ETSO-C146e

Date: 21.2.2018

European Aviation Safety Agency

European Technical Standard Order

Subject: STAND-ALONE AIRBORNE NAVIGATION EQUIPMENT USING THE GLOBAL POSITIONING SYSTEM AUGMENTED BY THE SATELLITE BASED AUGMENTATION SYSTEM

1 - Applicability

This ETSO provides the requirements which stand-alone airborne navigation equipment using the Global Positioning System (GPS) augmented by the Satellite-Based Augmentation System 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.

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 Gamma or Delta 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, except as modified by Appendix 2 and 4 of this ETSO.

Classes Gamma and Delta of equipment are defined in DO-229E, Section 1.4.

The standards in this ETSO apply to equipment intended to accept a desired flight path and provide deviation commands keyed to that path. Pilots and autopilots will use these deviations to guide the aircraft. Except for automatic dependent surveillance with Class Gamma, 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.

Applicants shall have all the data necessary to evaluate the geo stationary (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 shall 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 with 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.

ETSO-C146e
Date: 21.2.2018

APPENDIX 1

Reserved.

APPENDIX 2

MPS for stand-alone airborne navigation equipment using GPS augmented by SBAS

This Appendix describes required modifications and additions to RTCA/DO-229E for compliance with this ETSO. This Appendix adds a new Section 1.8.3 on cybersecurity and GPS spoofing mitigation and additional required leg types in Section 2.2.1.3 to RTCA/DO-229E.

The new Section, 1.8.3, contains no new requirements but 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.

The new 2.2.1.3 leg type requirements are applicable to Class Gamma equipment only and are necessary to properly execute published instrument procedures designed to provide maximum efficiency, flexibility, and aircraft eligibility. These instrument procedure designs may include RNAV components and/or leg types associated with conventional procedures. The modifications and additions to Section 2.2.1.3 are necessary to ensure Class Gamma equipment can properly execute current and future instrument procedure designs.

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'[2] 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

[2] 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

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-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, is 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.

2.2.1.3 Path Definition

Replace the list of required leg types in the first paragraph after the last sentence as shown:

The desired path shall be defined according to the following leg types:

Leg Type	Description
IF	Initial Fix
CF	Course to Fix leg
DF	Direct to Fix leg
TF	Track to Fix leg
FA	Fix to Altitude leg
FM	Fix to Manual Termination
VA	Heading to Altitude leg
VI	Heading to Intercept
VM	Heading to Manual Termination
CA	Course to Altitude Leg

Holding legs

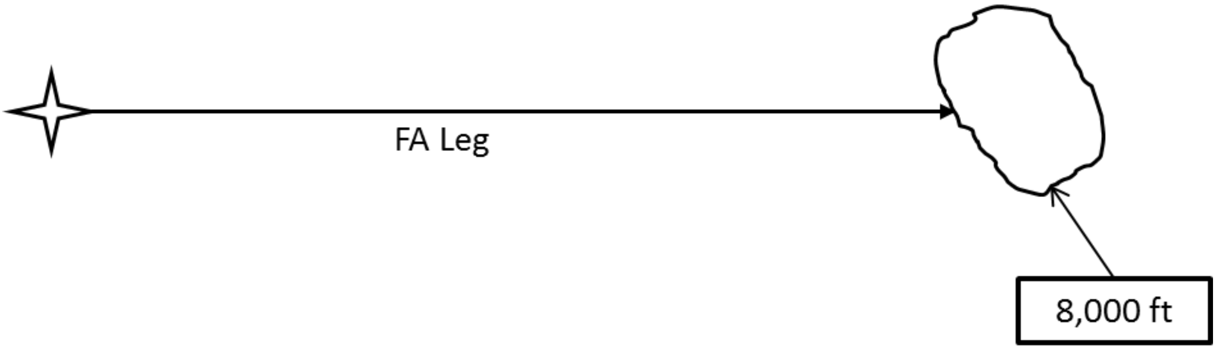
Leg Type	Description
HA	Terminates at an altitude
HF	Terminates at a fix after one orbit
HM	Manual termination

Note: There is no intent to require a heading or altitude source connected to the equipment to automatically execute leg types with heading or altitude components. Manual equipment inputs for heading/altitude with manual aircraft control methods are acceptable for these leg types.

Replace Section 2.2.1.3.6 as shown and add the following leg type descriptions. Re-number existing paragraphs (starting with 2.2.1.3.7) to account for the newly added sections:

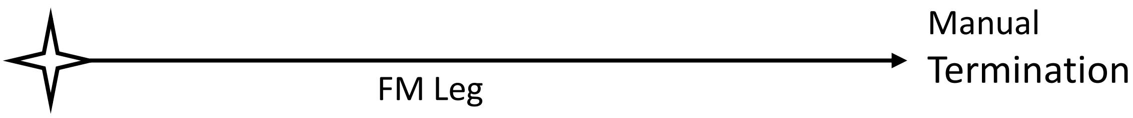
2.2.1.3.6 Fix to Altitude (FA).

An FA leg shall be defined as a specified track over the ground from a database waypoint to a specified altitude at an unspecified position.



