Increasing International Civil Aviation Resilience: A Proposal for Nomenclature, Categorization and Treatment of New Interference Threats

Ignacio Fernández-Hernández, *European Commission*
Todd Walter, *Stanford University*
Ken Alexander, *Federal Aviation Administration*
Barbara Clark, *Federal Aviation Administration*
Eric Châtre, *European Commission*
Chris Hegarty, *MITRE*
Manuel Appel, *DLR*
Michael Meurer, *DLR*

Abstract
Electromagnetic interference can degrade civil Global Navigation Satellite System (GNSS) signals and services, and in some cases result in integrity failures. The aviation community is well-aware of such threats due to the proliferation of interfering-capable equipment including personal electronic devices (PEDs), personal privacy devices (PPDs), GNSS repeaters, mis-operated test equipment, low-cost software-defined radio cards, and the foreseeable proliferation of more sophisticated spoofing devices in the future. Protection against such interference is under consideration for the next-generation of avionics standards.

This paper is intended to support the definition of new avionics standards that address these interference threats. First, it provides a current review of the technical literature with a focus on aviation. Then, the paper compiles the existing nomenclature, taking into account definitions from regulatory bodies. Next, the paper identifies categories of threat emissions. Later, the assets to protect and use case under analysis are presented, followed by a discussion of detection and mitigation responses. The paper continues with a list of detection and mitigation actions that can be implemented at different stages of the avionics receiver. Finally, the paper concludes with a discussion on possible treatment of specific threat categories in the next generation of standards.

This paper is intended to provide a framework for discussing standards, recommended practices, and test procedures for the treatment of emissions that may be encountered by future equipment. Common nomenclature and threat categorization of jamming and spoofing threats was not available prior to this effort. The framework is the result of several months of iterations including research institutes, GNSS providers, and air navigation service providers. This work provides a common framework that can be used for threat modeling and quantitative risk analysis to enable development of future requirements and associated test procedures in the next generation of aviation standards.

Background

This section presents a short review on general radio frequency interference, with a focus on the treatment of interference, jamming and spoofing threats in current aviation standards. GPS/Galileo/GNSS radio frequency interference has been a subject of study since the beginning of GPS [1]. In 2001, the Volpe Report [2] provided a wide assessment of the impact of GPS disruptions in critical applications, including aviation, which increased awareness of the

consequences of such disruptions. Since then, a wealth of literature focused on GNSS interference, but with different ways to classify interference were produced [3] [4] [5]. For example, reference [3] classifies GNSS interference as *wideband* or *narrowband*, where these two types include waveforms, such as harmonics from other band signals, energy spillover from adjacent bands, and intentional, in-band interference such as chirp jammers, pseudolites or spoofers. On the other hand, another reference [4] treats interference depending upon whether the interference is statistically independent from GNSS signals and its effect can be approximated by an increase in thermal noise, or whether the interference is correlated with GNSS signals and is assimilated as spoofing. This reference also presents canonical interference models as wideband, narrowband, the main case being CW (Continuous Waveform), or *matched spectrum*, and presents typical interference waveforms, including natural interference, such as solar bursts or scintillation, or man-made, including unintentional, accidental interference, and spoofing. This *natural* vs. *man-made* interference distinction is also presented in other references, such as reference [6].

The ICAO SARPS ([7], APP-B) treats unintentional interference in avionics receivers by defining CW interference masks, and accepted noise-like interference thresholds vs. bandwidth (Figs B-15/18) for different flight phases. For example, receivers must function in the presence of in-band CW interference below -150.5 dBW for GPS C/A-code tracking. RTCA SC-159 Minimum Operational Performance Standards (MOPS) define a Standard Received Signal and Interference Environment (SBAS MOPS [8], Appendix C) and propose test procedures for acquisition in the presence of interference and interference rejection (S2.5.4 and S2.5.7, respectively), although reduced to CW. The FAA GNSS Intentional Interference and Spoofing Study Team (GIISST) studied potential means to deal with new threats and then divided the threats into *intentional interference* and *spoofing* [9].

With regard to interference caused by jamming, the signals and effects of many typical jammers are analyzed in several references [10] [11] [12] [13]. Reference [14] reports on the delayed use of a new aviation service in order to allow ground system improvements to mitigate the effects of such illegal signals. While many reported jammers of these types use swept-tone signals, a more recent monitoring of jammers reported in reference [15] shows a wide variety of jammer fingerprints. A recording platform for different jamming events as well as an analysis is described in [16]. Jamming countermeasures depend upon the jamming emission type: Automatic Gain Control (AGC) and carrier to noise density ratio (C/N_0) monitoring can detect unusual power levels due to interference [12], stopband filtering mitigates out-of-band transmissions or adjacent energy spillover [3], pulse blanking can mitigate the effects of pulsed interference [17] [18], and notch filtering can be effective against continuous waves including the typical swept tones of PPDs [13]. Other more sophisticated anti-jamming measures include the use of controlled radiation pattern antenna (CRPA) jammer nulling or inertial measurement units (IMUs) [3].

Regarding interference caused by spoofing, this risk has been highlighted since at least 2003 [19] and the ease of building simple spoofers has been growing ever since [20] [21]. However different types of spoofers have to be distinguished as well as the know-how to build and operate complex spoofers. As with jamming, spoofing events have been observed, for example, recently in the Black Sea [22] and in the vicinity of the Kremlin [23]. Tests under laboratory conditions are reported in [24] and show the vulnerability of aeronautical receivers for different types of spoofing. Experimental results confirm the feasibility of certain attacks [25] [26].

Regarding possible spoofing detection and mitigation, reference [19] proposes countermeasures at both the signal processing level (J/N, C/N_0, antenna phase difference, deep acquisition), and navigation processing level (position/time checks, multisensory position consistency, and RAIM/FDE). In the last decade, spoofing has been demonstrated on multiple occasions for academic and research purposes [27] and several references provide an overview of some potential spoofing threats and countermeasures, including mathematical representations [28] (which is focusing on the observable and positioning layer and describing authentication schemes, however synchronization aspects are not explicitly handled) and attack and detection techniques based on current spoofer and receiver capabilities [29]. Investigations aiming at the assessment and design recommendations of a GNSS receiver's signal processing layer are shown in [30] and [31], the latter particularizing the spoofing detection requirements, environments and possible countermeasures to the aviation domain.

Nomenclature and Threat Categorization

This section presents existing nomenclature for interference types, highlighting the pros and cons of that nomenclature in this context. This section then outlines a framework in order to present the range and types of emissions that avionics may experience.

Intentional interference is generally referred to as interference whose purpose is to disrupt signal reception. Jammers such as PPDs may therefore fall into this category. However, such devices are not intentionally intended to interfere with air navigation services. Most effects of PPDs on air navigation services are collateral. Similarly, even though most GNSS repeaters are not placed to intentionally mislead avionics receivers, they represent an integrity threat comparable to some intentional spoofers, if not treated.

