signals, the cost of mounting a spoofing attack

risers explicitly. However, faster DSPs or FPGAs would make a multi-signal attack possible. Thus, claims that spoofing will get unfeasible in a multi-signal environment or due to precise real-time positioning requirements are misleading and give a false sense of security. The ubiquity of GPS has made the launching of a spoofing attack very attractive in the pursuit of financial gain. Moreover, in the context of an increasing dependency of critical infrastructures on GNSS, a spoofing attack could have destabilizing effects and thus, authenticatable signal architectures are needed. In [15, 13, 14], an overview is given of different possible user and signal authentication methods. Possibilities range from navigation message authentication (NMA), public and private spreading code authentication to navigation message encryption and spreading code encryption.

Navigation Message Authentication denotes the authentication of satellite signals by signing digitally the navigation message. The navigation message consists of a data block D_N , containing the navigation data, and a digital signature D_S , which is computed by hashing the data block and subsequently encrypting the hash value with a signing key k_s . The receiver authenticates the incoming signal by comparing the hash function of the data blocks with the outcome of the decrypted signature, using the publicly known validation key k_v . Therefore, the receiver can only authenticate the signal after reception of the entire navigation message and the digital signature, resulting in a authentication delay. Time to alert requirements used in civil aviation, can not be met.

Public and Private Spreading Code Authentication can be added to NMA, using additional spreading codes in certain time windows. Spread spectrum security codes (SSSC) are an enlargement of the digital signature in the form of pseudorandom sequences. In public spreading code authentication the digital signature of the current navigation message is used to generate the SSSCs. Private spreading code authentication on the other hand, uses the digital signature of the last navigation message as seed to generate the spreading code sequence, encrypted with a symmetrical encryption system. For the public authentication method, time-to-alert limits can not be achieved, while for the private method, authenticity can be accomplished in every time window.

Navigation Message Encryption uses a symmetric system to encrypt the data modulated on the satellite ranging signals. This system can provide authentication if the user community is trustworthy or by encapsulating the symmetric encryption key in tamper-resistant hardware.

Spreading Code Encryption can accomplish user and signal authentication. Yet, the process is far more complex.

NMA has some attractive characteristics. It does not need any tamper-resistant hardware in the user terminal, key distribution can be managed efficiently by means of a public

key infrastructure and finally, NMA does not require the dissemination of confidential information to the user community. Therefore, NMA is the preferred technology for GNSS authentication. Ideally, the combination with a non-cryptographic spoofing countermeasure should be implemented.

The final paragraph illustrated the different, effective cryptographic spoofing countermeasures. The reality on the other hand is unfortunately less reassuring. Currently, the military GPS services apply user and signal authentication methods by means of spreading code encryption. Still, no cryptographic authentication is foreseen for the future civil GPS signals. For Galileo the perspectives differ along the different services. For the Open Service (OS), signal authentication nor data encryption are foreseen. For the Safety of Life (SoL), Commercial service (CS) and Public Regulated Service (PRS), different signal and user authentication methods are anticipated. For none of the augmentation systems, cryptographic methods are planned.

5 Impact assessment of RFI

RF interference can be sorted according to several characteristics. Distinction is first made between wideband and narrowband interference. Further, interference can be classified according to its properties in time, i.e. its continuous or pulsed nature. GNSS receivers are tolerant to pulsed interference as long as the pulses are short with respect to the bit duration of the GNSS signal. The worst interference case is a continuous interference. The need to understand the robustness of GNSS receivers against RF interference necessitates a brief introduction in Direct-Sequence Spread Spectrum (DSSS) [20]. The basic principle of spread spectrum techniques is that the signal occupies a larger bandwidth than the necessary bandwidth for transmission. Thus, the technique allows to receive signals below the noise floor, it enables different users to use the same signal bandwidth and - what is important in this discussion - has a high resistance against RFI and intersymbol interference which is due to multipath components. The modulation of the signal makes use of a spreading code. During demodulation, the received signal is correlated with a synchronized version of this spreading code. The received signal can be represented as $r(t) = s(t) + n(t) + i(t)$, where $s(t)$ is the transmitted signal, $n(t)$ is noise and $i(t)$ is the interference. Considering only the interference term, during the despreading $i(t)$ is multiplied by the spreading sequence $s_c(t)$, resulting in their convolution $I(f) * S_c(f)$ in the frequency domain. Hence, the interference energy is spread over the bandwidth of the spreading code and by demodulation the power of the interference is reduced by the processing gain $G = BW_{code}/BW_{data}$.

In this section, we give first an overview of the robustness of GNSS receivers against wideband and narrowband interference. Further, a deduction of the maximum jammer-to-signal ratio will be presented. This analysis provides more insight in the relation power-distance of the jammer, allowing proper operation of the GNSS receiver. Finally reference is made to some more detailed literature.

5.1 Impact of wideband and narrowband interference

Wideband interference is defined here as interference with a bandwidth greater than the one of the victim signal [7]. The power spectral density (PSD) of the interferer is added to the PSD of the ambient noise and consequently the ratio C/N_0 becomes $C/(N_0 + J_0)$, and as such the wideband interference is considered as additional noise. If $n_{tot}(t) = n(t) + i(t)$, the despreaded noise is represented by $n'(t) = n_{tot} s_c(t)$. However, $n'(t)$ has approximately the same Gaussian distribution as $n(t)$ and therefore, spreading and despreading have no impact on the raise of the carrier-to-noise ratio for wideband interference.

Still, the benefit of DSSS is huge when we consider narrowband interference. We stated already before that the processing gain of the spread spectrum modulation is given by $PG = BW_{code}/BW_{data}$. This holds when the spectrum of the GNSS signal is smooth. The GPS signal uses however a finite length spreading code. Due to the repetitive nature of

the spreading code the spectrum features line components. In what follows, we illustrate the impact of the line spectrum on the processing gain. The received signal is equal to $\sqrt{P}D(t)x(t) + \sqrt{2P_J}\cos(2\pi f_J t + \theta_J)$. P is the baseband GPS power and P_J is the power in the interference signal. D is the data and x represents the C/A code.² The correlation of the spreading code with signal plus interference gives:

$$S + J = x(t) * (\sqrt{P}D(t)x(t) + \sqrt{2P_J}\cos(2\pi f_J t + \theta_J)) \quad (1)$$

When the spreading code is aligned, we find that

$$S = \frac{1}{T} \int_0^T \sqrt{P}D(t)x(t)x(t)dt \quad (2)$$

$$= \sqrt{PD} \quad (3)$$

The treatment of the interference term is far more complex. We find that

$$J = \frac{1}{T} \int_0^T \sqrt{2P_J}\cos(2\pi f_J t + \theta_J)x(t)dt \quad (4)$$

$$= \frac{\sqrt{2P_J}}{2T} \left(\exp(j\theta_J) \int_0^T x(t)\exp(j2\pi f_J t)dt + \exp(-j\theta_J) \int_0^T x(t)\exp(-j2\pi f_J t)dt \right) \quad (5)$$

It can be shown that the processing gain is

$$PG = 10\log_{10}N - 10\log_{10}\left(|\text{sinc}(\pi f_J T_C)|^2\right) - 10\log_{10}\left(|X_{code}(f_J)|^2\right) - 10\log_{10}\left(\sum_{l=-\infty}^{\infty} \left|\text{sinc}\left(\pi T_B\left(f_J - \frac{l}{NT_C}\right)\right)\right|^2\right) \quad (6)$$

In the last formula, it is important to note that the processing gain is reduced by the spectrum of the C/A code X_{code} at the frequency f_J . If the interference falls together with a strong line of the C/A line spectrum, this term can amount to 10dB.

5.2 Effect analysis of RF interference

For the analysis of the effects of RF interference, we will follow the forthcoming line of thought [6]. Starting from the unjammed SNR, we compute the effective SNR that can be tolerated as a result of jamming. Comparing the unjammed SNR and the effective SNR, the allowable jammer-to-signal ratio can be calculated. Subsequently the range to this interference source can be computed.

The unjammed C/N_0 ratio at baseband is given by:

$$C/N_0 = S_r + G_a - 10\log(kT_0) - N_f - L(\text{dB} - \text{Hz}) \quad (7)$$

with: S_r - the received GPS signal power (dBW)

G_a - the antenna gain toward the satellite (dBic)

²The carrier signal has been ignored during analysis. Baseband signals are considered.

<i>J/S environment</i> (dB)	<i>Signal</i>		
	<i>L1 C/A</i>	<i>L1 P(Y)</i>	<i>L2 P(Y)</i>
Wideband	34.7	44.2	43.4
Spread Sprectum	33.4	43.0	42.1
Narrowband	31.7	41.2	40.4

Table 4: Jammer-to-signal ratios for 28.0 dB-Hz tracking threshold

$10\log(kT_0)$ - thermal noise density (dBW-Hz); k Boltzmann's constant

N_f - receiver noise figure including antenna and cable losses (dB)

L - implementation losses and A/D converter loss (dB)

The minimum received signal power is defined by [21] and is equal to -159.6, -162.6 and -165.2 dBW for L1 C/A, L1 P(Y) and L2 P(Y) codes respectively. Assuming the minimum power level for a GPS C/A signal, an antenna unity gain toward the space vehicle, a receiver noise figure $N_f = 4\text{dB}$ and implementation loss and A/D converter loss $L = 2\text{dB}$, we finally obtain an unjammed carrier to noise power ratio $C/N_0 = 38.4\text{dB-Hz}$. The second step is to compute the level to which the unjammed C/N_0 is reduced by RF interference. This metric is called the equivalent carrier-to-noise power density ratio and is related with the jammer-to-signal power ratio J/S as follows:

$$J/S = 10\log\left[QR_c\left(\frac{1}{10^{[C/N_0]_{eq}/10}} - \frac{1}{10^{(C/N_0)/10}}\right)\right](\text{dB}) \quad (8)$$

where R_c is the GPS PRN code chipping rate and Q is the spread spectrum processing gain adjustment factor, depending on the type of interference (narrowband, wideband spread spectrum or wideband gaussian noise). The rule-of-thumb tracking threshold is considered is 28 dB-Hz. Substituting this value in formula 8, we obtain $J/S = 34.7\text{dB}$. An overview of different possible scenarios is given in Table 4. The allowable jammer-to-signal ratio seems a weak constraint, but taking into account the actual signal power levels, it becomes clear that the jammer power necessary to disturb the proper functioning of the receiver is as well very small. With $J_r = 10\log j_r$ we can rearrange the equation $J/S = J_r - S_r$ (dB) as follows:

$$j_r = 10^{(J/S+S_r)/10} \quad (9)$$

Using the minimum received signal power level for L1 C/A code and the most optimistic jamming performance for the C/A code, according to formula (9) the incident jammer power is $j_r = 3.1623 \times 10^{-12}\text{W}$. Finally we will compute the operating range of the GPS receiver from the source of RF interference, given the effective radiated power (ERP) of the interference source. The formula of the link budget of the transmitted jammer power is given by:

$$ERP_j = J_r - G_j + L_p + L_f(\text{dBW}) \quad (10)$$

with: ERP_i - the effective radiated power of the transmitter $J_t + G_t$

J_r - the incident jammer power (dBW)

G_t - the GPS receiver antenna gain toward jammer (dBic)

L_p - the free-space propagation loss $20\log\left(\frac{4\pi d}{\lambda_j}\right)$ (dB)

d - the range to the jammer

λ_j - wavelength of the jammer frequency

Solving formula 10 for the range d , we get for a 2W transmitted signal $d = 26.6\text{km}$. Note however that in the former calculations we supposed a clear line of sight between the jammer source and the GPS receiver. In reality the RF interference signals will be attenuated by the curvature of the earth, foliage, buildings and so forth.

5.3 Effects of interference on GPS C/A receiver

Since the C/A code has a 1 ms period, the spectrum consists of line components spaced by 1kHz with approximately a $(\sin x/x)^2$ power spectral envelope. Consider now a narrow-band interfering signal $I(t) = K\cos(\omega t + \theta)$ and suppose that its frequency matches one of the C/A line components. The worst case interference signal would only be attenuated by 18.3 dB. However, even if the frequency of an interference source would fall within the tracking band, only one satellite will be affected since all satellites have different Doppler profiles. A proper setting of the AGC or use of spatial selectivity techniques can further alleviate this risk.