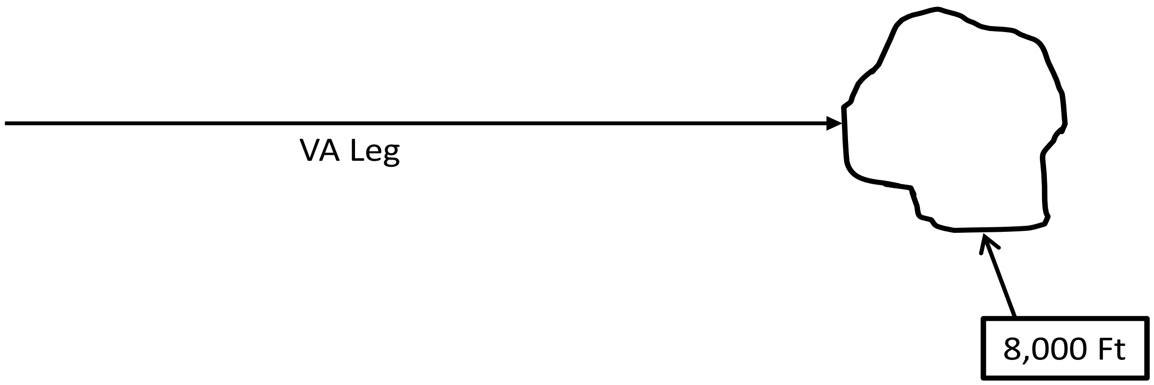
2.2.1.3.7 Fix to Manual Termination (FM).

An FM leg shall be defined as a specified track over the ground from a database fix until a manual termination of the leg.



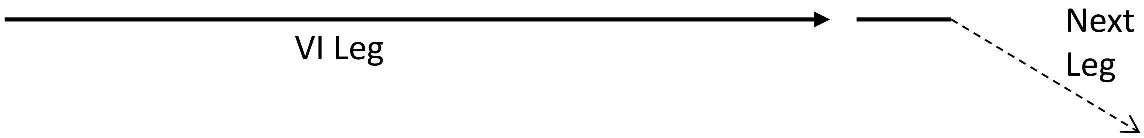
2.2.1.3.8 Heading to Altitude (VA).

A VA leg shall be defined as a specified heading to a specific altitude termination at an unspecified position. No correction is made for wind.



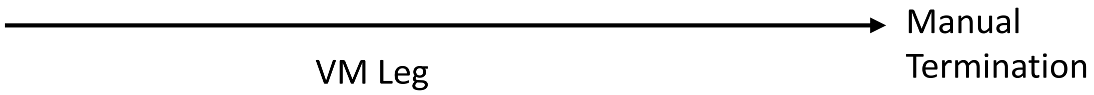
2.2.1.3.9 Heading to Intercept (VI).

A VI leg shall be defined as a specified heading to intercept a subsequent leg at an unspecified position. No correction is made for wind.



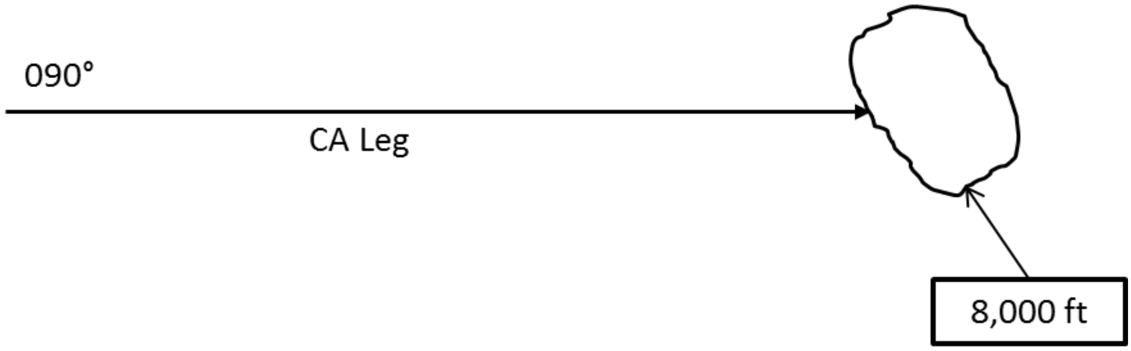
2.2.1.3.10 Heading to Manual Termination (VM).

A VM leg shall be defined as a specified heading until a manual termination of the leg. No correction is made for wind.



2.2.1.3.12 Course to Altitude (CA).

A CA leg shall be defined as a specified course to a specific altitude at an unspecified position. The course is flown making adjustment for wind.



2.2.1.3.13 Hold to Altitude (HA).

An HA leg is a holding pattern which terminates at the next crossing of the hold fix when the aircraft altitude is at or above the specified altitude. The altitude is provided by the navigation database. The source of the magnetic variation needed to convert magnetic courses to true courses is detailed in Section 2.2.1.3.12.

2.2.1.3.14 Hold to Fix (HF).

An HF leg is a holding pattern which terminates at the first crossing of the hold fix after becoming established on the inbound course. This is typically after the entry procedure is performed. The source of the magnetic variation needed to convert magnetic courses to true courses is detailed in Section 2.2.1.3.12.

2.2.1.3.14 Hold for Clearance (manual termination) (HM).

An HM leg is a holding pattern which terminates only after flight crew action. The source of the magnetic variation needed to convert magnetic courses to true courses is detailed in Section 2.2.1.3.12.

Table 2-14 through Table 2-20.

The tables incorrectly reference and label RTCA/DO-160 Sections 16.5.1.2 and 16.6.1.2 regarding ’2.1.1.7 Acquisition Time’ and ’2.1.1.9 Reacquisition Time.’ Change the table references as follows:
The MOPS Initial Acquisition Time requirement (2.1.1.7) applies to both AC and DC equipment under abnormal operating conditions (DO-160E Sections 16.5.2 and 16.6.2) and the Satellite Reacquisition Time requirement (2.1.1.9) applies to both AC and DC equipment under normal operating conditions (DO-160E Sections 16.5.1 and 16.6.1).

APPENDIX 3

Reserved.

APPENDIX 4

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

At 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 no CNAV data, which is defined in Appendix III of IS-GPS-200D, is used, for which the SBAS does not provide integrity.