The International Telecommunication Union (ITU) Radio Regulations (Vol 1, Art I, Sect VII) [32] define interference as "*The effect of unwanted energy due to one or a combination of emissions, radiations, or inductions upon reception in a radiocommunication system, manifested by any performance degradation, misinterpretation, or loss of information which could be extracted in the absence of such unwanted energy*". This definition relates interference to the *effect* in the receiver, as opposed to the source or the intention. ITU classifies interference as *permissible, accepted* or *harmful*, where harmful interference is defined as *"Interference which endangers the functioning of a radionavigation service or of other safety services or seriously degrades, obstructs, or repeatedly interrupts a radiocommunication service operating in accordance with Radio Regulations"*. While the ITU definition does not explicitly mention *jamming* or *spoofing*, both are implicitly considered within the definition of interference, in the terms *"performance degradation"*, *"loss of information"*, and "*misinterpretation"*.

The proposed top-level types of harmful interference threats in this paper are *Jamming* and *Spoofing*, where:

- *Jamming* denotes emissions that do not mimic GNSS signals, but rather interfere with the receiver's ability to acquire and track GNSS signals.
- *Spoofing* denotes emissions of GNSS-like signals that may be acquired and tracked in combination with or instead of the intended signals.

This top-level categorization is irrespective of the intention of the emitter. Purely unintentional interference (e.g., an improperly installed GNSS repeater or mis-operated test equipment), collateral

interference (e.g., a PPD) or dedicated, malicious interference (e.g., a dedicated aircraft spoofer), are therefore all considered categories of Jamming and Spoofing. According to this definition, devices generating GNSS-like signals with PRN codes [3], sometimes referred to as *smart jammers*, will, despite their name, be considered as spoofing. Therefore, jamming threats generally lead to a *denial of service* and only affect continuity and availability, while spoofing threats can lead to an *integrity failure* if the spoofing signals are treated as valid GNSS signals and therefore spoofing threats are generally considered more dangerous. Nevertheless, since signal correlation and measurement generation processes are internal to the receiver, it cannot be *a priori* discarded that jamming threats can lead to incorrect or highly inaccurate propagated measurements in current receivers with integrity impacts as well. For example, the current SBAS MOPS mentions that "*Excessive CW interference could cause large pseudorange errors*" and proposes to treat interference in order to fulfil the requirement of *Integrity in the Presence of Interference*, S2.1.1.12, [8]. Similar requirements will be needed for the newly considered threats and one of the objectives of this framework is that future standards should address jamming threats in order to preclude possible integrity failures.

Jamming
J1 - Collateral Jammers
J2 - High Power Interferers
J3 - Targeted Jammers
J4 - Targeted Sophisticated Jammers

Spoofing
S1 – Repeaters
S2 – Errant signals
S3 - Collateral Spoofers – Simulators
S4 - Collateral Re-radiating Spoofers
S5 - Targeted Spoofers – Simulators
S6 - Targeted Re-radiating Spoofers
S7 - Targeted Sophisticated Spoofers

Table 1 – New Categorization of Interference Types, Jamming (J1-J4) and Spoofing (S1-S7)

Table 1 presents a proposed means for interference categorization. It is intended to foster dialogue on the kinds of unwanted emissions that are possible and the effects on the receivers that need to be mitigated in the future standards. As mentioned above, the categorization addresses emissions from jammers and spoofers; however, different types of emissions can result in similar effects. For example, radiofrequency systems whose accidental emissions lead to jamming are assimilated into the J2 - *high-power interferers* category term which is also used in reference [9].

The term *collateral* is used when the aircraft is not the intended victim of the emission. However, this intent is not necessarily observable by the receiver. What is observable is that the position, code chip phase, power levels, etc. of the false signals, are unlikely to be aligned with the corresponding values for the true signals at the user antenna. Therefore, large positioning and pseudorange jumps can be expected as well as power levels that are either too weak or too strong.

The term *targeted* is used when the emissions are intended to specifically affect one or more aircraft. In this case, some effort has been made to align the interfering signals so that errors may not be as obvious at the receiver. The term *sophisticated* is used when the interfering signals are in their hardest-to-detect conditions, for example when multiple signals may be arriving from different directions.

The categories also take into account the anticipated effect in the receiver, the receiver response to the emission, and the general type of equipment required for the transmission. For example, while

S1- Repeaters and S3 - Collateral Spoofers–Simulators might trigger a similar detection response, they are considered in separate sub-categories, since the likelihood of encountering repeaters signals currently appears to be higher than the likelihood of encountering spoofers. Threats composed of a combination of threat categories will be categorized according to the most potentially harmful in the list (from J1 to S7), e.g. a targeted jamming (J3) + targeted spoofer re-radiation attack (S6) would be considered under S6, unless the resources and complexity required moves it into the category of *sophisticated* (S7).

There are many other properties that can be used to model different threats within each category (e.g., whether or not an emitter is on board the aircraft or external). The properties used were selected to provide a separation that reflects both the likelihood and vulnerability considering some previously investigated mitigations. This top-level separation can be revisited as the likelihood of various threats and their potential mitigations matures.

What follows is a definition of each of the threats including some illustrative examples from the literature and reported events, when available.

Jamming Categories

- **J1 - Collateral Jammers:** Jammers emitting signals that do not contain GNSS-specific features (see general threat categories provided above), often with low power and limited range. These sources may have the purpose of jamming GNSS devices other than the avionics receiver. Examples of collateral jammers include mobile satellite services (MSS) handsets and mobile or static, single- or multi-frequency PPDs used by individuals for privacy purposes, such as described in references [11], [13] or [10]. These devices can be on board the aircraft.

- **J2 - High Power Interference:** Misused military or civil transmitters or mis-operated test equipment which results in jamming over a broad area including regions with very high signal power. This definition is based on a definition by the FAA [9] that is extended to cover civil transmissions such as harmonics from FM or TV signals. For example, high power 3rd order harmonics of 525 MHz UHF TV signals in the L1 band [4] [33] are included in this category.

- **J3 - Targeted Jammers:** Jammers, e.g., those described in J1 or similar, when specifically operated against the aircraft. It includes the case where their power level remains sufficient to obscure the true signals for an extended period of time but perhaps not so high as to otherwise be easily detected. These jammers do not transmit GNSS-specific features, and are built, or procured, with limited resources; i.e., equipment and know-how is within reach through the internet at a low cost (~1000 USD).

- **J4 - Targeted Sophisticated Jammers:** Sophisticated jammers beyond the capabilities of J3, which include dedicated features to defeat existing jamming detectors or radio interference monitors. This category includes, for example, highly directive jammers such as *jamming guns* [23], or selective, intermittent jammers resulting in selective bit corruption or increased low power noise.

Spoofing Categories

- **S1 – Repeaters:** Devices rebroadcasting live GNSS signals from a fixed, or mobile position, typically used to improve indoor or in-vehicle coverage. For example, a misplaced or

misconfigured Galileo/GPS/GNSS repeater used for receiver signal acquisition within an airport hangar, whose signals leak out and spoof nearby aircraft receivers [34].