We consider now effects of interference on the correlator output [5]. The received signal is the sum of signal, gaussian noise and interference. The goal is to examine the spectrum of the interference at the correlator output in the in-phase channel. As a first example we consider a CW carrier interference. The GPS C/A reference signal is periodic and can be represented as follows

$$p(t) = \sum_{i=0}^{\infty} a_i \cos(i\Delta\omega t) + b_i \sin(i\Delta\omega t) \quad (11)$$

where $p = \pm 1$, has unit power and $\Delta\omega = 2\pi \times 1\text{kHz}$. The interference in the in-phase channel equals $Kp(t)\cos(n\Delta\omega t + \theta)$. The product $p(t)I(t)$ has a component $K(a_n \cos\theta + b_n \sin\theta)$ at the origin which is co-channel interference on the signal. The terms $2\Delta\omega t$ and higher in this product have been removed by low pass filtering. The power of the interference can be written as

$$K^2 \left(\frac{a_n^2 + b_n^2}{2} \right) = K^2 \left(\frac{c_n^2}{2} \right) \quad (12)$$

with $(a_n^2 + b_n^2) = c_n^2$ the power in the C/A line component at $n\Delta\omega$ and $\sum c_n = 1$. Hence, if θ is averaged over time, only half of the interfering energy can be found in the in-phase channel. The other half of interfering energy is then in the quadrature channel. It is however clear that if the interference phase is fixed and in phase with the reference carrier, then all interfering energy appears in the in-phase channel. In general the interference power in the correlator output is the convolution of the interference spectrum with each of the C/A reference signal line components. If the interfering signal matches

the offset and Doppler shift of one of the C/A line components, then the convolution translates the interference to baseband at $f = 0$ while the bandwidth of the original interference is maintained. Suppose that the interfering signal has a bandwidth of 10 Hz. At the exact frequency of a line component, almost all interference can pass through the narrow band filters of the code or carrier tracking loops. If on the other hand there is an offset between interference and the line component, then also the interference power will be offset in frequency from $f = 0$ and no interference will pass the tracking filters. Recall that the spectrum of the C/A code consists of line components spaced at 1 kHz with a power spectral envelope of $(\sin x/x)^2$. The power in a 1 kHz interval is collected in a line component with power $P_s/f_c \times 1\text{kHz}$. In the hypothesis of a 10 Hz interfering signal, the chance for the interference to match the frequency of a given satellite is 10 Hz/1 kHz or 1%. Unless more than one satellite has the same Doppler shift and the same line components, only one satellite out of those in view can be affected. As the interference bandwidth widens, only a portion of the interference will pass the narrowband coherent tracking filters. Let the interference bandwidth now be 1 kHz, which is exactly the line component spacing. The interference is now continuously spread over the entire channel. Only a fraction though of the interference power passes the tracking filter determined by the ratio $B_n/10^3\text{Hz}$, with B_n is the closed-loop noise bandwidth of the DLL. In this case all satellites are affected to varying degrees depending on the line component amplitude. Finally consider an interfering signal of 10kHz or more. In this scenario each line component is spread over the adjacent 10 line components. The interference power is spread over the entire C/A code spectrum and the effective interference noise density is approximately $P_I/10^6$.

As a reference, the thermal noise power is around -142 dBW. The interference levels required to disrupt the carrier and code tracking loops are well above that level. The only exception is narrowband interference that mostly affects only one satellite and where the interference frequency should be within 10 Hz of a strong C/A spectral line. Higher levels of interference are rather easy to discern from noise. The receiver can be designed to adapt to the interference and mitigate its effects. Recall that an adaptive quantizer can provide a considerable improvement in the presence of constant envelope interference, i.e. the interference above the noise level can be attenuated by 10 dB or more. Interference attenuation above 20 dB can be achieved using adaptive null steering antennas and adaptive frequency notch filters.

5.4 Signal degradation modeling

Another approach for signal degradation modeling has been proposed by the University of Calgary in [22]. Travelling from satellite to receiver, the GPS signal suffers from different forms of attenuation. Aside from the free space path loss, the signals encounter in the atmosphere ionospheric and tropospheric scintillation, as well as absorption. Close to the receiver, surrounding objects can cause masking and blocking. Finally, interference

(jamming) and environmental noise can have a substantial impact. The use of GPS is no longer restricted to open areas. Integration of a GPS receiver in cell phones (for instance for E911) requires the ability to acquire and track weak signals in urban canyons or even indoor. Those signals can be seriously degraded by blocking or multipath. The signal channel in the vicinity of the receiver antenna will be discussed, with emphasis on the fading and masking effects by surrounding objects.

The first Fresnel zone is defined as the the volume enclosed by an ellipsoid with two antennas at its foci such that the distance from a point on the ellipsoid to its foci is one wavelength longer than the direct distance between the antennas. GPS signals can now be divided in three categories. (i) a clear *line-of-sight signal* gets to the receiver without any object in the way of propagation. Attenuation originates from free space loss and absorption. (ii) For a *shadowed signal* the propagation takes place in the first Fresnel zone with attenuation (e.g. foliage). (iii) For a *blocked signal* the propagation in the first Fresnel zone is blocked. By diffraction and reflection the signal can be received.

The Urban Three State Fade Model (UTSFM) is used to describe the GPS signal fading distribution. The three types of signals explained before have a specific fading distribution expressed by different probability density functions (pdf). The composite amplitude probability density function is a weighted combination of Ricean, Rayleigh and Loo pdf's and is function of the elevation angle. It is demonstrated that the UTSFM is a useful method to describe and distinguish the fading distribution in urban, suburban and open area.

6 Interference detection

In Section 5 a survey of the possible impact of RFI on GNSS receivers is presented. This section explains several methods to detect the presence of RF interference. Different metrics are well known to evaluate the impact of RFI on GNSS receivers. A non-exhaustive list of those methods will be presented here.

A first approach to assess the interference in a GNSS receiver is by monitoring the behavior of the Automatic Gain Control (AGC) [23]. Receivers consist of an analog front-end and a digital part, responsible for code and carrier tracking. Sampling and quantization of the analog signal is performed resulting in the digital signal. The AGC can be considered as an adaptive gain amplifier designed to minimize the quantization losses. Implementation losses depend on the sampling rate, the quantization process and the precorrelation bandwidth. The degradation is function of the ratio k of the maximum quantization threshold to the input noise standard deviation σ . The AGC ensures that an optimal ratio is used, minimizing the quantization losses. One can notice that there is no dependence on the signal itself as it is negligible - below the noise floor - at this stage in the receiver. Since the AGC is driven by the ambient noise rather than the signal, the AGC can be a valuable tool assessing the noise environment.

When the received signal is digitized, a variety of methods - in different parts of the processing chain - is available to detect the presence of interference. Spectral analysis in the concerned GNSS frequency band is probably the most direct method to analyze the spectral components of the received signal. Further, interference effects can be monitored by the acquisition and code tracking performance. During the acquisition phase, different acquisition metrics have been proposed [24]. A first metric is defined as:

$$\alpha_{max} = 10 \log_{10} \left(\frac{R_p}{R_{2p}} \right)^2 \quad (13)$$

where R_p is the highest correlation peak and R_{2p} is the second highest correlation peak. A second metric is defined as follows:

$$\alpha_{mean} = 10 \log_{10} \left(\frac{R_p}{M_c} \right)^2 \quad (14)$$

The second metric represents the ratio between the highest correlation peak R_p and the mean value of the correlation floor M_c .

Another valuable technique for the characterization of interference is the estimation of the carrier to noise ratio. In the receiver, while the code is despread by multiplication with a local replica, the interference is spread over the bandwidth of the code. The spreading of the interference is identical to the spreading of the data in the transmitter. After multiplication with the local replica, a low pass filter is used. Only the spread interference lying within the bandwidth of this filter remains. The interference that passes the filter also depends on the amplitude of the nearest spectral line in the code line spectrum. The carrier to noise ratio at the output of the correlator can be used to estimate the frequency of the RFI. In [25] a technique is proposed to detect and

characterize continuous wave RF interference. The comparison between a mathematical expression of C/N_0 and an estimation of the actual carrier power to noise density ratio is used to determine the frequency of the interference. Yet, the power of the interference is estimated by the value of the AGC. The advantage of the proposed technique lies in the fact this post-processing technique does not require any additional hardware.

The use of signal to noise ratio or carrier to noise ratio is a widespread metric in wireless communications to evaluate the signal quality. In [26] an overview is given of the different post-correlation techniques to determine the carrier power to noise density C/N_0 . The interference can be originating from broadcast television, mobile satellite services, ultra wideband communications or in the case of intentional interference also from jamming or spoofing. Weak signal environments include urban area or indoor. Different methods have been assessed, analytically and by simulation. The narrow to wide power ratio method was shown to perform better in terms of noise in low signal to noise environments. In this method the I and Q samples are accumulated over an interval τ and further divided over M intervals. The narrow band power P_N and wide band power P_W are defined as follows:

$$P_N = \left(\sum_i^M I_{Pi} \right)^2 + \left(\sum_i^M Q_{Pi} \right)^2; P_W = \left(\sum_i^M (I_{Pi}^2 + Q_{Pi}^2) \right) \quad (15)$$

The narrow to wide power ratio $P_{N/W}$ is defined as the ratio of the two power measurements. In order to reduce the noise, the measurement is averaged over n iterations.

$$\bar{P}_{N/W} = \frac{1}{n} \sum_{r=1}^n \frac{P_{N,r}}{P_{W,r}} \quad (16)$$

Taking the expectation $E(\bar{P}_{N/W})$ and rearranging, gives

$$\tilde{c}/\tilde{n}_0 \approx \frac{M \bar{P}_{N/W} - 1}{\tau M - \bar{P}_{N/W}} \quad (17)$$

However, to obtain useful c/n_0 measurements in weak signal and high interference environments, long averaging times are necessary.

Yet another method is based on the definition of a new family of curves, the so called interference error envelope (IEE) [27]. The concept of the interference error envelope is to express the distortion of the discriminator function as a function of several parameters of the interfering signal, i.e. the frequency shift and the continuous wave phase. The IEE is then obtained considering the maximum and minimum values of the ranging errors over the entire range of phases. The obtained curves are a useful tool to assess the worst case errors for each continuous wave frequency. In particular the tool is very useful as a performance comparison tool for different modulations and different discrimination functions.

Finally, also the error vector magnitude (EVM) can be used as a detection metric for RF interference [28]. The EVM is widely used in wireless communications to assess

the channel quality. The EVM describes the quality of the modulation, quantifying the distance between the constellation points and their corresponding ideal locations. A maximum error vector magnitude threshold can be determined, corresponding with a minimum signal quality level, assuring bit error free reception.

7 Interference mitigation

7.1 Mitigation strategies

In Section 6 different methodologies to detect RF interference are introduced. The current section deals with interference mitigation. Mitigation strategies can be divided along the interference class (intentional or unintentional). Methods likely to be effective against *unintentional interference*, can possibly be of limited value with regard to specific intentional interference. Mitigation strategies that are used for unintentional interference vary from spectrum management and legal action, over detection and location algorithms, GPS modernization to anti-jam receiver architectures. By GPS modernization we understand a higher GPS signal power, C/A code on L2 and a more robust civil code on L5. It is very unlikely that an unintentional interference would jam the three employed frequencies simultaneously. Jam resistant receiver architectures comprise pre- and post-correlation methods. Precorrelation methods include spatial, temporal and spectral processing. Beam forming and null steering belong to the field of adaptive spatial processing and are the only effective means against broadband interference. These techniques require however multi-element antenna arrays. Polarization discrimination requires only a single antenna aperture and belongs to the class of the spatial filtering techniques. Postcorrelation methods on the other hand comprise enhanced signal processing techniques and the use of additional sensing. The mitigation of *intentional interference* for jamming include adaptive antenna arrays (spatial filtering), polarization discrimination and spatial-temporal filtering. For spoofing different approaches have been studied of which the angle-of-arrival discrimination is probably the most efficient. Matching the angle-of-arrival of the satellite signal is almost impossible for the spoofer. This technique requires however a multi-element antenna.

