This project has received funding from the European Union's Horizon Europe Programme

SHEPHERD

EASA.2022.C05

D2.2-D3.2

Identification of satisfactory industry standards and justification for not acceptable industry standards (Part 2)

Disclaimer

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Union Aviation Safety Agency (EASA). Neither the European Union nor EASA can be held responsible for them.

DELIVERABLE NUMBER AND TITLE:	D2.2-D3.2 Identification of satisfactory industry standards and justification for not acceptable industry standards (Part 2)
CONTRACT NUMBER:	EASA.2022.C05
CONTRACTOR / AUTHOR:	SHEPHERD consortium
IPR OWNER:	European Union Aviation Safety Agency
DISTRIBUTION:	Public

APPROVED BY	AUTHOR	REVIEWER	MANAGING DEPARTMENT
Marco Ducci (Project Coordinator)	Alexandra Florin (Wing) Andrei Tudor (ANRA) Damiano Taurino (Deep Blue) Dannick Riteco (Azur Drones) Diego Fernández Varela (Wing) Guido Manfredi (Volocopter) Joerg Dittrich (DLR) Lorenzo Murzilli (Murzilli Consulting) Marco Ducci (Deep Blue) Maxime Heinisch (Azur Drones) Michael Allouche Patricia García Pastor (ANRA) Pawel Trominski (Murzilli Consulting) Ronald Liebsch (Volocopter) Pasquale J. Capasso (EuroUSC Italia) Pranav Nagarajan (DLR) Sebastian Cain (DLR)	Alexandra Florin (Project Technical Lead)	N/A

DATE: 30.04.2024

SUMMARY

This document provides the outcome of the preliminary high-level assessment and subsequent detailed technical assessment conducted in accordance with the criteria and methodology developed by SHEPHERD to evaluate the suitability of the second half of the standards within the scope of the project in fulfilling the relevant requirements.

For each of the standards, it identifies and substantiates the list of recommended sections, subsections, paragraphs, or combination thereof that have been deemed suitable and, hence, may be used as a basis for a means of compliance (MoC) for the requirements or a part thereof. In the same manner, it also lists and provides clear justification for the elements of the standards that have been found not technically adequate and, thus, need to be tailored and/or complemented before being proposed as a MoC.

CONTENTS

Contents

ABBREVIATIONS

ACRONYM	DESCRIPTION
ACAS	Airborne Collision Avoidance System
ACJA	Aerial Connectivity Joint Activity
ADS-B	Automatic Dependent Surveillance – Broadcast
AEH	Airborne Electronic Hardware
AIS	Abbreviated Injury Scale
AMC	Acceptable Means of Compliance
API	Application Programming Interface
ARC	Air Risk Class
ARC	(FAA) Aviation Rulemaking Committee
ASD-STAN	AeroSpace and Defence Industries Association of Europe
ASSURE	Alliance for System Safety of UAS through Research Excellence
ATC	Air Traffic Control
ATS	Air Traffic Service
ATSP	Air Traffic Service Provider
CEN	European Committee for Standardization
CNS	Communications, Navigation & Surveillance
CRM	Crew Resource Management
CIS	Common Information Service
CISP	Common Information Service Provider
COTS	Commercial Off-The-Shelf
ConOps	Concept of Operations
CS	Certification Specification
CU	Command Unit
C2	Command & Control
C2CSP	C2 Communications Service Provider
C3	Command, Control & Communication
DAA	Detect and Avoid
DAL	Development Assurance Level
DAR	Dynamic Airspace Reconfiguration
DOI	Digital Object Identifier
DoS	Denial-of-Service
DSS	Discovery and Synchronization Service
DWC	DAA Well Clear
EASA	European Union Aviation Safety Agency
ED	(EASA) Executive Director
ED-	EUROCAE Document
ETSO	European Technical Standard Order
EU	European Union