- **S2 - Errant Signals:** A GNSS-like synthetic signal that is mistakenly taken for an operational GNSS signal. This category includes testing platforms transmitting signals which may mislead avionics receivers. For example, satellite-based test-beds [35], or ground-based test-beds [36] [37], if misconfigured, or misused, and transmit operational PRNs, would fall into this category. This category also includes pseudolites [38], generally intended to improve GNSS coverage and performance. Errant signals also includes PRN-like signal jammers that can be acquired and tracked by receivers resulting in false measurements [39].

- **S3 - Collateral Spoofers - Simulators:** Spoofers that transmit synthetically-generated, GNSS-like signals such as those discussed in reference [20] (case *A. Simplistic Attack.)*, or more recently, in reference [40]. The aim is of these spoofers is to deceive other receivers, such as personal location devices, smartphones, or automotive receivers, or all receivers within a certain area [22]. Their purpose is not intended to specifically deceive an avionics receiver. Therefore, while their transmitted signals may be self-coherent, they would not be coherent with the dynamics and signals tracked by the aircraft. This category includes spoofers that introduce incorrect or invalid digital data and possibly erroneous ranging used in processing signals and the calculation of PNT. Data spoofing can result in a range of effects, from incorrect outputs of PNT to receiver malfunction. Onset of data spoofing effects can be instantaneous or delayed, and effects can persist long after the spoofing attack has ended. False signals are unlikely to be aligned with the true signals and typically would lead to large, ranging/position jumps as well as power mismatches.

- **S4 - Collateral Re-radiating Spoofers:** Spoofers that transmit GNSS-like signals based on real time reception of actual GNSS signals. This includes the re-radiation of the full signal stream, selective re-radiation of GNSS signals with potentially different delays, receiver-spoofers ([20], B. *Intermediate Attack*), re-radiators of signals based on features from actual GNSS signals, including authenticated signals [41], or any combinations of the above. Their purpose is not to specifically deceive an avionics receiver. Therefore, this category's transmitted signals may be self-coherent, but would not be coherent with the dynamics and signals tracked by the aircraft and could result in loss of situational awareness. These signals would typically lead to large, ranging/position jumps as well as power mismatches.

- **S5 - Targeted Spoofers - Simulators:** Spoofers similar to S3, whose purpose is intended to deceive the avionics receiver. Therefore, their transmitted signals must be self-coherent and are intended to cohere with the dynamics and signals tracked by the aircraft, with potential technical limitations in the attack. They may initially have well matched ranging/positioning errors and may be preceded with jamming in order to unlock the receiver from the true signals. This category includes spoofers that introduce incorrect or invalid digital data and possibly erroneous ranging targeting the avionics receiver for its use in processing signals and the calculation of PNT. Data spoofing can result in a range of effects, from incorrect outputs of PNT to receiver malfunction. Onset of data spoofing effects can be instantaneous or delayed, and effects can persist long after the spoofing attack has ended. This category is limited to spoofers using a single transmitter that is built or procured with limited resources; i.e., equipment and know-how within reach through the internet at low cost (~1000 USD). These spoofers cannot estimate the aircraft position below a few-meter level accuracy.

- **S6 - Targeted Re-radiating Spoofers:** Spoofers similar to S4, but whose intended purpose is to deceive the avionics receiver. Therefore, their transmitted signals must be self-coherent, and intended to cohere with the dynamics and signals tracked by the aircraft, provided the technical limitations of the attack. They may initially have well matched ranging/positioning errors and may be preceded with jamming in order to unlock the receiver from the true signals. This category is limited to spoofers using a single receiver-transmitter, built or procured with limited resources; i.e., equipment and know-how within reach through the internet at low cost (~1000 USD). These spoofers cannot estimate the aircraft position below a few-meter level accuracy. Multiple targeted re-radiators that are not coherent with the dynamics and signals tracked by the aircraft can result in erroneous positioning and denial of positioning/navigation services.

- **S7 - Targeted Sophisticated Spoofers:** Spoofers whose target is the avionics receiver with a higher degree of sophistication than S5 and S6. They may be even carrier phase-aligned at the victim receiver's reception point, enabling the cancellation of the nominal signal (if the nominal signal is predictable). They include most coordinated multiple spoofing transmitter attacks, combined ground-based and air-based attacks, high accuracy aircraft location tracking, and attacks including combinations of the abovementioned threats requiring significant resources, etc.

Although the framework may be useful for multiple purposes, it is intended as a tool for the development of user receiver requirements. The reader is reminded that GNSS is not intended as a single means of aircraft navigation, but a source of information for the pilot/aircraft, among others, including other navigation systems and visual aids to navigation. Therefore, even in case of successful sophisticated GNSS spoofing that is not mitigated in the GNSS receiver, its effects can be mitigated by the pilot under most circumstances, making the threat potentially less effective, at the current time, than other non-GNSS related threats, which are out of scope of this document.

Assets to Protect, Use Case and Assumptions

According to the ICAO standard, the main function of GNSS as a radionavigation aid is that it "*shall provide position and time data to the aircraft*" ([7], 3.7.2.1.1). These position and time data are based on the GNSS signals providing GNSS measurements and data. As this framework relates to interference threats, receiver tampering threats were considered out of scope. Therefore, the assets to protect are the GNSS signals received by the receiver, including their carrier frequency and modulated spreading codes and data bits from which the measurements and data are extracted.

Concerning the type of operations supported, ICAO Annex 10 [7] Vol 1, Table 3.7.2.4-1 lists signal-in-space performance requirements for different operations. CAT-I precision approach is the most demanding operation listed in that table, particularly for the integrity requirement. The primary objective of this framework is to maintain integrity, CAT-I precision approach is the focus for this threat analysis. The CAT-I requirements as listed in ICAO Annex 10 [7], Vol 1, Table 3.7.2.4-1 are recalled in Table 2.

Accuracy horizontal 95%	Accuracy vertical 95%	Integrity	Time-to-alert	Continuity	Availability
16.0 m (52 ft)	6.0 m to 4.0 m (20 ft to 13 ft)	$1 - 2 \times 10^{-7}$ in any approach	6 s	$1 - 8 \times 10^{-6}$ per 15 s	0.99 to 0.99999

Table 2 – CAT-I requirements [7]

Additional guidance is provided in Annex 10 for system requirements to support operations with a 200 ft DA/H. Annex 10 also contains requirements to support lower than CAT-I minima operations. These requirements supplement those in Table 2. Most notably, additional requirements at the pseudorange level are imposed, including for integrity.

A relevant assumption for assessing the detection/mitigation measures, particularly of spoofing threats, is the initial state of the receiver. It is assumed in the use case, that the receiver is tracking valid signals and providing a valid PVT at the start of the precision approach. This assumption is also used in other spoofing mitigation references [29] [41] and is considered appropriate here, given the demanding conditions required for taking control of the signals in the previous phases of flight and maintaining control without the receiver detecting and rejecting those signals. It is also considered that the outcome of the threat analysis for the CAT-I use case is generally applicable for other phases of flight, except when noted. Surface operations can be also subject to jamming/spoofing with a similar likelihood. In these cases, the interference may be easier to detect at an airport, due to the presence of multiple aircraft that might detect the interference and especially if appropriate airport monitoring controls are deployed. These measures may protect start-up and acquisition processes, when a receiver may be most vulnerable to spoofing. However, the assumption that capabilities are available to detect jamming/spoofing threats is not valid for many start-up locations.