7.2 Robust receiver design for interference mitigation

Figure 1 illustrates a GPS receiver with *spatial and spectral signal processing* for interference suppression. Spatial selectivity can be achieved for a single antenna with a antenna pattern with signal attenuation for low elevation angles. That is, when the elevation drops below 5 deg, effects as multipath, obstruction and ionospheric/tropospheric delay can become the dominant error sources. The interfering signals from ground-based jammers can be eliminated as well. If more antennas are available, satellite receiver channels can be switched between antennas with higher gain in different directions and elevation angles. Furthermore, a set of antennas can also be used as phased arrays with additional gain in the directions of the satellites in view. Alternatively, adaptive nulling antennas can be designed contributing to spatial interference suppression. Satellite and interfering signals have generally a large angular separation. Based on this assumption a vast number of LMS and signal-to-noise enhancing adaptive antenna array techniques have been developed, enhancing the gain toward the signals of interest and attenuating

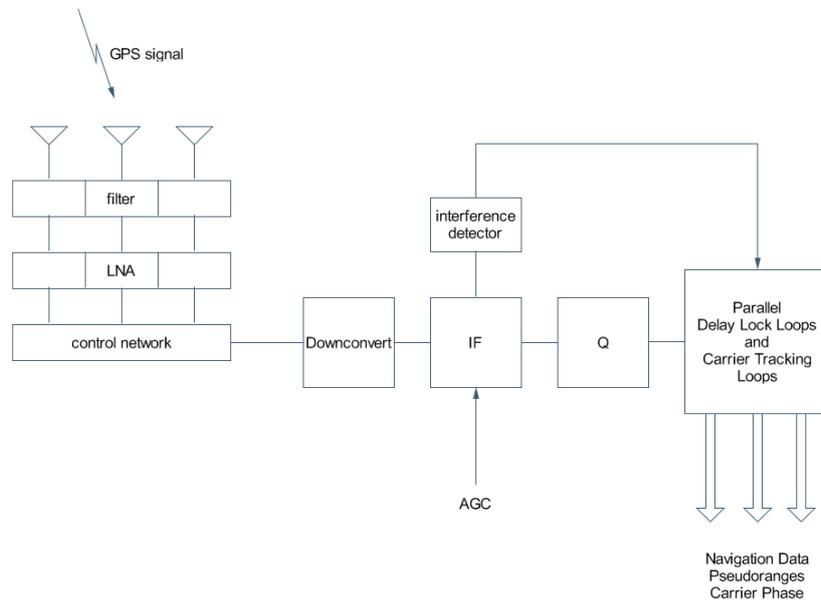


Figure 1: GPS receiver

interference. Further, spectral differentiation can be attained by several stages of RF and IF filtering. An overload protection is often implemented in the receiver front end to prevent saturation in the presence of high power pulsed interference. RF filtering is also applied to anticipate out-of-band interference. The RF/IF filter may be set with a larger bandwidth yielding a higher accuracy, alternatively a small bandwidth could be chosen for the higher selectivity against out-of-band interference. The automatic gain control (AGC) is an important device that selects the signal power levels such as to minimize the performance degradation of the quantization process. The principle of operation is based on a jamming-to-noise power measurement J/N . If the AGC control voltage level is different from the thermal noise root mean square, then some other signal is controlling the AGC. Since the signal of interest is well below the thermal noise floor, a J/N measurement above the noise level indicates the presence of interference. A precise measurement of the AGC control voltage is a good estimate of the J/N ratio which is in turn a good estimate of the jamming-to-signal power ratio. Often signal blanking is included in the AGC.

7.3 Spectral and spatial signal processing

Different measures to cope with interference can be distinguished [5]; some of them already have been described:

1. Front-End filtering techniques which can be subdivided into two main groups:

- *Bandpass RF filtering* to prevent out-of-band interference. The front-end pre-filter should have sharp cutoff with deep stopband characteristics capable of suppressing high out-of-band power. Placing a passive filter between the antenna and the preamp results however in a certain performance degradation. Every dB of insertion loss adds one dB to the receiver noise figure, which in turn reduces the tracking threshold with one dB. A cavity filter can be used. This type of filter has very low insertion loss and outstanding stopband characteristics. In addition to the prefilter, additional filtering is required before and after each local oscillator in the mixing stages of the downconverter. Very narrow filter bandwidths can be synthesized and improve the receiver performance against out-of-band interference.
 - *Pulse blanking* to reduce the impact of high level pulsed interference and to prevent LNA overload. A typical example of pulsed interference is a radar transmitter. A good design practice is to implement a limiter just ahead of the preamp, clipping high-power signals. The clipping action has a low duty cycle and mostly does not cause a GPS receiver to fail. The loss in C/N is directly proportional to the duty cycle of the pulse jammer.
2. Adequate number of quantizing levels and proper setting of the AGC to ensure full processing gain
 3. Careful design of code and carrier tracking loops
 4. External navigation aiding enhancements can be implemented in the receiver, for instance inertial measurement units (IMUs), Doppler radar etc. They provide an overdetermined solution of the positioning problem and thus, they add robustness to the receiver under RF interference conditions. Yet, external enhancements are large and/or expensive. Hence, they are usually not integrated in commercial receivers.

Nevertheless, it is obvious that sufficiently high levels of interference will overload any type of radionavigation system, that is, also GPS. We note that under most circumstances the interference levels that disrupt the proper functioning of a receiver are well above the thermal noise level, either in peak power spectral density or total power. This means that a total power measurement or a spectral density measurement are very simple but effective means to detect the presence of interference. Once detected, different measures can be taken. The Kalman filter can be adjusted to give lower weight to the measurements. Adaptive antenna nulling and adaptive notch filtering are other techniques to alleviate the effects of interference.

It is relatively easy to distinguish narrow-band interference above the thermal noise level. Once the interference is estimated, for instance by a DFT, this estimate can be fed to an adaptive frequency notch filter algorithm. This is illustrated in Figure 2. In this approach, the interference estimation is used to adjust the tap coefficients of the

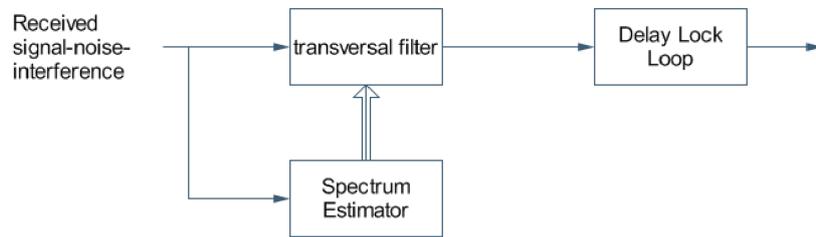


Figure 2: Interference cancellation using nonparametric spectral estimation

transversal filter. The tap coefficients are denoted by $h(k)$, $k = 0, 1, \dots, K - 1$ and

$$H(k) = \sum_n^{K-1} h(n) e^{-j2\pi nk/K} \quad (18)$$

If power spectral measurements $P(kR_s/K)$ are made with R_s the sampling rate, in order to whiten the output spectrum we get then

$$H(k) = \frac{1}{\sqrt{P(kR_s/K)}} e^{-j2\pi(K-1)k/2K} \quad (19)$$

Applying this approach, an interference reduction of 15 dB can be achieved when the interference is originally 20 dB above the background spectrum. An alternative solution is illustrated in Figure 3. The notch filter is tuned for example by DFT measurement so

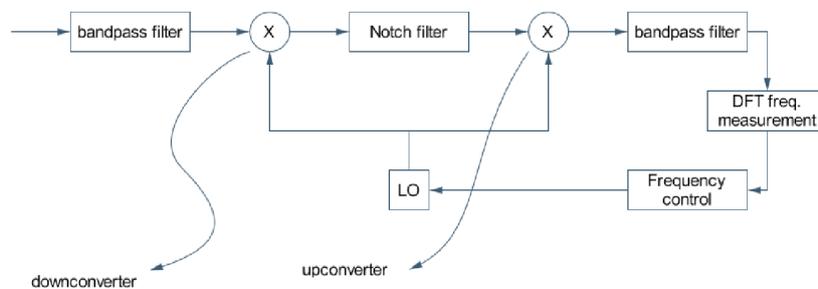


Figure 3: tunable frequency notch filter

as to minimize the total power fed to the correlator if interference is detected.

Another approach for interference mitigation is located much earlier in the processing chain. *Adaptive antennas* or *spatial signal processing* can be used for point source interference. For a satellite navigation system there are in general M separate signal sources. An adaptive antenna array consists of N antenna elements and deals with M satellite signals. A general configuration is shown in Figure 4. In this setup the antenna array is followed by M adaptive weight matrices and controllers, each of them tuned and optimized for a single satellite. There exists a great variety of possible antenna arrays. First of all, we can form a series of M single-beam antennas, each of them pointing to

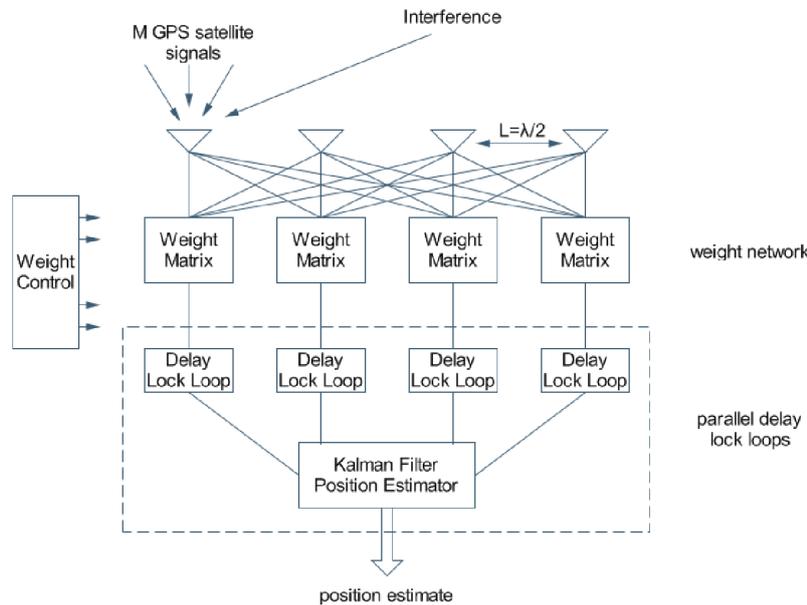


Figure 4: General configuration of an adaptive antenna array

a navigation satellite. Alternatively a single multiple-beam antenna can be formed with M peaks in the antenna pattern. The approach of programmable multi-beam antenna arrays requires the knowledge of the satellite orbits. A multiple-beam adaptive array of N elements can form $N-1$ separate beams and each beam can null $N-2$ separate interfering sources. The resolution capability of the array determines the minimum angular separation between a beam maximum and a null. The resolution capability is determined by the array aperture size. A first implementation of an adaptive null steering antenna is the least-mean-square (LMS) error adaptive array. This algorithm minimizes the mean-square error between the output of the weight matrix $s(t)$ and a reference signal $r(t)$. This reference signal is the C/A code which can easily be generated. Both signals should be aligned in time and frequency by means of the delay lock loop and carrier phase lock loop. Nevertheless, the performance of this technique is limited by the poor SNR of the received signal, unless sufficient antenna gain is provided by the antenna array. A second type of adaptive antenna arrays is the Applebaum array. In this approach, the weighting matrix attempts to maximize the ratio of the output signal power with respect to the output power of noise and interference. This methodology requires the knowledge of the angle of arrival so as to generate the steering vector. With the Applebaum array the beam is indeed steered in the direction of the signal of interest, while the interfering signals are attempted to be nulled. Finally, we consider a variant of the Applebaum array, called the power inversion array. For this type of adaptive antenna array, nor an estimate of the signal waveform nor the angle of arrival are required. This algorithm attempts to

minimize the total output power, under the constraint not to set all weights equal to zero.