ACRONYM	DESCRIPTION
EUROCAE	European Organisation for Civil Aviation Equipment
EUSCG	European UAS Standards Coordination Group
EVLOS	Extended Visual Line Of Sight
FAA	Federal Aviation Administration
ft	Feet
GHz	Gigahertz
GM	Guidance Material
GSMA	Global System for Mobile (Communications) Association
GTOW	Gross Take-Off Weight
GUTMA	Global UTM Association
HIRF	High-Intensity Radiated Field
ID	Identification
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IEL	Indirect Effects of Lightning
IR	Implementing Regulation
ISMS	Information Security Management System
ISO	International Organization for Standardization
J	Joule
JARUS	Joint Authorities for Rulemaking on Unmanned Systems
KE	Kinetic Energy
kg	Kilogram
lb	Pound-mass
LTE	Long-Term Evolution
LUC	Light UAS operator Certificate
MASPS	Minimum Aviation System Performance Standards
MNO	Mobile Network Operator
MoC	Means of Compliance
MOPS	Minimum Operational Performance Standards
MRB	Materials Review Board
MTOM	Maximum Take-Off Mass
NAA	National Aviation Authority
N/A	Not Applicable
OI	Operational Intent
ORA	Operational Risk Assessment
OSED	Operational Services and Environmental Description
OSO	Operational Safety Objective
QA	Quality Assurance
QAM	Quality Assurance Manual
QAP	Quality Assurance Program
QAR	Quality Assurance Record

ACRONYM	DESCRIPTION
RDP	Rolling Development Plan
RF	Radio Frequency
RMJM	Requirements Management and Justification Matrix
RPAS	Remotely Piloted Aircraft System
RPS	Remote Pilot Station
RTA	Run-Time Assurance
RTCA	Radio Technical Commission for Aeronautics
SAIL	Specific Assurance and Integrity Level
SC	Special Condition
SCMP	Software Configuration Management Plan
SDO	Standards Developing Organisation
SDP	Software Development Plan
SDS	Software Design Specification
SECO	Security Officer
SG	Sub-(working)group
SHEPHERD	Standards Evaluation Project supporting European Regulations for Drones
SIL	Safety Integrity Level
SL	Software Level
SLA	Service Level Agreement
SMS	Safety Management System
SORA	Specific Operations Risk Assessment
SOUP	Software Of Unknown Pedigree
SPEC	'Specific' (category)
SQAP	Software Quality Assurance Plan
SRM	Safety Risk Management
SRS	Software Requirement Specification
STM	Surveillance and Tracking Module
sUAS	Small Unmanned Aircraft System
SVP	Software Verification Plan
SW	Software
SWaP	Size, Weight and Power
TCAS	Traffic Alert and Collision Avoidance System
TLOS	Target Level of Safety
TMPR	Tactical Mitigation Performance Requirement
TR	Technical Requirement
TRM	Threat Resolution Module
TSO	Technical Standard Order
UA	Unmanned Aircraft
UAS	Unmanned Aircraft Systems
US	United States (of America)
USSP	U-space Service Provider

ACRONYM	DESCRIPTION
UTM	UAS Traffic Management
VLOS	Visual Line Of Sight
WG	Working Group
WRAN	Wireless Regional Area Network
3GPP	3rd Generation Partnership Project
4D	Four-Dimensional

1. Introduction

This document provides the outcome of the preliminary high-level assessment and subsequent detailed technical assessment conducted in accordance with the criteria and methodology developed by SHEPHERD to evaluate the suitability of more than twenty standards in fulfilling the relevant requirements. The assessed standards, which involve approximately half of the standards within the scope of SHEPHERD, are the following ones:

