ETSO-C145e
Date: 21.2.2018

European Aviation Safety Agency

European Technical Standard Order

Subject: AIRBORNE NAVIGATION SENSORS USING THE GLOBAL POSITIONING SYSTEM AUGMENTED BY THE SATELLITE BASED AUGMENTATION SYSTEM

1 - Applicability

This ETSO provides the requirements which airborne navigation sensors using the Global Positioning System (GPS) augmented by the Satellite-Based Augmentation System (SBAS) that are designed and manufactured on or after the date of this ETSO must meet in order to be identified with the applicable ETSO marking.
The standards of this ETSO apply to equipment intended to provide position information to a navigation management unit that outputs deviation commands referenced to a desired flight path. Pilots or autopilots will use these deviations to guide the aircraft.

2 - Procedures

2.1 - General

Applicable procedures are detailed in CS-ETSO, Subpart A.

2.2 - Specific

None.

3 - Technical conditions

3.1 - Basic

3.1.1 - Minimum performance standard

Standards set forth for functional equipment Class Beta in RTCA document DO-229E, Minimum Operational Performance Standards for Global Positioning System/Satellite-Based Augmentation System Airborne Equipment, dated December 15, 2016, Section 2, as modified by Appendix 2 and 4 of this ETSO.
Class Beta equipment is defined in DO-229E, Section 1.4.
The standards in this ETSO apply to equipment intended to provide position, velocity, and time information for a navigation management unit application that outputs deviation commands keyed to a desired flight path, or a non-navigation application such as an automatic dependent surveillance-broadcast (ADS-B) or terrain awareness and warning system (TAWS). In navigation applications, pilots or autopilots will use the deviations output by the navigation management unit to guide the aircraft. In non-navigation applications, the position, velocity, and time outputs will provide the necessary inputs for the end-use equipment. These ETSO standards do not address integration issues with other avionics.

3.1.2 - Environmental standard

See CS-ETSO, Subpart A, paragraph 2.1.
The required performance under test conditions is defined in RTCA document DO-229E, Minimum

Operational Performance Standards for Global Positioning System/Satellite-Based Augmentation System Airborne Equipment, dated December 15, 2016, Section 2.4.

3.1.3 - Software

See CS-ETSO, Subpart A, paragraph 2.2.

3.1.4 - Airborne electronic hardware

See CS-ETSO, Subpart A, paragraph 2.3.

3.2 - Specific

3.2.1 - Failure condition classification

See CS-ETSO, Subpart A, paragraph 2.4.
Failure of the function defined in paragraph 3.1.1 of this ETSO is a:

— *Major* failure condition for loss of function and malfunction of en route, terminal, approach lateral navigation (LNAV), and approach LNAV/vertical navigation (VNAV) position data,
— *Major* failure condition for loss of function of approach localiser performance without vertical guidance (LP), and approach localiser performance with vertical guidance (LPV) position data, and
— *Hazardous* failure condition for malfunction of approach (LP and LPV) position data resulting in misleading information.

3.2.2 - Additional Specific

If the equipment can satisfy the requirements of RTCA/DO-229E only when used with a particular antenna, the use of that antenna (by part number) shall be a requirement on the installation.
This requirement shall be included in the installation manual (IM) as a limitation.

The applicant shall have all the data necessary to evaluate the geostationary (GEO) satellite bias as defined in RTCA/DO-229E, Section 2.1.4.1.5 available for review by EASA.

If the equipment uses barometric-aiding to enhance FDE availability, then the equipment shall meet the requirements in RTCA/DO-229E, Appendix G.

3.3. - Functional qualifications.

None.

4 - Marking

4.1 - General

Marking as detailed in CS-ETSO, Subpart A, paragraph 1.2.

4.2 - Specific

At least one major component must be permanently and legibly marked with the operational equipment class as defined in Section 1.4.2 of RTCA document DO-229E (e.g., Class 2). A marking of Class 4 indicates compliance to Delta-4 requirements. The functional equipment class defined in Section 1.4.1 of RTCA document DO-229E (e.g. Gamma, Delta) is not required to be marked.
It is sufficient to declare the proper functional equipment class in the DDP (declaration of design and performance).

5 - Availability of referenced document

See CS-ETSO, Subpart A, paragraph 3.

APPENDIX 1

Reserved.

APPENDIX 2
ADDITION TO RTCA/DO-229E SECTION 1.

This Appendix adds a new Section 1.8.3, on cybersecurity and GPS spoofing mitigation to RTCA/DO-229E. The new section provides information for cybersecurity and spoofing mitigation to make RTCA/DO-229E consistent with the new RTCA MOPS template and RTCA/DO-253D, Minimum Operational Performance Standards for GPS Local Area Augmentation System Airborne Equipment.

1.8.3 Cybersecurity and Spoofing Mitigation.

This section contains information to address intentional interference with the GPS. Spoofing is caused by RF waveforms that mimic true signals in some ways, but deny, degrade, disrupt, or deceive a receiver's operation when they are processed. Spoofing may be unintentional, such as effects from the signals of a GPS repeater, or may be intentional and even malicious. There are two classes of spoofing:

— Measurement spoofing introduces RF waveforms that cause the target receiver to produce incorrect measurements of time of arrival or frequency of arrival or their rates of change;
— Data spoofing introduces incorrect digital data to the target receiver for its use in processing of signals and the calculation of PNT.