7.4 Comparison of different interference mitigation techniques

In what follows, different mitigation techniques are introduced [29]. The interference consists of sinusoidal signals and pulsed waves. In order to assess the performance of the filtering techniques, we define two metrics: processing gain and correlation gain. To define the filtering technique a simplified model of the signal and the receiver is used (Figure 5). The input signal has the form $r(t) = s(t) + g(t) = AP_r(t)\exp(i\theta_s(t)) + g(t)$, with A the signal amplitude, $P_r(t)$ the C/A code and $g(t)$ the complex noise. The correlation

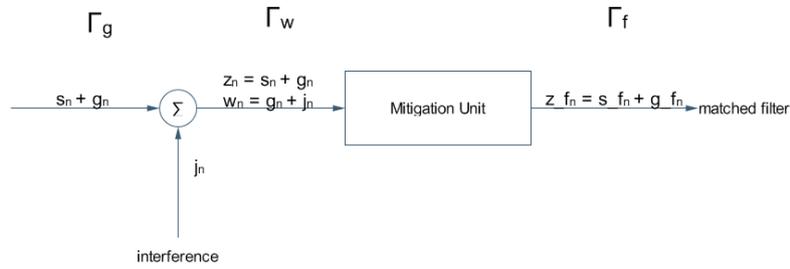


Figure 5: signal model

gain is now defined as

$$G_{\Gamma} = \frac{\Gamma_f}{\Gamma_g} \quad (20)$$

with Γ_g is the SNR in absence of the interfering signal. Γ_f is the SNR at the output of the interference mitigation unit. The processing gain is defined as

$$G_t = \frac{\Gamma_f}{\Gamma_w} \quad (21)$$

where Γ_w is the SNR in the presence of the non-filtered interference. The goal is to design a filter that cancels the interference out while leaving the GPS signal intact. This filter has the following properties

$$\begin{cases} G_{\Gamma} = 1 \\ G_t \approx \gamma_{JG} = \frac{J}{G} \\ J: \text{interference power} \quad J \gg G \end{cases} \quad (22)$$

The first technique applied consists of a pre-whitening linear filter in front of the conventional receiver. However, the presence of wideband FM or pulsed jammers cause a considerable loss of correlation. Hence, an adaptive notch filter architecture is proposed. This architecture consists of an estimation unit, a mitigation unit and finally a zero filtering unit. The estimation cell is designed to determine the characteristics of

the interfering signal. The number of jammers as well as the amplitude and frequency slope of the interfering signal can be specified. The estimation unit is subsequently used to control the mitigation unit. In this part, the quantification noise is reduced and the processing gain can be adjusted. The third unit, the zero filtering unit, serves to eliminate the components at the beating frequencies, in presence of multiple jammers. This filtering technique has a good performance in the presence of multiple slowly varying jammers. A processing gain close to the ideal value γ_{jg} can be obtained; the correlation gain on the other hand is function of the number of jammers, on the frequency and the frequency slope of the jammers. The filter performance is measured by the correlation gain.

The second group of techniques is based on detection theory. For weak signals buried in non-gaussian noise, the locally optimum receiver is determined. Compared to a conventional receiver, this type applies a non-linear function to the amplitude of the complex input signal. The non-linear operator is deduced from the PDF of the noise amplitude. This method is particularly suitable for pulsed jammers and fast varying swept jammers. Nevertheless, in the presence of multiple jammers with gaussian-like statistics the technique of amplitude processing in the time domain becomes inefficient. In this case, spectral amplitude processing can improve the correlation gain. However, this kind of filter is highly complex and becomes ineffective in the presence of strong pulsed interference.

8 Relevant interference scenarios

In Section 4 an overview has been given of the possible sources of intentional and unintentional interference. In this chapter, we select and detail two scenarios of unintentional interference that are of great interest.

8.1 UWB interference on GPS

UWB technology can be defined as a wireless transmission scheme with a large fractional bandwidth:

$$B_f = \frac{B}{f_c} = \frac{f_h - f_l}{(f_h + f_l)/2} \geq 0.25 \quad (23)$$

where f_h and f_l are the high and low cut-off frequency of the signal, respectively.

The Federal Communications Commission (FCC) has a reserved approach in the regulatory process of UWB because of the uncertainty surrounding UWB interference on other technologies such as GPS. Because UWB employs a frequency range already occupied by wireless telephone carriers etc., the National Telecommunications and Information Administration (NTIA) searched for a compromise that ensured that UWB transmissions would not interfere with existing technologies as cellular telephones, security systems and GPS. Recall that GPS will become the cornerstone for air navigation for all phases of flight (en-route, precision and non-precision approach) and that it is the preferred technology for different safety-of-life applications. In the literature voices can be heard minimizing the effect of UWB interference on GPS, as well those that indicate the potential of UWB signals to interfere severely. In what follows an overview is given.

8.1.1 NTIA report on UWB/GPS compatibility

In February 2001 the NTIA published a report on the assessment of compatibility between ultrawideband (UWB) systems and GPS receivers [30]. The primary objective of the study was to define maximum allowable UWB equivalent isotropically radiated power (EIRP) levels that don't affect nominal GPS operation. Three types of GPS receivers were selected for the testing: C/A code tracking receivers (which represent the bulk of the civil GPS receivers), semi-codeless receivers (for low-dynamic, high-precision applications) and C/A code-tracking receivers with multiple, narrowly-spaced correlators (for enhanced accuracy and mitigating multipath). The interfering signals considered can be categorized by their pulse repetition time, the modulation type (constant PRF, on-off keying, dither) and the states of gating. Two performance criteria were handled: break-lock and reacquisition. Break-lock refers to the disruption of signal lock between the GPS receiver and the satellite. The reacquisition threshold is defined as the UWB power level that results in an abrupt increase in reacquisition time. Closed system (conducted) and radiated measurements have been performed for both a single UWB transmitter as well as multiple (aggregate) UWB transmitters. The measurements results can be summarized as follows:

- ☑ *Pulse Repetition Frequency*: increasing the PRF up to 5 MHz and 20 MHz, CW-like interference susceptibility to the C/A code receiver was observed.
- ☑ *Dither* is an intentionally applied form of noise. Dithering of the UWB pulses in the time domain are effective in spreading the spectral lines in the frequency domain, leading to a signal that is more noise-like. The GPS C/A code receiver is approximately 10 dB less sensitive to the noise-like UWB signals as compared to those CW-like UWB signals.
- ☑ *Aggregate UWB transmitters*: the advantage of dithering is lost as few as three UWB transmitters are present.
- ☑ *Maximum allowable EIRP level*: has been determined for all UWB signal permutations.

8.1.2 Potential interference to GPS from UWB transmitters

Since GPS is a weak signal with receiver power levels of about -130 dBm, there is an obvious concern of potential interference with other technologies. In what follows the operation of unlicensed UWB devices is considered ([31], [32] and [33]). Previous field trials have shown the potential interference of UWB on GPS. Therefore the Department of Transportation (DOT) has funded a study at Stanford University between the two technologies. For aviation purposes the primary metric to evaluate interference is accuracy. Yet, for land users the criterion is acquisition time, as emergency vehicles may need to quickly obtain the GPS signal after signal loss due to obstructions (urban canyon, tunnels, etc.).

The test philosophy that has been handled is a RFI-equivalence concept that relates the UWB interference impact on GPS to that of broadband white noise. The UWB interference impact is determined equivalent to a known level of broadband white noise, where the GPS receiver just meets its performance criterion. This has been done for different UWB waveforms, for different types of GPS receivers and for different performance criteria. UWB transmissions cover various combinations of pulse repetition frequency (PRF), burst duty cycle, random on-off keying (OOK) and Pulse Position Modulation (PPM). GPS receivers can be divided into aviation receivers, low-cost OEM receivers and a high-grade general purpose receiver. Finally, the test approaches cover accuracy testing, loss-of-lock and signal acquisition performance.

The results of the test campaign can be summarized as follows:

- ☑ Pulse-like interference (i.e. low pulse repetition frequencies) can yield noise equivalence factors that are up to 33 dB less damaging than broadband white noise. CW-like interference can be 10 dB more damaging than broadband noise. In general increasing PRFs lead to higher impact on receiver performance. It was noticed that GPS is extremely sensitive to the PRF of 19.94 MHz. The receiver lost lock with a minimal addition of UWB power. In fact, looking at the spectrum of the UWB and

the GPS signal, it is clear that a large spectral spike of the UWB signal coincides with the peak of the GPS L1 main lobe. When no distinct spectral lines are visible, UWB signals even with high PRFs appear as additional broadband white noise in the resulting spectrum.

- ☑ Loss-of-lock testing has been conducted for the OEM receivers. The same trend is perceived. UWB signals that generate spectral lines are the most problematic for GPS receivers, regardless the specific type of receiver.
- ☑ The same trend was discerned for acquisition testing.
- ☑ Methods reducing the appearance of spectral lines have been investigated. Different types of Pulse Position Modulation have been considered. The more random the appearance of the pulses, the greater the reduction of the height of the spectral lines. However, even with modulation and a low PRF, distinct spectral lines can still be found falling within the GPS spectrum. Significant performance variations in the GPS receiver are observed corresponding with slight changes in the PRF. The specific impact depends on the clock drift, the PRN code and the UWB PRF.
- ☑ There is a strong correlation between the most and least damaging cases for both accuracy and acquisition testing. This gives evidence that the performance trends are not isolated to one mode of receiver operation. Rather, the presence of UWB signals will impact all phases of GPS signal processing.

The list of test scenarios that have been tested is in no means exhaustive. Possibly, more damaging cases can be found. More study is necessary to fully address the UWB interference issue.

8.1.3 Theoretical approach for assessing UWB interference to GPS receivers

GPS receivers are highly sensitive to interference since the receiver power levels are extremely low. The study performed by the GPS Joint Programme Office discusses the FCC limits (2002) that are imposed on a broad range of UWB devices [34]. The GPS JPO does not recommend a relaxation of those UWB emission levels, permitted in the GPS frequency band. The main technical concerns with UWB devices are (i) the aggregate effect to the noise floor of different UWB devices in one area and (ii) the effect of one UWB transmitter in close proximity of a GPS receiver, which will be discussed in the following. Formerly, there have been two popular approaches to assessing UWB interference: the testing of UWB waveforms on GPS receivers and UWB interference link budgets. Concerning the many testing campaigns of UWB waveforms, the general conclusion was that UWB signals degrade the GPS receiver performance. Yet, it is clear that no consistent testing approach has been applied. Since different wave forms, power levels, receivers and performance criteria were handled, no solid conclusions could be drawn. Still, for the interference link budget approach, critic was ubiquitous. The starting point

of this approach is the maximum interference environment a GPS receiver can tolerate and works backwards to determine the maximum EIRP an interferer can transmit. Margin upon margin is stacked with very little justification.

The GPS JPO began with addressing the interference problem analytically. One UWB receiver was considered as a best-case scenario. If the effect of one UWB device could be shown to degrade GPS receiver performance, then it is highly likely that the aggregate effect of different UWB devices would degrade the performance even more.

For *noise-like interference* we define the effective isotropic radiated power density as $EIRPD_{UWB}$ in units of dBm/MHz. Noise-like interference causes the noise floor to increase. Note that an increase of the noise floor of only 1 dB degrades GPS receiver performance. In order to quantify the raise of the noise floor, the interferers EIRPD and its distance should be known. In this study a distance of 6 feet is applied. This could correspond with an office or a crowded urban setting. The UWB impact on the GPS receiver noise floor can now be calculated as follows. The received interference density I_O in dBm/MHz is given by

$$I_O = EIRP_{UWB} - L_P \quad (24)$$

where L_P is the path loss in dB and given by

$$L_P = 20\log(f) + 20\log(D) - 27.55 \quad (25)$$

where f is frequency in MHz and D is separation distance in meter. The noise floor increase is now given by

$$NF_{inc} = 10\log(10^{\frac{I_O}{10}} + 10^{\frac{NF_{GPS}}{10}}) - NF_{GPS} \quad (26)$$

As illustrated in Figure 6, the noise floor increases dramatically with increasing EIRP of one single UWB transmitter at a distance of 2 m. The FCC agreed on a 1 dB allowable increase of the noise floor which led to a permitted UWB noise-like emission level of -75.3 dBm/MHz in the GPS frequency band. However, it should be noted that a drastic increase in the noise floor is also observed in case the distance GPS receiver to UWB transmitter is decreasing.

UWB transmissions can also generate *continuous wave or CW-like interference*. This CW-like interference does not raise the noise floor, yet can degrade the receiver performance much more severely than noise-like interference. We define now for CW-like interference the UWB effective isotropic radiated power as $EIRP_{UWB}$ in dBm. Then, the received interference power I_r is given by

$$I_r = EIRP_{UWB} - L_P \quad (27)$$

The power spectrum of the C/A code has a line structure due to its finite length unlike the power spectrum of infinite or very long codes as the P-code. The latter has a continuous $\frac{\sin x}{x}$ power spectrum. The processing gain of the C/A code tend to infinity for a interferer that is far from a spectral line whereas it will be heavily reduced in presence of a CW-like

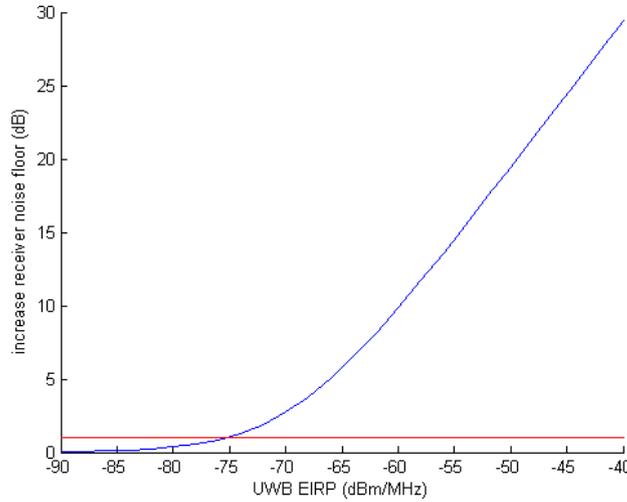


Figure 6: GPS receiver noise floor increase vs. UWB EIRP

interferer that lies nearby a spectral line. Besides, the processing gain also depends on which spectral line coincides with the interferer. The density of the CW signal that gets through the correlator depends on the processed CW power and an effective processing gain PG_{eff} , depending on the magnitude of the spectral line. The interference density for a single line is given by

$$I = I_r - 10\log(PG_{eff}) \quad (28)$$

Moreover, if a large number of UWB lines coincides with strong C/A code spectral lines, the processing gain will be further reduced. For multiple CW interferers or a single interference source containing multiple lines, we can write:

$$I = I_r - 10\log\left(\sum_{i=1}^N PG_{eff}\right) \quad (29)$$

UWB CW emissions are allowed up to -85.3 dBm. This level of interference has about 5% as much power as a -131 dBm GPS signal. Some receivers today are tracking signals at -141 and -151 dBm. The susceptibility to CW interference for those receivers goes up to 25% and equal power respectively. This is a serious problem for indoor GPS applications.