ID	SDO	Reference	Version	Title
1	ASTM	F1583-95(2019)	2019	*Standard Practice for Communications Procedures – Phonetics*
2	ASTM	F3002-14a	2014	*Standard Specification for Design of the Command and Control System for Small Unmanned Aircraft Systems (sUAS)*
3	ASTM	F3003-14	2014	*Standard Specification for Quality Assurance of a Small Unmanned Aircraft System (sUAS)*
4	ASTM	F3005-14a	2014	*Standard Specification for Batteries for Use in Small Unmanned Aircraft Systems (sUAS)*
5	ASTM	F3178-16	2016	*Operational Risk Assessment of Small Unmanned Aircraft Systems (sUAS)*
6	ASTM	F3201-16	2016	*Standard Practice for Ensuring Dependability of Software Used in Unmanned Aircraft Systems (UAS)*
7	ASTM	F3269-21	2021	*Methods to Safely Bound Behaviour of Aircraft Systems Containing Complex Functions Using Run-Time Assurance*
8	ASTM	F3298-19	2019	*Standard Specification for Design, Construction, and Verification of Lightweight Unmanned Aircraft Systems (UAS)*
9	ASTM	F3364-19	2019	*Standard Practice for Independent Audit Program for Unmanned Aircraft Operators*
10	ASTM	F3365-19	2019	*Standard Practice for Compliance Audits to ASTM Standards on Unmanned Aircraft Systems*
11	ASTM	F3367-21a	2021	*Standard Practice for Simplified Methods for Addressing High-Intensity Radiated Fields (HIRF) and Indirect Effects of Lightning on Aircraft*
12	ASTM	F3389/F3389M-21	2021	*Standard Test Method for Assessing the Safety of Small Unmanned Aircraft Impacts*
13	ASTM	F3548-21	2021	*Standard Specification for UAS Traffic Management (UTM) UAS Service Supplier (USS) Interoperability*

ID	SDO	Reference	Version	Title
14	ASTM	F3600-22	2022	*Standard Guide for Unmanned Aircraft System (UAS) Maintenance Technician Qualification*
15	C3 link spectrum & technology standards mapping			– ASTM F3002-14. *Standard Specification for Design of the Command and Control System for Small Unmanned Aircraft Systems (sUAS)* – ASTM F3298-19. *Standard Specification for Design, Construction, and Verification of Lightweight Unmanned Aircraft Systems (UAS)* – CEN & ASD-STAN prEN 4709-001:2021. *Aerospace series – Unmanned Aircraft Systems – Part 001: Product requirements and verification.* – ISO 21384-2:2021. *Unmanned Aircraft Systems - Part 2: UAS components* – EUROCAE ED-266. *Guidance on Spectrum Access, Use and Management for UAS* – IEEE 802.15.3c-2009 on Bluetooth technology – IEEE 802.11-2020 on WIFI technology (2.4 GHz + 5 GHz Band) – IEEE 802.22-2017 on Wireless regional area network (WRAN)
16	IEC	IEC 62133-2:2017 + AMD1:2021	2021	*Secondary cells and batteries containing alkaline or other non-acid electrolytes – Safety requirements for portable sealed secondary cells, and for batteries made from them, for use in portable applications – Part 2: Lithium systems*
17	ISO	ISO 21384-2:2021	2021	*Unmanned aircraft systems – Part 2: UAS components*
18	ISO	ISO 21384-3:2023	2023	*Unmanned aircraft systems – Part 3: Operational procedures*
19	ISO	ISO 23629-7:2021	2021	*UAS Traffic Management (UTM) Part 7 – Data Model for Spatial Data*
20	RTCA	RTCA DO-366A	2020	*Minimum Operational Performance Standards (MOPS) for Air-to-Air Radar for Traffic Surveillance*
21	RTCA	RTCA DO-386	2020	*Vol I Minimum Operational Performance Standards for Airborne Collision Avoidance System Xu (ACAS Xu)*

For each of the standards above, this document identifies and substantiates the list of recommended sections, subsections, paragraphs, or combination thereof that have been deemed suitable and, hence, may be used as a basis for a means of compliance (MoC) for the relevant requirements or a part thereof. In the same manner, it also lists and provides clear justification for the elements of the standards that have been found not technically adequate and, thus, need to be tailored and/or complemented before being proposed as a MoC.