Either class of spoofing can cause a range of effects, from incorrect outputs of PNT to receiver malfunction. The onset of effects can be instantaneous or delayed, and the effects can continue even after the spoofing has ended. Improperly used or installed GNSS re-radiators act like spoofers. Re-radiators replay and GNSS emulator devices can present misleading information to GNSS equipment and/or could cause lasting effects.

Equipment manufacturers should implement measures to mitigate processing of erroneous data. Cross-checks of GNSS sensor data against independent position sources and/or other detection monitors using GNSS signal metrics or data checks can be implemented in the antenna, receiver, and/or through integration with other systems at the aircraft level. Data validity checks to recognize and reject measurement and data spoofing should be implemented in the receiver. Additional guidance and best practices related to GPS equipment can be found in the U.S. Department of Homeland Security document 'Improving the Operation and Development of Global Positioning System (GPS) Equipment Used by Critical Infrastructure'[1] and GLOBAL POSITIONING SYSTEMS DIRECTORATE SYSTEMS ENGINEERING & INTEGRATION: INTERFACE SPECIFICATION, IS-GPS-200, Navstar GPS Space Segment/Navigation User Interfaces, Revision H, IRN-IS-200H-003, 28 July 2016.

Aircraft equipment information vulnerabilities (such as cybersecurity risks) have been present for digital systems since the development of the personal computer (PC) in the late 70's and even longer for RF systems, and the advent of internet connectivity has substantially increased those risks. Typically, access to navigation receivers has been controlled such that they are considered vulnerable only through RF signals and OEM and/or aircraft operator controlled processes for maintenance and update. In some cases, aircraft GNSS receivers may be field-loadable by approved personnel, requiring physical access and physical interface to the ground receivers. However, it is expected that not all aircraft in the future will rely on such physical isolation for the security of avionics. Internet and Wi-Fi connectivity have become popular as a means for aircraft or equipment manufacturers to update installed avionics software, to update databases, or provide an alternate means of communicating with the flight crew or cabin (e.g., in-flight entertainment, weather, etc.).

In most countries, the State provides oversight of safety-of-flight systems (sometimes referred to as 'authorised services') which provide information to aircraft, such as ILS, VOR, GNSS, and DME, to name a few. However, the State typically does not provide oversight on 'non-trusted' connectivity such as the internet, Wi-

[1] https://ics-cert.us-cert.gov/sites/default/files/documents/Improving_the_Operation_and_Development_of_Global_Positioning_System_(GPS)_Equipment_Used_by_Critical_Infrastructure_S508C.pdf .

Fi, or manufacturer-supplied equipment interfaces which permit input of externally-supplied data into aircraft systems. A manufacturer may expose aircraft information vulnerability through equipment design, or become vulnerable as a result of being connected to a common interface. Therefore, it is important that manufacturers consider aircraft information security risk mitigation strategies in their equipment design, particularly when the equipment is responsible for an interface between the aircraft and aircraft-external systems.

Apart from any specific aircraft-information-security-related performance requirements that are contained in the MOPS, it is recommended that manufacturers look at a layered approach to aircraft information security risk mitigation that includes both technical (e.g., software, signal filtering) and physical strategies. From a technical perspective, for example, this could include signal spoofing detection capabilities or more stringent, multi-factored authentication techniques such as passwords, PINs, and digital certificates. From a physical perspective, a manufacturer could consider connectors that require special tools to remove them to prevent passenger tampering; although navigation avionics are typically located in an avionics bay inaccessible to passengers. And finally, but just as important, manufacturers should consider supply chain risk management; for example, if a manufacturer is outsourcing software code development, are the contractor and its staff properly vetted?

Civil Aviation Authorities (CAAs) have a regulatory interest when an applicant's design makes use of a non-trusted connectivity where the installation can potentially introduce aircraft information security vulnerability. This requires the applicant to address not only the information security vulnerabilities and mitigation techniques for the new installation, but to also consider how vulnerability could propagate to existing downstream systems. Therefore, it is recommended that manufacturers reference their equipment aircraft information security review and mitigation strategies in the equipment's installation manual so that the applicant can consider them in meeting the installation regulatory requirements.

APPENDIX 3

Reserved.

APPENDIX 4

This Appendix prescribes EASA modifications to RTCA document DO-229E, Section 2.

In Section 2.1.1.2, after the first sentence add:

> 'The demodulation of data from the GPS signals shall be restricted to the necessary subset of the data defined in Appendix II of IS-GPS-200D, "Navstar GPS Space Segment / Navigation User Interfaces", December 2004, provided on RF link L1. The pseudo-ranging shall be performed on RF link L1 utilizing the coarse/acquisition (C/A) code.'

This is to ensure that only the L1 NAV data, for which the SBAS provides corrections and integrity, is used, and that no CNAV data, which is defined in Appendix III of IS-GPS-200D, is used, for which the SBAS does not provide integrity.