The theoretical analysis presented has sufficiently been validated by test. As the noise floor is increased, the GPS receiver experiences a linear degradation of the SNR up to loss-of-lock. It is critical that the UWB emission levels stay intact to ensure continued GPS operations.

8.1.4 Co-locating UWB and GPS radios

The possibility of co-locating UWB and GPS transceivers is investigated in [35]. Starting from a theoretical analysis, the conclusion can be drawn that a UWB transmitter conform to FCC specifications at a distance of 1.33 meter could degrade the receiver sensitivity with 3 dB. Former theoretical analysis led to ambivalent conclusions. Some concluded that one single emitter at the FCC limit could raise the GPS noise floor with 1 dB [34], whereas others stated that UWB interference on GPS was negligible. Recently, a research team integrated a high-performance GPS receiver in a multimode radio that features GSM, UWB, Bluetooth and WLAN [36]. GSM is identified as the main source of intermodulation distortion, but UWB is left unaddressed. In what follows the interference from a commercially available UWB transmitter is quantitatively assessed. UWB architectures can be subdivided into (i) impulse radio based UWB, implementing time hopping and direct sequence spread spectrum and (ii) multi-band orthogonal frequency division multiplexing (MB-OFDM) UWB. MB-OFDM emerged as the clear industry favorite and is focused on in the remainder.

The incident power for a receiver located in line-of-sight and with negligible multipath can be calculated by:

$$P_i = \frac{EIRP}{4\pi R^2} A_e \quad (30)$$

where: P_i - is the incident power in W

$EIRP$ - is the effective radiated power in W

R - is the separation distance in meters

A_e - is the effective aperture size of the receiving antenna in m^2

If we assume that the UWB devices transmits at the FCC limit of -75.3 dBm in the 1MHz GPS band, we can calculate at what distance the incident power is identical to the thermal noise power. In that case the noise floor raises with 3 dB. The thermal noise is given by:

$$P_N = kTB \quad (31)$$

where: P_N - is the noise power in W

k - is the Boltzmann constant, $1.38E-23$ J/K

T - is the absolute temperature in Kelvin

B - is the bandwidth in Hertz

The noise floor can be quantified as -114 dBm. Quantifying equation 30 yields a distance of 1.33 meter.

Measurements have been performed to validate the theoretical analysis. Because the goal was to investigate the opportunity to co-locate UWB and GPS radios, measurements have been made with a distance of 1 cm. The conclusion of this research was that the UWB device's circuitry produces more interference in the GPS L1 band than the antenna.

8.1.5 SW approach to assess UWB interference on GPS receivers

The testing that has been conducted so far on the UWB interference on GPS receivers, left several questions unanswered. First, since a wide variety of receiver hardware has been used, it is difficult to associate specific factors with the degradation of the GPS receiver performance. Furthermore, the metrics that have been used to assess the performance were restricted to the error in pseudorange and the UWB power levels causing loss-of-lock. Finally, only a limited number of UWB waveforms and power levels have been tested up to present. The main advantage of a software approach is the flexibility in the testing [37]. The framework used for the SW implementation consists of an input component, a processing component and an analysis component (Figure 7). Each

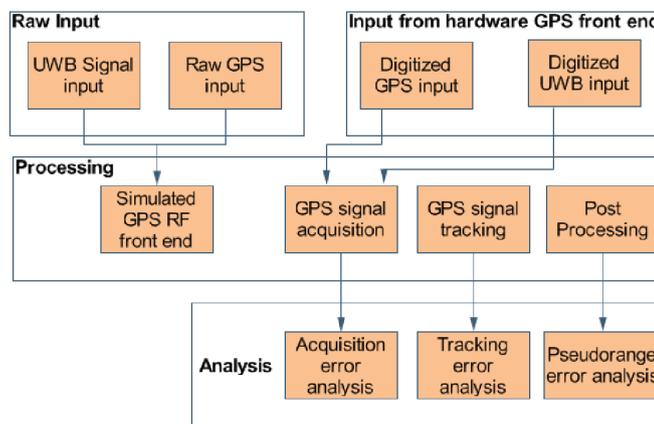


Figure 7: framework for UWB interference on GPS receivers

component in the framework can have different implementations. The advantage of the software approach is that any kind of data source, signal form, processing architecture and analysis method can be tested with a minimum amount of software redesign. Where traditionally acquisition and tracking is performed using hardware, a software GPS receiver implements those functions in software. The RF front end is the only hardware component in the receiver. The software approach can for instance be used to characterize the effect of aggregate UWB devices on GPS performance or to test new GPS signals. Acquisition, tracking and post-processing algorithms can be easily implemented and evaluated.

8.2 TV/FM interference on GPS

A study has been performed on the interference of GPS signals caused by licensed transmitters [38]. The interfering transmitters were selected for having their frequency or harmonics in or near the GPS L1 frequency band. The study focuses on the interference

on civil aviation GPS receivers and encompassed the following steps:

- ☑ *Required accuracy with respect to phase of flight:* Determination of the accuracy during en-route, non-precision approach and precision approach.
- ☑ *Signal quality:* After setting of the accuracy/pseudorange error, the signal quality requirements are determined. For instance, for the precision approach the pseudorange rms error shall not exceed 0.7 m corresponding with a signal to noise plus interference ratio $C/(N_0 + I_0)$ of 30 dBHz.
- ☑ *Out-of-band signals:* The majority of the interfering signals is situated out of the GPS L1 frequency band. The off-frequency interference resistance is mainly determined by the antenna/preamplifier signal rejection characteristics.
- ☑ *Sources of interference:* The transmitter frequency lies between 50 and 2000 MHz. Moreover, the fundamental frequency lies in the range 1315-2000 MHz or the harmonics fall in the band 1565-1585 MHz. The culprits are FM or TV transmitters with an output power exceeding 50 kW. Spurious emission levels are of utmost importance.
- ☑ *Results:* Most of the interference originates from FM and TV broadcast transmissions, when the spurious emissions limits are used. Also VHF ground-based radionavigation transceivers at airports can be a sources of interference. If the spurious emission suppression of the FM and TV broadcast transmitters is better, then the RF interference on GNSS due to these emissions virtually disappears. The low levels of RF interference can be due to the harmonic suppression capability of the antenna. Measurements illustrate that high suppression values are attained, explaining why hardly any incident has been reported.

Strong out-of-band signals In [24] it has been shown that digital/analog TV transmissions represent a potential interference source for GNSS applications. The impact on the overall receiver chain is studied for real out-of-band transmissions. The results discussed are obtained during data collections in the area of Turin. The measurement campaign revealed the presence of interference sources and strong harmonics. When evaluating the impact of interference sources, several aspects should be taken into account such as the interference power, the bandwidth, spectrum shape and time characteristics. The experiments were performed in suburban area where the DVB-T and VHF/UHF broadcasting antennas were in line-of-sight of the GPS receiver antenna. The impact of the interference has been estimated over the entire processing chain. As a first step the power spectral density at the front-end output was evaluated. The spectrum changes significantly over time and spurious peaks appear. Further, there are large variations in the AGC gain, affecting the code tracking accuracy. At the correlators' output, the signal amplitude does not have a constant envelope. The measurements in the Turin area con-

firm that corrupted signals at the front-end output can make the digital signal processing of a GNSS receiver problematic.

Hybrid TV/GPS technology Even though TV signals can possibly interfere with GPS, they can as well be used to enhance the positioning problem in environments with harsh wireless signal conditions. In spite of the global coverage of GPS signals, GPS receivers have not been able to solve the problems related to positioning in urban and indoor areas. At Stanford University there have recently been research on the hybrid positioning systems combining GPS and television signals ([39], [40], [41]). A way to address the problem of the poor availability of GPS signals in harsh urban environments, is the adoption of powerful terrestrial signals. Many of those land-based signals have frame synchronization codes, equivalent to GPS spreading codes. Study has been done on terrestrial positioning systems using WiFi, TV and cellular signals. Among those candidate signals, digital TV signals are the most appropriate due to the high signal power levels, fixed geometries and frequency diversity. TV signals are FDMA (frequency division multiple access) signals spread over a wide range of frequency bands. The frequency diversity is convenient regarding interference issues and also provides additional means against multipath errors, since different channels experience different multipath. Digital as well as analog TV standards contain frame synchronization codes. As a consequence they can be used for positioning purposes. However, since they are not designed for positioning, there are some extra challenges. First there is the lack of transmission time tag and second transmitters demonstrate poor clock stabilities. A performance analysis is done in terms of signal powers, bandwidths and error sources. The first step is the calculation of the signal to noise ratio based on nominal transmission power and distance between receiver and transmitter. Then, a theoretical performance limit is calculated from the estimated SNR by the Cramer-Rao bound (CRLB).

$$\sigma_{\rho} \geq \sqrt{\frac{1}{\gamma\beta^2}} \quad (32)$$

where: ρ - is the pseudorange measurement
 σ_{ρ} - is the pseudorange standard deviation
 γ - is the SNR
 β - is the signal bandwidth

The combined gain of power and bandwidth leads to a 36 dB SNR gain of TPS (television positioning system) over GPS, demonstrating the physical superiority of TPS. However, since the signals are not designed for positioning applications and they travel in more harsh multipath conditions, there tend to be more outlying pseudorange measurements in terrestrial signal-based positioning compared to satellite-based positioning systems. Conventional receiver autonomous integrity monitoring (RAIM) systems assume a single satellite failure. In order to handle the multi-fault case, the traditional RAIM algorithms should be modified.

9 Implemented HW for interference mitigation

Some HW implementations have already been discussed to quantify the interference on GPS. [35] discussed the interference of a commercially available UWB transmitter on a GPS receiver in close proximity. In what follows, three more examples are treated in more detail.

The Luleå University of Technology developed a network of low cost ASIC front end modules for detection and localization of interference sources in the GPS L1/E1 band [42]. The key concept is a network of independent monitoring stations connected to a central server. Once an interference source is detected by one of the monitoring stations, the localization is performed by combining the data from the several stations (Figure 8). The power levels of each GPS signal are below the noise floor. Hence, a sudden increase or

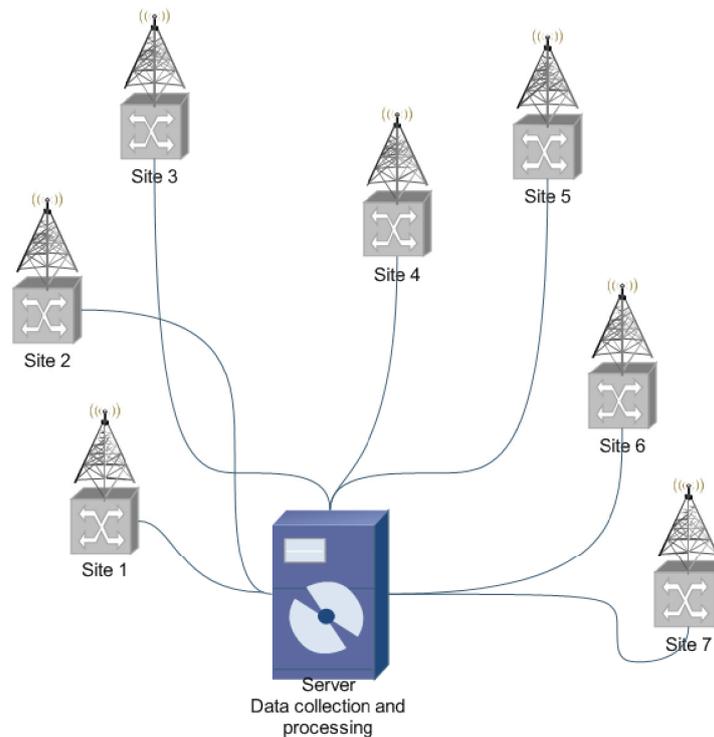


Figure 8: basic network layout

decrease in power levels indicates the presence of an interference source. Slow changes in power levels that can be due to changes in antenna temperature or the number of visible antennas are filtered out. The localization of the interference source can be done by monitoring the automatic gain control (AGC) power or by applying hyperbolic localization. Both localization techniques have been verified by test and produce results

with an accuracy within a few tens of meters.