Additionally, the comparative analysis of IEC 61508 as an alternative to DO-178C, not part of the original scope of SHEPHERD, was presented to and reviewed by EASA in the framework of the project, resulting in its annexation to this final deliverable.

2. Main considerations and assumptions

2.1 General

- The list of standards and associated requirements within the scope of SHEPHERD was built upon the work performed and deliverables published by the AW-Drones project, and aligned with the Unmanned Aircraft Systems (UAS) Rolling Development Plan (U-RDP) of the European UAS Standards Coordination Group (EUSCG).
- The standards already recognised by EASA as suitable standards for the SORA requirements, U-space regulation, and SC Light-UAS through MoC or AMC & GM have not been re-assessed by SHEPHERD and are, therefore, considered out of scope of the project.
- The assessment criteria and work methodology ensuring impartial, systematic, and consistent evaluation of standards developed by SHEPHERD have been rigorously applied.

2.2 Requirements

- The SORA requirements' wording and content are those of SORA v2.5 published by JARUS for external consultation in December 2022.
  NOTE: In a few specific instances, the latest available draft of JARUS SORA v2.5 has been used instead; this is clearly stated and the relevant wording is reflected.
- Both SC Light-UAS medium- & high-risk requirements have been considered.
- As SC Light-UAS provisions are limited to UAS with a MTOM of up to 600 kg, unlike the requirements contained in SORA, which does not provide any mass limitations, some standards have been assessed against both the relevant SC Light-UAS provision(s) and the corresponding SORA requirement(s).
- The AMC & GM to Implementing Regulation (EU) 2021/664, as published by EASA in December 2022, have been considered along with the U-space regulatory requirements.

2.3 Outcome

- For each standard, a list of sections, subsections, paragraphs, or combination thereof that have been deemed suitable to show compliance with each requirement within scope and may be used as a basis of a means of compliance (MoC) is provided.
- Analogously, each section, subsection, or paragraph of the standards deemed not technically suitable to show compliance with the relevant requirements is identified, substantiating the required tailoring and/or complementing required before being proposed as a MoC.

3. Summaries of the standard assessments

3.1 ASTM F1583-95(2019)

3.1.1 Introduction

The objective of this section is to present the outcome of the preliminary high-level assessment and subsequent detailed technical assessment of *ASTM F1583-95(2019). Standard Practice for Communications Procedures – Phonetics* conducted in accordance with the criteria and methodology developed by SHEPHERD to evaluate the standard's suitability in fulfilling the following requirements:

- TMPR VLOS/EVLOS, SAIL II to VI – ARC-b to ARC-d;
- SORA v2.5 OSOs:
  - OSO#16 Integrity Criterion#2, SAIL I to VI – Low (L) to High (H);
- EASA's remote crew training-related requirements:
  - AMC1 UAS.SPEC.050(1)(d) and UAS.SPEC.050(1)(e);
  - AMC2 UAS.SPEC.050(1)(d) and UAS.SPEC.050(1)(e); and
  - AMC3 UAS.SPEC.050(1)(d) and UAS.SPEC.050(1)(e).

It identifies and substantiates the list of recommended sections, subsections, paragraphs, or combination thereof of ASTM F1583-95(2019) that have been deemed suitable and, hence, may be used as a basis for a means of compliance (MoC) for the requirements or a part thereof. In the same manner, it also lists and provides clear justification for the elements of the standard that have been found not technically adequate and, thus, need to be tailored and/or complemented before being proposed as a MoC.

3.1.2 General remarks

ASTM F1583-95(2019) provides phonetic communication procedures. It mainly focuses on how to transmit a written or voice message, including a phonetic alphabet, numerals, and punctuation in speech and print.

This standard does not address the following requirements:

- OSO#16 Assurance Criterion#2;
- AMC2 UAS.SPEC.050(1)(d) and UAS.SPEC.050(1)(e); and
- AMC3 UAS.SPEC.050(1)(d) and UAS.SPEC.050(1)(e).