While the focus of this paper is on CAT-I approach, the countermeasures are also applicable for other phases of flight or procedures (en-route, terminal, or other approach procedures demanding a lower GNSS performance). The countermeasures identified are generally applicable to an aircraft receiving valid GNSS signals, irrespective of the aircraft's phase of flight; however, CAT-I and its integrity requirements was used as the assumed baseline.

While the assumptions here presented are considered representative for this initial analysis, they will be validated in the process of modelling the threats and defining testing procedures for future standards.

Threat Treatment and Detection/Mitigation Responses

The treatment of the interference categories could be identified as: *mandatory*, *recommended*, *future*, or *not applicable*. The following definitions are offered to motivate discussion of the receiver minimum outputs and capabilities:

- **Mandatory**: Threat to be treated in the next set of avionics receiver standards.
- **Recommended**: Treatment of the threat in the next set of avionics standards is recommended but not mandatory and may be addressed at the aircraft level or by other means within the aircraft.

- **Future**: Possible treatment of the threat in future avionics standards.

The assignment of the treatment is expected to be a collaborative community effort, first focusing on the foreseen or desirable allocation of mitigation responsibility to the receiver.

The avionics are only one part of the air vehicle or platform-level system. In addition to the GNSS antenna, other aircraft components may have essential roles in determining the navigation and guidance solution used by the pilot or autopilot. The response of the avionics, the integrated air vehicle, and aircrew will ultimately determine the robustness against, or vulnerability to, the unwanted emissions. Planned responses need to consider real-time and maintenance actions. The following range of detection responses is envisaged:

- **None:** No action taken.
- **Record:** Record pertinent data about the event for later downloading and analysis.
- **Report:** Transmit information about the event to ATC and or airline maintenance for potential subsequent action.
- **Alert (Advise/Caution):** Provide information to dependent aircraft systems and/or the pilot that anomalies have been detected and the position may not be reliable.
- **Deny:** A valid GNSS solution is no longer provided. Relay information to other aircraft systems and/or the pilot that an alternate navigation source must be used.
- **Mitigate:** Prevent the anomaly from affecting the integrity of the GNSS solution; continue to operate using GNSS.

Treatment actions related to detection (Record, Report, Advise/Caution and Deny) and Mitigate can be combined in the threat treatment. Recommendations on specific avionics, aircraft and pilot responses are beyond the scope of this paper.

Countermeasures

This section explores some possible detection and mitigation measures against the abovementioned threats. These potential mitigations are based on jamming and spoofing protections defined in the literature (e.g., reference [29] presents a similar exercise, but not particularized for the aviation use case and receivers) and on specific spoofing/ jamming mitigation techniques developed or assessed by the FAA for aviation use. This paper complements the countermeasures proposed in [31] with additional references and some traceability to the threat categories they can mitigate. Figure 1 presents a list of potential countermeasures, grouped in blocks according to the applicable part of the receiver, or avionics, addressed, including the antenna, front end, signal processing (including all processes between ADC and tracking loop outputs), navigation (including measurement-level and PVT-level computations), platform (including all additional blocks that can be embedded in the receiver), and "other", to include countermeasures added at the operational procedures level, in the Flight Management Systems (FMS), or based on alternative navigation systems, which are not the focus of this work. Note that some of these techniques, or particular implementations may be covered by patents. The analysis of the intellectual property rights (IPR) status of the proposed techniques is beyond the scope of this paper. It should be noted that severe restrictions are imposed on inclusion of techniques covered by IPRs in avionics standards.

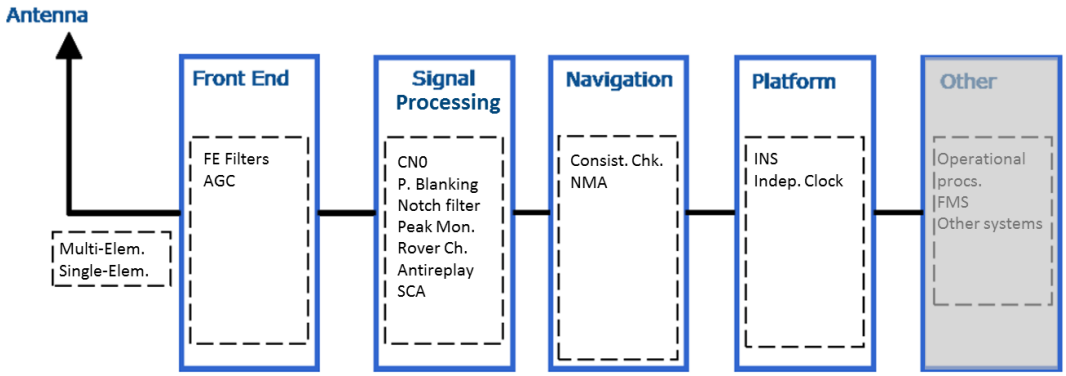

Figure 1 – Countermeasures

What follows is a brief description of each countermeasure:

- **Multi-Element Antennas**: Measures based on multi-element antennas. This countermeasure includes CRPA null techniques to null the direction of arrival of the jamming/spoofing source(s) [42] and other multi-element antenna techniques against jamming/spoofing as shown in [25] [43] [44]. They are effective against most interference threats. Their implementation complexity is a priori high and in principle most potential options are out of scope for initial next-generation equipment due to cost and export restrictions.

- **Single-Element Antennas**: Measures based on single-element LHCP/RHCP antennas [45] [46] or related to elevation masking to limit/prevent emissions from low or below-zero elevation sources [47]. Elevation measures, while useful in some cases, may not be sufficient for threats to surface operations, takeoff, or jamming/spoofing emissions from middle elevations (e.g., hilltops or buildings). Masking applied above the typical elevation mask can degrade performance due to the reduction in number of available satellites.

- **AGC&C/N_0**: AGC [48] and C/N_0 are complementary countermeasures and are proposed to be used in combination [49]. They are available within the receiver so the implementation complexity is low. AGC&C/N_0 are useful for detecting all threats, particularly jamming (J1, J2, J3) and non-targeted, non-sophisticated spoofing (especially S1). AGC&C/N_0 monitoring detects abnormal power emissions and is also effective in combination with other measures (e.g., peak monitoring and rover channels) for other types of spoofing, including targeted and sophisticated spoofing (S3-S7). These techniques may also be effective to detect S2 unless errant signals are received at similar power levels as GNSS signals.

- **Filtering**: Filtering at the receiver RF front end (RFFE) and signal processing are grouped together in this countermeasure category. Filtering includes analog or digital filters such as stopband filters to filter signals in the adjacent bands (J2) or notch filters [13] for CW/swept tones of jammers (J1, J3). Filter implementation complexity can be medium or high, depending on the filtering scheme and the receiver design.