The Nokia Research Centre illustrated the difficulties posed by integrating a GPS receiver in a multiradio terminal [36]. The radio ASIC integrating a cellular system as well as GPS in a cellular phone is considered as one of the most severe and hostile radio environment challenges. The GPS receiver chain was integrated as part of a multiband and multimode receiver, designed for GSM and WCDMA (cfr. Figure 9). The objective was to

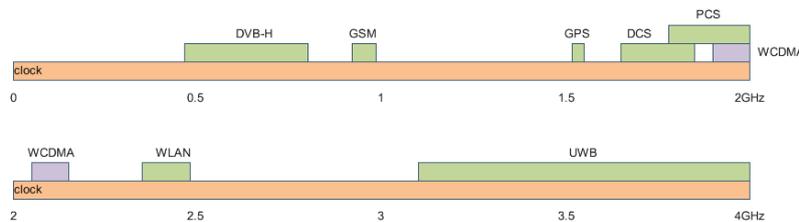


Figure 9: frequencies of radio systems in a terminal

share hardware resources with some existing ASICs. A solution is proposed adding GPS to an existing receiver supporting GSM and WCDMA systems, with only minor additions and changes to the circuitry. The GPS receiver has state-of-the-art performance without degrading the GSM and WCDMA functionality.

The German Aerospace Centre (DLR) studied the potentially critical interference environments for mass market receivers [43]. They carried out an interference measurement campaign in the framework of the GJU project GIRASOLE. As Galileo enters the GNSS fields, it is compared to its predecessors with regard to accuracy, integrity, availability and robustness. The biggest advantage for the user will be a bigger availability and precision in urban area by processing signals from different systems, for instance GPS and GALILEO. As a consequence, mass market receivers will also increase the bandwidth of their front ends. Changing the bandwidth of the front end signifies as well altering the interference impact for GPS. DLR tested several mass market receivers to quantify the impact. Scope was to identify the interference environment by measurement, characterize the interference and model an actual interference scenario. A big diversity of interfering signals was acquired, ranging from continuous wave, broadband signals to pulsed interference. A wideband signal with three subcarriers and fixed frequency separation was selected. For the simulations worst case situation was assumed with a carrier frequency of the interfering signal matching perfectly with the GPS centre frequency. Several metrics have been used to evaluate the performance of the mass market receivers. Acquisition and tracking threshold are defined as the ratio C/N enabling acquisition and tracking respectively. Besides, the code tracking error is analyzed to evaluate the performance. The hardware receivers that have been tested are **Novatel EuroPak-15a** and **NordNav R30**.

	Acquisition Threshold ISR	Tracking Threshold ISR
Software Rx GPS	25dB	35dB
Software Rx GALILEO	30dB	35dB
Hardware Rx Novatel	26dB	40dB
Hardware Rx NordNav	33dB	40dB

Table 5: comparison of acquisition and tracking thresholds

With increasing interference-to-signal ratios (ISR) for GPS or GALILEO the code tracking error increases considerably for values greater than 20dB. However, the maximum code error before loss of lock is with 2.2m for GALILEO much less than the 4.5m in the GPS case. The C/N level decreases non-linearly with increasing ISR. An overview is given in Table 5.

10 Summary

This report discusses the relevance of a RF interference impact assessment on Global Navigation Satellite Systems and contains an overview of state-of-the-art detection and mitigation techniques. The first chapters make three important statements. First, the GNSS signal power levels are extremely low, due to the distance the signals have to travel. These low signal power levels motivate the use of spread spectrum techniques. Further, it has been shown that unintentional RF interference is ubiquitous. In close proximity to the GNSS frequency bands, services are active for satellite communications, TV broadcasting, radar and UWB applications. These services can cause problems of different nature: out-of-band emissions, harmonics or intermodulation products. Finally, despite the weak signal environment, GNSS is increasingly used in critical applications. In aviation, GNSS gives a solution for all phases of flight. Monitoring of dangerous goods relies on GNSS as well as the precise distribution of time. The use of GNSS in critical applications explains the existence of intentional interference.

The weak signal environment, presence of intentional and unintentional interference and the use of GNSS in critical applications urges for an impact assessment of RFI. Narrowband and wideband interferers have been discussed. In the case of narrowband interferers, it has been shown that the impact of the interferer depends on its proximity to one of the spectral lines of the code spectrum. Further, an acceptable jammer-to-signal ratio has been calculated and the corresponding operating range of the GNSS receiver from the source of interference has been deduced.

There is a clear need for a methodology or a metric to estimate the GNSS signal environment. Several techniques have been introduced, assessing and characterizing the interference in different parts of the GNSS receiver. The different metrics cover spectral analysis, monitoring of the behavior of the AGC, monitoring of the acquisition and tracking performance and estimation techniques of the carrier power to noise density ratio. Furthermore, the main interference mitigation techniques have been discussed, comprising of spatial and spectral signal processing.

Finally, emphasis has been given to the scenario of UWB interference. This topic has been studied thoroughly, by means of experiments as well as analytically. It has been shown that different performance criteria have been used and a extensive list of scenarios has been tested. Main result of those studies is the quantification of maximum allowable EIRP levels for all UWB signal permutations. A relaxation of the current UWB emission levels in the GNSS frequency bands is not recommended.

ANNEX A: Interference Detection

Multicorrelator receivers for interference detection and identification

Interference is a relevant issue with respect to the use of GNSS in aviation. A large amount of methods have been developed to mitigate the interference effects. These methods range from spatial processing with antenna arrays over spectral discrimination to amplitude detection. Also multicorrelator techniques can be applied to deal with the interference threat [44]. The possibility to characterize the interference effects on the tracking loops by the analysis of the shape of the correlation peak has been demonstrated.

The first step in the algorithm is the detection of the presence of a disturbing signal. The impact of a CW jammer on the correlator output has been demonstrated. The amplitude of the distortion depends on the relative amplitude of jammer and received GPS signal, on the frequency offset between jammer and the nearest C/A code line and finally on the height of that spectral line. Since an interfering signal distorts the correlator output, the FFT of the output can indicate the presence of interference. In the second step of the algorithm, the number of sinusoidal signals and their respective characteristics as central frequency and bandwidth are determined. This is done by applying parametrical methods, based on autoregression models such as Prony or ESPRIT. Finally, the instantaneous estimates are postprocessed. The statistical postprocessing brings robustness with regard to outliers and additional stability of the method.

Analysis of RF interference effects on A/D conversion

The effects of interference on A/D conversion depends on the instant in the processing chain where the A/D conversion appears [6]. Distinction can be made between pre- and postcorrelation A/D converters (Figure 10). The pre-correlation A/D conversion is

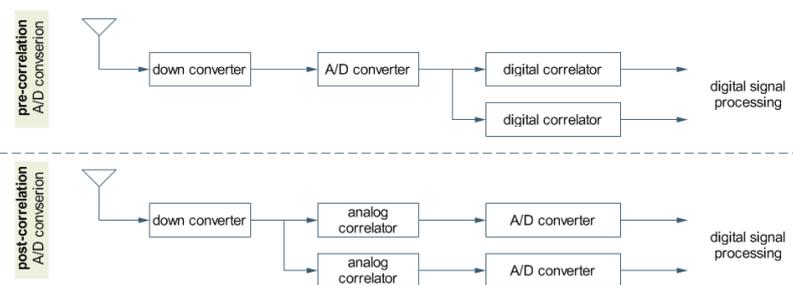


Figure 10: comparison of pre-correlation and post-correlation A/D conversion

performed at IF and the digital IF becomes a shared function by all the digital receiver channels. The post-correlation A/D conversion on the other hand is performed at base-band for each correlated output. This requires multiple A/D converters for each channel.

Because of the benefit of component reduction, virtually all GPS receivers have pre-correlation A/D conversion.

Nonetheless, the drawback of pre-correlation A/D conversion is the increased vulnerability to continuous wave (CW) interference. After the downconversion, the power spectrum still contains the CW signal and consequently the CW content is applied to the precorrelation A/D converter. This is in particular precarious for 1-bit converters. As a result of the CW content, the zero crossings of the converter input signal are no longer determined by the GPS signals and random noise, but are dominated by the CW signal. A post-correlation A/D converter on the contrary is not to the same extent subject to CW jamming. The correlation process that despread the GPS signals, spreads in addition the CW interference into broadband interference before it reaches the A/D converter. This wideband noise has a significantly reduced peak power and thus the postcorrelation A/D converter is protected against CW interference. The processing gain achieved against CW jamming by the spread spectrum signal is defined by the jammer-to-signal power ratio at the antenna ant the J/S ratio beyond the A/D convertor. At the antenna this ratio is given by

$$\left(\frac{j}{s}\right)_{ant} = \frac{J^2}{P_s} \quad (33)$$

with J the CW jammer power and P_s the signal power, both at the receiver input. After the A/D conversion, we get:

$$\left(\frac{j}{s}\right)_{AD} = \frac{\left(\frac{J^2}{R_c}\right)2R_b}{P_s} \quad (34)$$

where R_c is the GPS PRN code chipping rate and R_b is the data modulation bandwidth. Accordingly, the processing gain is given by

$$P_G = \frac{\left(\frac{j}{s}\right)_{ant}}{\left(\frac{j}{s}\right)_{AD}} = \frac{R_c}{2R_b} \quad (35)$$

This means the processing gain against CW interference is directly proportional to the code chipping rate and inversely proportional to the data modulation bandwidth. The pre-correlation A/D converter is not protected by this spread spectrum processing and hence experiences the full CW interference.

Quantizer effects in the presence of interference

In the following we will demonstrate that the performance of a one-bit quantizer degrades substantially in the presence of a coherent CW tone with respect to the same quantizer in presence of white thermal noise of the same power [5]. Yet, a well-designed multibit ADC can effectively reduce the interference effects if the quantizer levels are properly set. Two forms of interference will be considered. Gaussian noise simply adds to the Gaussian thermal noise of the receiver. Sinusoidal noise on the other hand can

be of CW, narrowband or wide band form. The metric to quantify and analyze the quantizer performance is the SNR at the quantizer-correlator output with respect to the input SNR. It is well known that the output signal-to-interference ratio is degraded by 6dB in the presence of a strong sinusoidal signals with a large frequency offset. The degradation is much more relevant if the sinusoidal interfering signal has the same frequency and phase. In that case, the interference can suppress the desired signal by much more than 6dB and capture the receiver. The signal model used in the following discussion is shown in figure 11. We suppose that the signal along with gaussian noise and sinusoidal

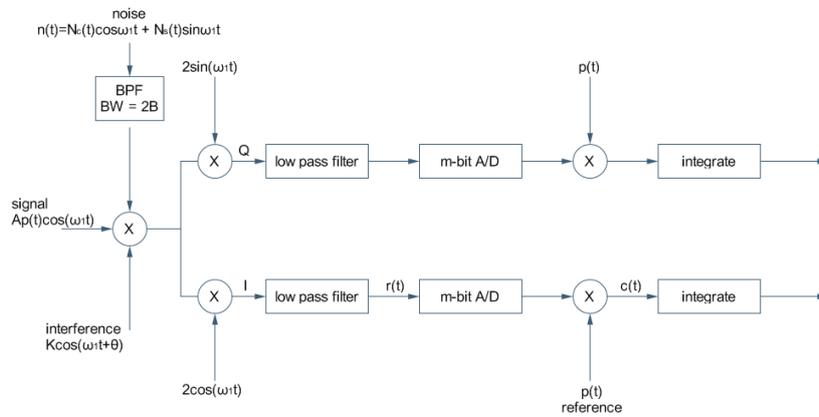


Figure 11: signal model for an m-bit A/D converter

interference has been downconverted to baseband. Moreover, it is assumed that the filters have a sufficiently wide bandwidth such that filter distortion effects are negligible. The input $r(t)$ to the coherent quantizer channel is than the low-pass filter output $r(t) = Ap(t) + K\cos\theta(t) + N_c(t)$, where A is the desired signal amplitude, $p(t)$ the spreading code equal to ± 1 with equal probability and K the interfering signal amplitude. The bandlimited white noise $N_c(t)$ is assumed to have zero mean, variance σ^2 and gaussian statistics. The input to the quantizer has probability density $\frac{1}{2}Normal(\mu_+, \sigma) + \frac{1}{2}Normal(\mu_-, \sigma)$, with $\mu_+ = K + A$ and $\mu_- = K - A$. Following the processing chain of figure 11, the quantizer output is defined as $Q_m[r(t)]$ with Q_m the m-bit quantizer characteristic; the correlator output at last is $c(t) = p(t)Q_m[r(t)]$. The degradation in quantizer-correlator SNR output with regard to the quantizer input signal-to-thermal-noise ratio is given by

$$R(K, \sigma, A, m, \Delta) = \frac{SNR_o}{A^2/\sigma^2} \quad (36)$$

where m is the number of bits in the quantizer and Δ is the quantizer interval. It should be noted that R is function of the interference environment (K, σ) , but also depends on the setting of the quantizer by the number of bits and the quantizer interval.

We start the study with the analysis of a one-bit quantizer with a received input consisting of a unit amplitude bi-phase modulated signal, gaussian noise and sinusoidal interference. A coherent interference of sufficient size is able to capture the receiver

completely. That is, the quantizer output has almost no correlation with the input C/A pseudo-random noise $p(t)$. At larger levels of the interference, the degradation of the quantizer output SNR relative to the quantizer input SNR rapidly increases up to 30dB. The interference level at this stage is not much higher than the receiver thermal noise figure. If tolerance against coherent constant envelope sinusoidal interference is required, the one-bit quantizing is unacceptable. Hitherto, we supposed that the sinusoidal interference was in phase with the signal of interest. If the interference is out of phase by some angle θ , then the effective interference becomes $K\cos\theta$ instead of K . With the angle θ is slowly varying, the signal is periodically attenuated. On the other hand, if there is a large frequency offset between interference and signal of interest, then the output of the quantizer can be computed by averaging over θ in the $K\cos\theta$ -term.

Yet, we can opt for a two-bit quantizer. If the quantizer interval Δ is selected equal to 0 or ∞ , the operation of the two-bit quantizer is reduced to a one-bit quantizer. It can be shown that there is a minimum value of SNR degradation depending on the quantizer interval Δ . In case of interference with Gaussian statistics the best performance is reached as $\Delta = \sqrt{\sigma_n^2 + \sigma_I^2}$, where σ_n and σ_I are respectively the noise and the interfering power levels. We assume now that the signal of interest is subject to gaussian noise and constant, coherent sinusoidal interference of amplitude $K\cos\theta$ with θ constant. In this case, there is a range of quantizer interval settings exposing an acceptable SNR degradation. This range of quantizer settings grows however narrower with increasing sinusoidal interference. Besides, we call attention to the fact the with increasing interference, the degradation doesn't increase proportionally with total noise plus interference power, as would be the case for Gaussian interference. The optimum setting of the AGC is given by $\Delta = \sqrt{\sigma^2 + K^2}$. In this case, the constant interference simply acts as a constant bias and the interference effect itself is suppressed by the quantizer. Still any variation in interference magnitude or phase would reduce this nulling effect. Consider a slowly varying interference phase θ and suppose the quantizer lever is kept constant at $\Delta = \sqrt{\sigma^2 + K^2}$, then the degradation also varies slowly with the phase offset. Finally, consider an sinusoidal interference that is frequency offset with regard to the center frequency of the PN signal. The AGC performance is now determined by the time average of the interference. The optimum quantizer interval is, once again, equal to $\Delta \cong \sqrt{\sigma^2 + K^2}$.

Finally, we discuss the performance of a three-bit quantizer. If there is no sinusoidal interference the minimum degradation occurs with a quantizer interval $\Delta = \frac{\sigma}{\sqrt{3}}$. The minimum degradation is 0.1613 dB vs 0.5415 dB for the two-bit quantizer. Furthermore, the quantizer setting is less sensitive than the 2-bit AGC. The optimum quantizer interval corresponds once again to $\Delta = \sqrt{\sigma^2 + K^2}$.

As a final remark, we want to call attention to the fact that all discussed quantizers are uniform quantizers with equal step sizes. It can however be shown that non-uniform the interference suppression performance increases when non-uniform stepsizes are used. This benefit does not occur though with thermal noise only.

ANNEX B: Detailed Literature on Interference Mitigation

Robust signal quality monitoring [45] As discussed before, RF interference can jeopardize the availability, accuracy and integrity of the GPS signal. As the RFI power levels increase, the GPS accuracy decays and can lead to loss of lock. For integrity-critical applications such as auto-landing systems in aviation, the threat of loss of integrity has to be monitored. Therefore it is necessary to evaluate the quality of the received signal, detecting the presence of RFI and raising an alert of reduced GPS integrity. Former algorithms for interference detection and integrity monitoring comprise parity checks, ground based integrity monitoring and receiver autonomous interference monitoring (RAIM). Parity checks verify errors in the data stream, but don't give any timing information. Ground based integrity monitoring doesn't give information on local introduced interference, originating for instance on local electronic devices. RAIM computes position solutions based on different sets of satellites. This requires an overspecified navigation problem. The method proposed studies the effects of interference on raw receiver signals and pseudorange errors. The signal quality is measured based on correlator-level measurements (correlator output power variance, carrier phase jitter, etc.).

Multicorrelator techniques [46] Signal anomalies discussed in this work originate from multipath and soft failures of the signal generating hardware. A signal quality monitor detecting evil waveforms in the presence of multipath is presented. Moreover a real-time tracking error compensator algorithm is introduced providing significant accuracy improvement.

Interference detection and localization [47] The Generalized Interference Detection and Localization System (GIDL) combines different domains ranging from interference detection, advanced signal processing, beamforming and null-steering, signal source localization etc. The GPS receiver can be implemented with different measures against interference. Bandpass filters are used to prevent out-of-band RF interference, pulse blanking reduces the effects of pulsed interference, full processing gain is assured by selecting the appropriate number of quantizing levels and Automatic Gain Control (AGC). A flexible simulation and testing environment is provided by the SW radio implementation. Former work on GPS interference localization has already been performed. Different algorithms have already been implemented in order to specify the number of interference emitters and their directions (Multiple Signal Classification etc.). Multipath direction finding and multipath mitigation techniques for GNSS have been proposed and tested. GPS adaptive antenna arrays have been developed. The core of this work is the presentation of an optimized design.

Navigation accuracy and interference rejection for GPS adaptive antenna arrays [48] The ultimate aviation objective for GPS is auto-land. This requires high levels of accu-

racy and integrity during final approach and landing. The need for RF threat mitigation is obvious. Multi-element antenna arrays using space-time adaptive processing improve significantly the signal to interference plus noise ratio (SINR). The drawback of the spatial and temporal filtering is the introduction of biases in the GPS measurements. A tradeoff has to be made between interference rejection and measurement biases. The proposed architecture is intended to meet the requirements for accuracy, interference rejection and integrity. Code-phase positioning has a lower bound on accuracy of several meters for C/A code and tens of centimeters for P(Y) code. Differential carrier phase measurements on the other hand has a lower bound accuracy in the order of one centimeter. The carrier-phase difference is comprised of a integer number of entire carrier cycles (the integer cycle ambiguity) and a fractional carrier-phase. The interference rejection is tackled with controlled reception pattern antenna (CRPA) arrays. The CRPA increases the SINR by enhancing the array gain in the direction of the desired signals and attenuating interference signals. Weighting factors in the antenna array can be determined deterministically or adaptively. The integrity requirements are met by high-performance integer ambiguity resolution algorithms. However, multi-element antenna arrays may introduce additional biases most mainly by electromagnetic coupling and spatial/temporal filtering. Mutual coupling between the array elements changes the electromagnetic response of each antenna, while temporal processing deteriorates signal distortion and the corresponding biases. Bias mitigation is performed by antenna equalization and line-of-sight-based bias compensation. In order to alleviate the processing demands for the receiver, deterministic corrections can be applied which are function of the arrival direction and signal frequency. For a deterministic beamforming CRPA, the weighting coefficients are deterministically determined by the array geometry and the satellite ephemeris. Hence, the corresponding biases likewise are deterministic and may be calibrated. Yet, for an adaptive antenna array, the weighting coefficients are function of the noise environment. As a consequence the biases are not deterministic and can not be calibrated a priori.

Mitigation of signal biases introduced by a CRPA [49] In this work Joint Precision Approach and Landing Systems (JPALS) are considered. An aircraft carrier is a harsh multipath environment where service should be maintained in the presence of hostile RFI. CRPA arrays have striking benefits concerning multipath mitigation and interference rejection. However the code and carrier phase biases introduced by the array should be mitigated. Two different mitigation schemes are presented.

Phase effects analysis of CRPAs [50] The mechanism that an antenna array uses to change the reception pattern is the alternation of phase of each antenna channel. Therefore, any possible effect on the carrier phase content should be characterized. The magnitude and location of the phase effect depend on the exact configuration of the array. The phase pattern of each antenna element in a CRPA is different and is modeled as a function of azimuth and elevation.

More detection and location of interference sources [51] Digital phased array data can be used to detect and locate GPS interference sources. By cross-correlating the signals of the different antenna elements, the direction of arrival of the interfering signal can be obtained. In the presence of only GPS signals, the cross-correlation product only observes noise, since the GPS signals are below the noise floor of the receiver. But then in the presence of an interfering signal, power will be detected in the cross-correlation product.

Multiple signal direction finding and interference reduction techniques [52] In cellular communication networks, frequency bands are re-used based on the physical separation of the different cells. Ground-based receivers can either just pick up the desired signal or the desired signal dominates the interfering signals. Airborn platforms on the other hand can receive signals originating from different cells using the same frequency. Several radio transmitters using the same frequency cause crosstalk or co-channel interference. Harmonics or intermodulation products can also yield interference and mask the signal of interest (SOI). Interference reduction or signal copy is the process of extracting the SOI out of the interference and background noise.

Even though different radio transmitters can use the same carrier frequency, the angle of arrival of those different sources is often well separated. Spatial processing techniques can be applied for direction finding (DF) and subsequently for interference reduction. Each element m of an antenna array receives data from d signals. For every antenna element we can write

$$x(k) = a(\theta_1)s_1(k) + a(\theta_2)s_1(2) + \dots + a(\theta_d)s_d(k) + n(k) \quad (37)$$

$$= A(\theta)s(k) + n(k) \quad (38)$$

where: k - is the sampling time

$s_l(k)$ - is the scalar representing the l^{th} signal

$a(\theta_l)$ - is the antenna array response in the direction of the l^{th} signal

$n(k)$ - is additive white noise

Since the signals overlap spectrally, spectral filtering is not capable of isolating the signal of interest. Spatial filtering uses beamforming and passes the SOI while nulling the co-channel interference

$$\hat{s}_l(k) = w_l^H x(k) \approx \alpha s_l(k) + w_l^H n(k) \quad (39)$$

In this equation \hat{s}_l is the estimate of the l^{th} signal and w_l is the beamformer for extracting the l^{th} signal. There are several approaches to perform direction finding or angle-of-arrival (AOA) estimation. In direct direction finding estimation the AOA is computed based on the received data. Other algorithms, copy-based direction finding algorithms, make use of the beamforming weighting vector of the desired signal of interest. One of the remaining variables for multiple signal direction finding is the retrieval of the array response vector for each signal. The main approaches to determine the array response

vector are signal-subspace techniques and property restoral techniques. The MUSIC (multiple signal classification) algorithm belongs to the first group of techniques. The first step is to determine the number of active signals d . Next, the signal subspace is computed based on the eigenvectors of the received data, associated with the largest eigenvalues. Finally, we define the array manifold, i.e. the set of antenna array response vectors. The intersection of the array manifold and the signal subspace determine the angle-of-arrival estimates.

As a conclusion, many algorithms are available to alleviate the co-channel interference. The data processing results in co-channel environments are impressive. Accurate estimates of angle-of-arrival are possible for signals separated by 0.1 beamwidths or more. SIR can improve with 20-30 dB, even for challenging scenarios. Different algorithms for multiple signal direction finding can be implemented on a single DSP processor chip.