- **Pulse Blanking:** Includes measures to mitigate pulsed interference (J2), such as those already used for DME/TACAN pulse mitigation in the L5 band [50]. Pulse blanking can be implemented at a low/medium complexity.

  Peak Monitoring and Control Loop Parametrization: Includes protection measures based e.g. on the use of several correlators to detect peak forms that may suggest targeted spoofing tracking loop liftoff attacks (S5, S6, S7), as e.g., described in reference [29] as *Correlation function distortion monitoring* or reference [49]. Peak monitoring requires additional correlators per channel compared to standard correlator implementations. Implementation complexity is considered medium/high, depending on the availability of correlators. Simultaneous tracking of the nominal and spoofing peak (for overlapping peaks) is shown in [51]. Regarding control loop parametrization to force spoofers to synchronize with the authentic signals, an investigation aimed at evaluating robust configurations (i.e. requiring a higher level of synchronization of the spoofer in terms of frequency offset and time delay) of the receiver loops can be found in [30].

- **Rover Channels:** Includes protection measures based on a continuous acquisition process to detect correlation peaks around the tracking peak from spoofing signals or vestigial signals, if already under influence of spoofing [52] [19]. Rover channels can prove very useful to detect all kinds of spoofing (S1-S7), and particularly targeted spoofing (S5, S6, S7). Maximum benefits are provided by continuous acquisition and tracking. Implementation complexity is considered medium/high.

- **Spreading Code Authentication:** Includes spreading code authentication in GNSS ARNS signals, receiver sample storage and cryptographic functions (first presented in reference [19], as Spread Spectrum Security Codes, or SSSC). This mitigation is useful against spoofing, especially against simulated signals (S2, S3, S5). Spreading code authentication is not foreseen to be added in the near-term by GNSS providers in the ARNS bands.

- **Consistency Checks:** Includes all types of GNSS consistency checks at the Measurement, Position, Velocity, Time and Frequency level. It is considered very effective to detect and sometimes mitigate non-targeted spoofing (S1-S4) at a low complexity (software-level modification). Consistency checks include:
  - Measurement consistency over time; e.g., pseudorange jumps based on a step detector, as already addressed in the MOPS ([8], 2.1.1.5.1). Consistency checks can detect abrupt measurement jumps from non-targeted spoofing and errant signals (S1, S2, S3, S4).
  - RAIM/FDE, including consistency checks of measurements at a given position fix and the detection of faulty, inconsistent measurements. The measure can be effective against unintended (S1, S2) and collateral spoofing (S3, S4), particularly in transitional times when the receiver tracks a majority of valid signals and a minority of spoofing signals.
  - Position and Velocity checks over time, including abnormal position, sudden jumps due to tracking repeater signals (S1), a static or slow-moving position reported (S1, S3, S4), or any changes not consistent with the aircraft dynamic model.
  - Time and Frequency checks over time, including time jumps in disagreement with the expected receiver clock oscillator stability (e.g., S3, S5), or abnormal clock frequency drifts induced by a spoofer delaying the signal stream (S6, time-based meaconing attacks) [29]. Mitigations can also include time comparisons between trusted time

sources (obtained, e.g., at startup in a controlled environment, and later time measurements e.g., before start of an approach).
    - Navigation data checks, including checking that the SBAS, IODC/IODE or other data are within valid ranges, and there are no abnormal values, or data sequencing overtime, avoiding incorrect PNT outputs or receiver malfunction [53]. Navigation data checks may help preclude S2 (if errant signals have abnormal data) or S3-S5 (simulators).
    - Aircraft level checks using independent measurements (e.g., cross-checks with IRU and other navigation sensors and timing sources).

- **Navigation Message Authentication (NMA)**: This countermeasure will be included in the Galileo Open Service [54] [55] and is also under study for GPS [56] [57] and SBAS [58] [59]. NMA ensures navigation data authenticity by cryptographic authentication through digital signatures or equivalent protocols. This mitigation would require a software-level implementation for the cryptographic operations and a mechanism for receipt and storage of a public key in the receiver. Cryptographic information can be updated generally over the air and sporadically through other means. Medium implementation complexity (software level). Requires cryptographic protocol and management of the public keys. NMA is effective in detecting all simulated signals (S2, S3, S5) in isolation and re-radiators (S1, S4, S6) when combined with signal replay detection and consistency checks. If lightweight cryptographic protocols such as TESLA [60] are used, detection may require loose time synchronization obtained from a time consistency check. The authentication verification requires additional time which depends on the format of the message.

- **Signal Replay Detection:** Requires unpredictable signals using NMA or spreading code authentication (SCA) and dedicated signal processing, including partial signal accumulation and later verification upon reception of the cryptographic information [41]. Effectiveness depends on the signal used, in particular, the amount and periodicity of unpredictable codes, and whether the detection capability is implemented at code, or symbol level, since code-based features of SCA are more difficult to replay than symbol-based features of NMA. This capability also depends on the implementation of receiver anti-replay checks [61]. Receiver complexity is medium/high depending on the technique employed. Useful against re-radiators and sophisticated spoofing (S4, S6, S7). In the case of NMA, vulnerabilities of the channel coding may be exploited [62] if the unpredictable symbols are not properly chosen [63].

- **Inertial Measurement Units (IMUs):** Useful for detection of all jamming and spoofing threats (J1-S7) where the GNSS and IMU information is inconsistent. Can also provide mitigation by coasting on the IMU position while the GNSS signals are unavailable or declared/suspected to be under threat. An IMU may, or may not, be integrated in the GNSS receiver. The IMU may, or may not, rely on the GNSS for initialization and bias estimation. Some benefits may be achievable with a less than traditional navigation grade IMU. An aviation anti-spoofing approach based on IMUs is described in [64].

- **Independent Clock Reference:** This is a generic category that includes countermeasures based on additional clock-related hardware and therefore excludes the timing consistency checks addressed above. Application of this mitigation capability may require the use of a more stable, independent oscillator (e.g., a chip scale atomic clock (CSAC) or real-time clock (RTC) for loose time synchronization).