ANNEX C: Detailed Literature on UWB Interference on GNSS

In-band interference of three different UWB signals in GPS L1 band [53] Three different types of pulse waveforms to generate UWB signals are tested: a Gaussian pulse is used, then a Gaussian doublet (composed of two amplitude reversed Gaussian pulses with time gap between the pulses) and finally, the third derivative of the Gaussian pulse. For an UWB system the spectral allocation is determined by the pulse waveform and the pulse width. Using a Gaussian doublet doesn't alter the power spectrum envelope but introduces some spectral nulls. Those nulls can be used to mitigate the interference threats. The spectrum of the third derivative of the Gaussian pulse goes twice as high as the one of the Gaussian pulse. However, the generation of the waveform is far more complex. Concerning the modulation technique, a system using direct sequence spread spectrum interferes less than the system using time hopping.

Coexistence of UWB and other wireless systems [54] The large bandwidth required by UWB, can not be allocated exclusively. Therefore the assessment of the interference caused by UWB on existing systems is of primary importance to ensure coexistence and to guarantee acceptance of UWB technology. Similar to many other wireless local area network systems, it should be noted that UWB terminals are in sleep mode for a large percentage of time and will not emit constantly on maximum power. Different from the results presented in the open literature, it is found that there is no risk for UMTS, GPS and DCS receivers operations, especially when the carrier frequency is selected to lie in the 3.1-10.6 GHz band.

References

- [1] John A. Volpe National Transportation Systems Center. Vulnerability assessment of the transportation infrastructure relying on the global positioning system - final report, august 2001.
- [2] Kenneth Martin. GPS timing in electric power systems. ION GPS, september 1999, Nashville, TN.
- [3] P. Mann and E. Butterline. Global positioning system use in telecommunications. ION GPS, 1998.
- [4] S.J. Harding. Study into the impact on capability of UK commercial and domestic services resulting from the loss of GPS signals. Technical report, Qinetiq, 2001.
- [5] J.J. Parkinson, B.W. Spilker. *Global Positioning System Theory and Applications*. AIAA, 1996.
- [6] Elliott D. Kaplan. *Understanding GPS Principles and Applications*. Artech House, 1996.
- [7] P. Misra and P. Enge. *Global Positioning System: Signals, Measurements and Performance*. Ganga-Jamuna Press, second edition, 2006.
- [8] James Bao-Yen Tsui. *Fundamentals of global positioning system receivers*. Wiley, 2005.
- [9] Nel Samana. *Global Positioning: Technologies and Performance*. Wiley-Interscience, 2008.
- [10] Jay R. Sklar. Interference mitigation approaches for the global positioning system. *Lincoln Laboratory Journal*, 14(2), 2003.
- [11] T.A Stansell. Expert advise - location assurance. *GPS World*, 2007.
- [12] J.S. Warner and R.G. Johnston. A simple demonstration that gps is vulnerable to spoofing. *Journal of Security Administration*, 2003.
- [13] G. Hein, F. Kneissi, J.-A. Avilla-Rodriguez, and S. Wallner. Authenticating gnss: Proofs against spoofs, part 1. *Inside GNSS*, pages 58-63, July/August 2007.
- [14] G. Hein, F. Kneissi, J.-A. Avilla-Rodriguez, and S. Wallner. Authenticating gnss: Proofs against spoofs, part 2. *Inside GNSS*, pages 71-78, September/October 2007.
- [15] L. Scott. Anti-spoofing and authenticated signal architectures for civil navigation systems. *proc. ION/GNSS conference*, September 2003. Portland, OR.

- [16] T.E. Humphreys, B.M. Ledvina, M.L. Psiaki, W. O'Hanlon, and P.M. Kintner. Assessing the spoofing threat: Development of a portable GPS civilian spoofer. *proc. ION/GNSS*, September 2008. Savannah, GA.
- [17] P.Y. Montgomery, T.E. Humphreys, and B.M. Ledvina. Receiver-autonomous spoofing detection: experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer. *ION International Technical Meeting*, January 2009. Anaheim, CA.
- [18] P.Y. Montgomery, T.E. Humphreys, and B.M. Ledvina. A multi-antenna defense: Receiver-autonomous GPS spoofing detection. *Inside GNSS*, pages 40-46, March/April 2009.
- [19] E.L. Key. Techniques to counter GPS spoofing. Febr 1995. internal memorandum, MITRE Corporation.
- [20] Andrea Goldsmith. *Wireless Communications*. Cambridge University Press, 2005.
- [21] Navstar. Icd-gps-200 interface control document, 1994.
- [22] Changlin Ma, Gyu-In Jee, Glenn MacGougan, and Gerard Lachapelle. GPS signal degradation modeling. *ION GPS 2001*, september 2001. Salt Lake City, UT.
- [23] F. Bastide, D. Akos, C. Macabiau, and B. Roturier. Automatic gain control (AGC) as an interference assessment tool. *ION GPS*, 2003.
- [24] B. Motella, M. Pini, and F. Dosis. Investigation on the effect of strong out-of-band signals on global navigation satellite systems receivers. *GPS Solutions*, 12(2), march 2008.
- [25] A.T. Balaei, A.G. Dempster, and J. Barnes. A novel approach in detection and characterization of CW interference of GPS signal using receiver estimation of C/N0. *proceeding of IEEE/ION PLANS*, pages 1120-1126, 2006.
- [26] P.D. Groves. GPS signal-to-noise measurement in weak signal and high-interference environments. *Journal of the Institute of Navigation*, 52(2), 2005.
- [27] B. Motella, S. Savasta, D. Margaria, and F. Dosis. An interference impact assessment model for GNSS signals. *proc. ION GNSS conference*, 2008. Savannah, Georgia.
- [28] M. Wildemeersch and J. Fortuny-Guasch. A laboratory testbed for GNSS interference impact assessment. *proc. ION GNSS conference*, 2009. Savannah, Georgia.
- [29] V. Valmettes, F. Pradeilles, and M. Bousquet. Study and comparison of interference mitigation techniques for GPS receiver. *ION GPS 2001*, september 2001. Salt Lake City, UT.

- [30] David S. Anderson, Edward F. Drocella, Steven K. Jones, and Mark A. Settle. Assessment of compatibility between uwb systems and global positioning system (GPS) receivers. Technical report, NTIA, february 2001.
- [31] M. Luo, D. Akos, S. Pullen, and P. Enge. Potential interference to GPS from UWB transmitters - phase 1a: Accuracy and loss-of-lock testing for aviation receivers. Technical report, Stanford University, october 2000.
- [32] M. Luo, M. Koenig, D. Akos, S. Pullen, and P. Enge. Potential interference to GPS from UWB transmitters - phase ii: Accuracy, loss-of-lock, and acquisition testing for GPS receivers in the presence of UWB signals. Technical report, Stanford University, march 2001.
- [33] M. Luo, D. Akos, M. Koenig, G. Opshaug, and P. Pullen, S. Enge. Testing and research on interference to GPS from UWB transmitters.
- [34] B.M. Titus et al. Assessing ultra wide band UWB interference to GPS receivers. ION GPS, september 2002, Portland, OR.
- [35] Tyler Van Slyke, B. Kuhn, and B Natarajan. Measuring interference from a UWB transmitter in the GPS L1 band. *IEEE*, 2008.
- [36] Mikael Gustafsson et al. A low noise figure 1.2-V CMOS GPS receiver integrated as a part of a multimode receiver. *IEEE Journal of Solid-State circuits*, 42(7), july 2007.
- [37] Y.T. Morton, M.P. French, Q Zhou, J.B.Y. Tsui, D.M. Lin, M.M. Miller, and D. Janning. Software approach to access UWB interference on GPS receivers. *IEEE A&E Systems Magazine*, january 2005.
- [38] F. Klinker and Pietersen O.B.M. Interference of GPS signals: Influence of licensed transmitters on the GPS signal quality in the netherlands' airspace. Nationaal Lucht-en Ruimtevaartlaboratorium.
- [39] Ju-Yong Do. Road to seamless positioning: Hybrid positioning system combining GPS and television signals. Technical report, Stanford University, april 2008.
- [40] Ju-Yong Do, M. Rabinowitz, and P. Enge. Multi-fault tolerant RAIM algorithm for hybrid GPS/TV positioning. ION NTM 2007, january 2007, San Diego, CA.
- [41] Ju-Yong Do, M. Rabinowitz, and P. Enge. Performance of hybrid positioning system combining GPS and television signals. *IEEE*, 2006.
- [42] J. Lindstrom, D. Akos, O. Isoz, and M. Junered. GNSS interference detection and localization using a network of low cost front-end modules, 2007.
- [43] Christian Weber, Andriy Konovaltsev, and Michael Meurer. Investigation of potentially critical interference environments for GPS/GALILEO mass marker receivers.

- [44] Frederic Bastide, Eric Chatre, and Christophe Macabiau. GPS interference detection and identification using multicorrelator receivers. *ION GPS 2001*, september 2001. Salt Lake City, UT.
- [45] Awele N. Ndili. *Robust GPS autonomous signal quality monitoring*. PhD thesis, Stanford University, august 1998.
- [46] Robert Eric Phelts. *Multicorrelator techniques for the robust mitigation of threats to GPS signal quality*. PhD thesis, Stanford University, june 2001.
- [47] Konstantin G. Gromov. *GIDL: generalized interference detection and localization system*. PhD thesis, Stanford University, march 2002.
- [48] David S. De Lorenzo. *Navigation accuracy and interference rejection for GPS adaptive antenna arrays*. PhD thesis, Stanford University, august 2007.
- [49] Ung Suok Kim. *Mitigation of signal biases introduced by controlled reception pattern antennas in a high integrity carrier phase differential GPS system*. PhD thesis, Stanford University, march 2007.
- [50] U.S. Kim, D. De Lorenzo, J. Gautier, and P. Enge. Phase effect analysis of patch antenna CRPAs for JPALS. ION GNSS 17th International Technical Meeting of the Satellite Division, 2004, Long Beach, CA.
- [51] A. Brown, S. Atterberg, and N. Gerein. Detection and location of GPS interference sources using digital receiver electronics. Proceedings of ION annual meeting, June 2000, San Diego, CA.
- [52] Frank McCarthy. Multiple signal direction-finding and interference reduction techniques. *Wescon Technical Conference*, pages 354-361, august 1993.
- [53] Matti Hamalainen et al. In-band interference of three kind of UWB signals in GPS L1 band and GSM900 uplink band. *IEEE*, 2001.
- [54] R. Giuliano and F. Mazzenga. On the coexistence of power-controlled UWB systems with UMTS, GPS, DCS1800 and fixed wireless systems. *IEEE Transactions on vehicular technology*, 54(1), January 2005.

How to obtain EU publications

Our priced publications are available from EU Bookshop (<http://bookshop.europa.eu>), where you can place an order with the sales agent of your choice.

The Publications Office has a worldwide network of sales agents. You can obtain their contact details by sending a fax to (352) 29 29-42758.

European Commission

EUR 24242 EN - Joint Research Centre - Institute for the Protection and Security of the Citizen
Radio Frequency Interference Impact Assessment on Global Navigation Satellite Systems
January 2010

Authors: Matthias Wildemeersch, Joaquim Fortuny-Guasch
EC Joint Research Centre, Security Technology Assessment Unit

Luxembourg: Publications Office of the European Union
2010 - 66 pp. - 21 x 29.7 cm
EUR - Scientific and Technical Research series - ISSN 1018-5593
ISBN 978-92-79-14989-4
DOI 10.2788/6033

Abstract

The Institute for the Protection and Security of the Citizen of the EC Joint Research Centre (IPSC-JRC) has been mandated to perform a study on the Radio Frequency (RF) threat against telecommunications and ICT control systems. This study is divided into two parts. The first part concerns the assessment of high energy radio frequency (HERF) threats, where the focus is on the generation of electromagnetic pulses (EMP), the development of corresponding devices and the possible impact on ICT and power distribution systems. The second part of the study concerns radio frequency interference (RFI) with regard to global navigation satellite systems (GNSS). This document contributes to the second part and contains a detailed literature study disclosing the weaknesses of GNSS systems. Whereas the HERF analysis only concerns intentional interference issues, this study on GNSS also takes into account unintentional interference, enlarging the spectrum of plausible interference scenarios.

The mission of the JRC is to provide customer-driven scientific and technical support for the conception, development, implementation and monitoring of EU policies. As a service of the European Commission, the JRC functions as a reference centre of science and technology for the Union. Close to the policy-making process, it serves the common interest of the Member States, while being independent of special interests, whether private or national

LB-NA-24242-EN-C



ISBN 978-92-79-14989-4



9 789279 149894