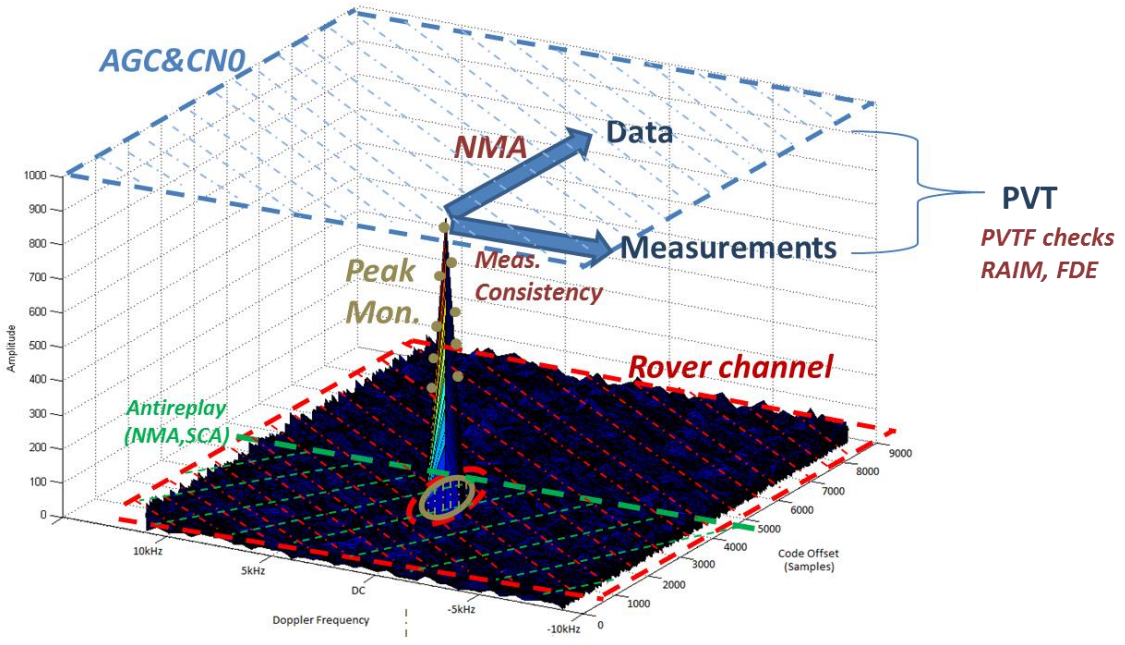

Figure 2 – Conceptual figure of jamming/spoofing countermeasures, including AGC&C/N0, rover channel, peak monitoring, anti-replay, NMA, and consistency checks at measurement / PVTF level

Figure 2 represents the proposed countermeasures in relation to the processing of a GNSS signal, and the generation of the measurements and data for the PVT computation. The AGC & C/N_0 defends from threats raising the interference power level by detecting, for example, high-power spoofing pushing vestigial signals at the post-correlation stage below the noise floor. The rover channel can defend the surroundings of the valid signal peak in both frequency and time and prevent spoofing attacks whereby a spoofing signal approaches and crosses the tracking loop to take control over the loop. Peak monitoring protects the tracking peak by detecting abnormal peak shapes from a spoofer that are roughly synchronized at the code level with the valid signals. In addition, anti-replay measures (requiring signal/data authentication and unpredictable signal features) force spoofers to estimate and replay the signal, adding a delay to a spoofed signal, or abnormal patterns on the unpredictable parts of the signal. Beyond the signal processing domain, NMA ensures that the data that is demodulated is authentic and provides signal unpredictability features that can be used against replay attacks. Note that an attacker might roughly synchronize the threat signal with the valid one, force a cycle slip and take control of the PLL and modify the data, if not authenticated. Inconsistency of the measurements can be detected through measurement consistency checks, and position, velocity, time and frequency (PVTF) consistency over time can be checked as well. The figure does not include desirable platform-level measures, such as consistency checks with IMU/INS, other independent sensors, or external clocks.

Multipath, which also includes GNSS-like signals, has not been included explicitly for the scope of this work as, while it can affect the position, it cannot be considered as a jamming/spoofing threat. It will always be a delayed version of the nominal PRN sequence received from the satellite. The received power is always lower. The satellite signals impinge from different directions. Therefore

multipath signals will affect the PRNs differently and are therefore not self-coherent. Modeling approaches for airborne multipath are discussed in [65] or [66], and proposed countermeasures must be able to discern between multipath and spoofing signals in order to avoid false alerts.

Combinations of Countermeasures

Out of the above countermeasures, some combinations seem particularly effective to mitigate many of the identified threats, yet simple to implement. The following is a first iteration toward defining a group of countermeasures that could be implemented considering their expected complexity and potential effectiveness. Once the threat model is defined in more detail, the effectiveness of these combinations must be re-verified. Any of the following combinations can have a higher degree of robustness by the addition of independent navigation (e.g., INS) or timing (independent clock) measures. From lowest to highest complexity, some possible combinations are:

1. **AGC&C/N_0 with consistency checks:** This combination can detect various non-targeted threats (J1, J2, J3 through AGC&C/N_0, and S1, S3, S4 through consistency checks, although these checks may prove insufficient against targeted spoofing (S5-S7) and some S2 cases (e.g., an errant SBAS-like signal used as a data channel only).

2. **AGC&C/N_0 with consistency checks and NMA**: With the addition of NMA, this combination can protect against all the threats in combination 1, plus guarantees the source of the data in all cases and the signal sources, in all instances except re-radiation. This measure adds protection capability against all S2 and S5 threats in addition to those in combination 1.

3. **AGC&C/N_0 with consistency checks, roving channel, and peak monitoring/control loop parametrization**: In addition to the threats protected in combination 1 (J1, J2, J3, S1, S3, S4), these techniques may provide improved protection against targeted attacks (S5, S6, S7), provided these attacks do not align with the valid signal at the code level and modify the data. Otherwise peak monitoring techniques may detect signals which are not fully aligned.

4. **AGC&C/N_0 with consistency checks, roving channel, peak monitoring/control loop parametrization, NMA, and anti-replay**: In addition to combination 3, NMA prevents the possibility of data modification (which may be the simplest targeted attack for signal-protected receivers). And, the anti-replay feature protects against most anti-replay attacks (except potentially highly sophisticated targeted spoofing attacks under S7).

In addition, IMUs [64], or other independent positioning sources and independent accurate time references, will improve the detection and mitigation capabilities of all of the above combinations.

Summary

A framework for categorizing emissions is described to enable discussion and to support the development of future aviation standards with protections against jamming and spoofing. This framework divides the emissions into 11 categories, 4 for jamming and 7 for spoofing, based upon a broad view of such interference, including collateral and targeted threats from different types of equipment and sophistication. A CAT-I approach is assumed as a use case to assess the possible countermeasure effectiveness. Protections for CAT-I operation are considered likely valid for other flight phases as well. A fairly exhaustive set of countermeasures is proposed based upon both the generic and aviation-specific work that was available on jamming and spoofing mitigation

measures, including measures at all stages of the avionics receiver (antenna, RFFE, signal processing, navigation, platform). Based on the effectiveness and easiness of implementation, countermeasures are grouped in four combinations, from AGC & C/N_0 and consistency checks alone, to AGC & C/N_0, consistency checks, authentication and signal processing measures (rover channel, peak monitoring, anti-replay). All of the combinations can be supported by the use of IMUs and independent clocks.

Acknowledgements
The work presented here was performed in coordination with the Resilience Sub-Group of the U.S.-/EU Working Group on the Design of Next Generation GNSS (WG-C).

Bibliography

[1] J. J. Spilker and F. D. Natali, "Interference Effects and Mitigation Techniques," in *Global Positioning System, Theory and Applications. Vol. I*, AIAA, 1996, pp. 717-771.

[2] John A Centre. Volpe National Transportation Systems, "Vulnerability Assessment of the Transportatopm Infrastructure Relying on the Global Positioning System," U.S. DoT, 2001.

[3] P. W. Ward, J. W. Betz and C. Hegarty, "GNSS Disruptions," in *Understanding GPS/GNSS Principles and Applications - Kaplan, Hegarty (eds) - Third Edition*, Artech House, 2017, pp. 549-617.

[4] T. Humphreys, "Interference," in *Handbook of Global Navigation Satellite Systems (P. Teunissen, O. Montenbruck, eds.)*, Springer, 2017, pp. 469-504.

[5] F. Dovis (Ed.), GNSS Interference Threats and Countermeasures, Artech House, 2015.

[6] G. H. Hagn, "Definitions of electromagnetic noise and interference.," in *IEEE International Symposium In Electromagnetic Compatibility*, 1977.

[7] International Civil Aviation Organization, "International Standards and Recommended Practices - Annex 10 - Aeronautical Telecommunications - Vol 1 - Radio Navigation Aids - Sixth Edition - No. 91," ICAO publications, 2018.

[8] RTCA SC-159, "Minimum Operational Performance Standards for Global Positioning System - Wide Area augmentation System Airborne Equipment - DO229E," 2016.

[9] K. Alexander and D. Lawrence, *GNSS Intentional Interference and Spoofing (presentation to RTCA)*, 2015.

[10] D. Borio, J. Fortuny and C. O'Driscoll, "Spectral and spatial characterization of GNSS jammers," in *Proc. 7th GNSS Vulnerabilities Solutions Conf. (pp. 1-17)*, Baska, Croatia , 2013, April.

[11] R. H. Mitch, R. C. Dougherty, M. L. Psiaki, S. P. Powell, B. W. O'Hanlon, J. A. Bhatti and T. E. Humphreys, "Signal characteristics of civil GPS jammers.," in *Proceedings of ION GNSS (Vol. 2011, pp. 20-23)*, 2011.

[12] E. Axell, F. M. Eklöf, P. Johansson, M. Alexandersson and D. M. Akos, "Jamming detection in GNSS receivers: Performance evaluation of field trials," *Navigation*, vol. 62, no. (1), pp. 73-82, 2015.

[13] D. Borio, C. O'Driscoll and J. Fortuny, "GNSS jammers: Effects and countermeasures," in *European Workshop on Satellite Navigation Technologies (NAVITEC)*, December 2012.

[14] FAA Navigation Team, "GPS Privacy Jammers and RFI at Newark Navigation Team AJP-652 Results," 2011.

[15] S. Lee, M. Dumville, M. Pattinson, T. Sarang, Z. Bhuiyan, Gabrielsson and V. Manikundalam, "Standardization of GNSS Threat reporting and Receiver testing through International Knowledge Exchange, Experimentation and Exploitation (STRIKE3)," in *한국통신학회 학술대회논문집*, 2017.

[16] A. Konovaltsev, S. Caizzone, K. Yinusa, M. Sgammini, E. P. Marcos, M. Appel, M. Cuntz, W. Elmarissi and M. Meurer, "Interference Detection and Characterization with an Array based GNSS Receiver using Conformal Antennas in Maritime Environments," in *Proceedings of the 30th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2017)*, Portland, 2017.

[17] C. Hegarty, A. Van-Dierendonck, D. Bobyn, M. Tran, T. Kim and J. Grabowski, "Suppression of Pulsed Interference through Blanking," in *Proceedings of the IAIN World Congress and the 56th Annual Meeting of The Institute of Navigation (2000), pp. 399-408.*, San Diego, CA, June 2000.

[18] J. Grabowski and C. Hegarty, "Characterization of L5 Receiver Performance Using Digital Pulse Blanking," in *Proceedings of the ION GPS*, 2002.

[19] L. Scott, "Anti-Spoofing & Authenticated Signal Architectures for Civil Navigation Systems," *ION GPS*, 2003.

[20] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon and P. M. Kintner Jr, "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in *Proceedings of the ION GNSS international technical meeting of the satellite division (Vol. 55, p. 56)*, 2008.

[21] Forbes, "Hacking A Phone's GPS May Have Just Got Easier," 7 AUG 2015. [Online]. Available: https://www.forbes.com/sites/parmyolson/2015/08/07/gps-spoofing-hackers-defcon/#17baab494efb.

[22] InsideGNSS, "Reports of Mass GPS Spoofing Attack in the Black Sea Strengthen Calls for PNT Backup," 24 July 2017. [Online]. Available: http://www.insidegnss.com/node/5555. [Accessed 23 8 2017].

[23] Russia Beyond, "Russia Beyond," 29 Aug 2017. [Online]. Available: https://www.rbth.com/defence/2017/08/29/down-with-the-drones-new-russian-weapon-to-combat-flying-machines_830114. [Accessed 15 Sep 2017].

[24] M. Appel, A. Hornbostel and C. Haettich, "Impact of Meaconing and Spoofing on Galileo Receiver Performance," in *7th ESA Workshop on Satellite Navigation Technologies NAVITEC*, 2014.

[25] M. Appel, A. Iliopoulos, F. Fohlmeister, E. P. Marcos, M. Cuntz, A. Konovaltsev, M. Meurer and F. Antreich, "Experimental Validation of GNSS Repeater Detection Based on Antenna Arrays for Maritime Applications," *CEAS Space Journal*, 2018.

[26] M. Cuntz, A. Konovaltsev and M. Meurer, "Concepts, Development, and Validation of Multiantenna GNSS Receivers for Resilient Navigation," *Proceedings of the IEEE*, vol. 104, pp. 1288-1301, 6 2016.

[27] T. Humphreys, "UAVs Vulnerable to Civil GPS Spoofing," *Inside GNSS*, 2012.

[28] C. Günther, "A Survey of Spoofing and Counter-Measures," *NAVIGATION, Journal of The Institute of Navigation*, vol. 61, no. 3, Fall 2014, pp. 159-177., 2014.

[29] M. L. Psiaki and T. E. Humphreys, "GNSS Spoofing and Detection," *Proceedings of the IEEE* , vol. 104, no. 6, 2016.

[30] T. Bamberg, M. Appel and M. Meurer, "Which GNSS tracking loop configuration is most robust against spoofing?," in *ION GNSS+ 2018*, 2018.

[31] C. Hegarty, A. Odeh, K. Shallberg, K. Wesson, T. Water and K. Alexander, "Spoofing Detection for Airborne GNSS Equipment," in *Proceedings of the ION GNSS+ 2018*, Miami, FL, 2018.

[32] International Telecommunication Union, "Radio Regulations Articles - Volume 1," ITU, 2016.

[33] R. Johannessen, S. J. Gale and M. J. A. Asbury, "Potential interference sources to GPS and solutions appropriate for applications to civil aviation," *IEEE Aerospace and Electronic Systems Magazine*, vol. 5(1), pp. 3-9, 1990.

[34] E. Steindl, W. Dunkel, A. Hornbostel, C. Hättich and P. Remi, "The impact of interference caused by GPS Repeaters on GNSS receivers and services," in *European Navigation Conference. ENC GNSS 2013*, Vienna, 2013.

[35] "Satellite Based Augmentation System test-bed project," [Online]. Available: http://www.ga.gov.au/scientific-topics/positioning-navigation/positioning-for-the-future/satellite-based-augmentation-system. [Accessed 23 Aug 2017].

[36] "GATE Testbed," [Online]. Available: http://www.gate-testbed.com/en/gate-overview.html. [Accessed 28 Aug 2017].

[37] "Automotive GATE," [Online]. Available: http://www.automotivegate.de. [Accessed 23 Aug 2017].

[38] C. O'Driscoll, D. Borio and J. Fortuny, "Scoping study on pseudolites -Technical Report JRC64608," Joint Research Centre, Ispra, IT, 2011.

[39] D. Lu, R. Wu, P. Li and Z. Su, "GPS smart jammer suppressin algorithm based on spatial APES," in *International Symposium on Intelligent Signal Processing and Communication Systems, 2007. ISPACS.* , 2007.

[40] L. Huang and Q. Yang, "GPS Spoofing - Low Cost GPS simulator," DEF CON 23, Las Vegas, 2015.

[41] T. Humphreys, "Detection Strategy for Cryptographic GNSS Anti-Spoofing," in *IEEE Transactions on Aerospace and Electronic Systems* , 2013.

[42] Y. H. Chen, S. Lo, D. M. Akos, D. S. De Lorenzo and P. Enge, "Validation of a controlled reception pattern antenna (CRPA) receiver built from inexpensive general-purpose elements during several live-jamming test campaigns.," in *Proceedings of the 2013 International Technical Meeting of The Institute of Navigation*, San Diego, California (pp. 154-163)., 2013.

[43] M. Appel, A. Konovaltsev and M. Meurer, "Robust Spoofing Detection and Mitigation based on Direction of Arrival Estimation," in *Proceedings of the 28th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2015)*, Tampa, 2015.

[44] M. Appel, A. Iliopoulos, F. Fohlmeister, E. P. Marcos, M. Cuntz, A. Konovaltsev, F. Antreich and M. Meurer, "Interference and Multipath Suppression with Space Time Adaptive Beamforming for Safety-of-Life Maritime Applications," *CEAS Space Journal*, 2017.

[45] E. McMilin, "Single Antenna Null-Steering for GPS & GNSS Aerial Applications," Ph.D. Dissertation, Stanford University, 2016.

[46] Y.-H. Chen, F. Rothmaier, D. Akos, S. Lo and P. Enge, "Towards a Practical Single Element Null Steering Antenna," in *Proceedings of the Institute of Navigation International Technical Meeting, January 2017*, Monterrey, CA.

[47] E. McMilin, D. S. De Lorenzo, T. Lee and P. Enge, "GPS Anti-Jam: A Simple Method of Single Antenna Null-Steering for Aerial Applications," in *Proceedings of the ION 2015 Pacific PNT Meeting*, Honolulu, Hawaii, 2015.

[48] D. M. Akos, "GPS/GNSS spoofing detection via automatic gain control (AGC)," *Navigation*, no. 59(4), pp. 281-290, 2012.

[49] P. Enge, T. Walter and K. Shallberg, *Detection of GPS Spoofing - for Working Group 2 of RTCA Special Committee 159 (presentation)*, 2017.

[50] G. X. Gao, L. Heng, A. Hornbostel, H. Denks, M. Meurer, T. Walter and P. Enge, "DME/TACAN interference mitigation for GNSS: algorithms and flight test results," *GPS Solutions*, vol. 17(4), pp. 561-573., 2013.

[51] A. Iliopoulos, C. Enneking, T. Jost, O. G. Crespillo, M. Appel and F. Antreich, "Robust Ranging in the Presence of Repeater Signals," in *ION GNSS+ 2017*, 2017.

[52] D. A. Anderson, "Advanced spoofer mitigation and geolocation through spoofer tracking". U.S. Patent US7764224B1, 2006.

[53] Dept. of Homeland Security, NCCIC, NCC, "Improving the Operation and Development of Global Positioning System (GPS) Equipement Used by Critical Infrastructure," January, 2017.

[54] European Commission , *COMMISSION IMPLEMENTING DECISION (EU) 2017/224 of 8 February 2017 (CS Implemeting Act)*, 2017.

[55] I. Fernández-Hernández, V. Rijmen, G. Seco-Granados, J. Simón, I. Rodríguez and J. D. Calle, "A Navigation Message Authentication Proposal for the Galileo Open Service," *NAVIGATION, the Journal of the Institute of Navigation*, 2016.

[56] Anderson, Jon M.; Carroll, Katherine L.; et al., "Chips-Message Robust Authentication (Chimera) for GPS Civilian Signals," in *ION GNSS+*, Portland, OR, 2017.

[57] A. J. Kerns, K. Wesson and T. Humphreys, "A Blueprint for Civil GPS Navigation Message Authentication," in *Proceedings of Position, Location and Navigation Symposium*, Monterey, 2014.

[58] P. Enge and T. Walter, "Digital Message Authentication for SBAS (and APNT)," in *ION GNSS+ 2014*, Tampa, FL, 2014.

[59] I. Fernández-Hernández, E. Châtre, A. D. Chiara, G. D. Broi, O. Pozzobon, J. Fidalgo, M. Odriozola, G. Moreno, S. Sturaro, G. Caparra, N. Laurenti and V. Rijmen, "Impact Analysis of SBAS Authentication," *NAVIGATION, Journal of the Institute of Navigation, Volume 65, Number 4*, vol. Vol. 65, no. No. 4, pp. 517-532, 2018.

[60] A. Perrig, R. Canetti, J. D. Tygar and D. Song, "The TESLA Broadcast Authentication Protocol," *CryptoBytes*, 2002.

[61] S. Cancela, J. Navarro, D. Calle, E. Göhler, A. D. Chiara, G. D. Broi, I. Fernández-Hernández, G. Seco-Granados and J. Simon, "Testing receiver resilience against signal replay attacks," in *ITSNT*, Toulouse, 2018.

[62] J. T. Curran and C. O'Driscoll, "Message Authentication, Channel Coding & Anti-Spoong," Porland, 2016.

[63] I. Fernández-Hernández and G. Seco-Granados, "Galileo NMA signal unpredictability and anti-replay protection," in *International Conference on Localization and GNSS (ICL-GNSS)*, 2016.

[64] Ç. Tanıl, S. Khanafseh, M. Joerger and B. Pervan, "An INS Monitor to Detect GNSS Spoofers Capable of Tracking Vehicle Position," *IEEE Transactions on Aerospace and Electronic*

Systems, vol. 54, pp. 131-143, 2 2018.

[65] M.-S. Circiu, S. Caizzone, M. Felux, C. Enneking and M. Meurer, "Improved airborne multipath modelling," in *ION GNSS+ 2018*, 2018.

[66] D. Gerbeth, M.-S. Circiu, M. Caamano and M. Felux, "Nominal Performance of Future Dual Frequency Dual Constellation GBAS," *International Journal of Aerospace Engineering*, pp. 1-20, 6 2016.