For further details on the rationale for the sections that have been considered as 'N/A' being too high-level requirements or similar to the requirements, as well as the rationale for the recommended sections, refer to the detailed technical assessment.

Sections 3, 4 and 5 of ASTM F1583-95(2019) were analysed against the following requirements:

- TMPR VLOS / EVLOS;
- OSO#16 Integrity Criterion#2; and
- AMC1 UAS.SPEC.050(1)(d) and UAS.SPEC.050(1)(e).

The result of the assessment was that these sections are not recommended because the coverage of the requirements is too low; they only provide phonetics principles.

3.1.3 Recommended sections

This subsection provides the list of recommended sections, subsections, paragraphs, or combination thereof of ASTM F1583-95(2019) that may be used as a basis for a MoC for the requirements or a part thereof as identified in the detailed technical assessment.

ASTM F1583-95(2019)			
Requirement	**Related SAIL Integrity / assurance**	**Recommended section(s), subsection(s), paragraph(s), or combination thereof**	**Additional relevant information**
N/A			

3.1.4 Non-recommended sections

This subsection provides the list of elements of ASTM F1583-95(2019) that need to be tailored and/or complemented before being proposed as a MoC for the requirements or a part thereof as identified in the detailed technical assessment.

ASTM F1583-95(2019)			
Section, subsection, or paragraph to be tailored / complemented	**Title / subject**	**Requirement and SAIL**	**Required tailoring / complementing**
See below			

TMPR VLOS / EVLOS

- Deconfliction scheme, phraseology adopted during UAS operations (normal, contingency, emergency situations), means adopted, and latencies are not covered.

OSO#16 Integrity Criterion#2

- Multi-crew coordination training is not fully covered; only phonetics principles are provided. Moreover, CRM is not addressed.

AMC1

- The theoretical training required by AMC1 is not covered; only phonetics principles are provided.

3.2 ASTM F3002-14a

3.2.1 Introduction

The objective of this section is to present the outcome of the preliminary high-level assessment and subsequent detailed technical assessment of *ASTM F3002-14a. Standard Specification for Design of the Command and Control System for Small Unmanned Aircraft Systems (sUAS)* conducted in accordance with the criteria and methodology developed by SHEPHERD to evaluate the standard's suitability in fulfilling the following requirements:

- SORA v2.5 OSOs:
  - OSO#06 Integrity & Assurance, SAIL II to VI – Low (L) to High (H); and
  - OSOs#08+ Integrity & Assurance, SAIL I to VI – Low (L) to High (H).

- EASA SC Light-UAS – Medium & High Risk provisions:
  - Light-UAS.2300;
  - Light-UAS.2575; and
  - Light-UAS.2600.

It identifies and substantiates the list of recommended sections, subsections, paragraphs, or combination thereof of ASTM F3002-14a that have been deemed suitable and, hence, may be used as a basis for a means of compliance (MoC) for the requirements or a part thereof. In the same manner, it also lists and provides clear justification for the elements of the standard that have been found not technically adequate and, thus, need to be tailored and/or complemented before being proposed as a MoC.

3.2.2 General remarks

ASTM F3002-14 does not address the following requirements:

- OSOs#08+, as it only addresses design requirements;
- Light-UAS.2300; and
- Light-UAS.2575(b).

For further details on the rationale for the sections that have been considered as 'N/A' being too high-level requirements or similar to the requirements, as well as the rationale for the recommended sections, refer to the detailed technical assessment.

NOTE: OSO#06 was assessed separately in a C3 link spectrum & technology standards mapping.

Additionally, F3002-14:

- does not include the 'communication' piece of C3 and only focuses on C2 (command & control);

- is limited to UA <25 kg (55 lbs). There is, however, no technical limitation to 55 lbs and each NAA could individually specify the weight limit;

- could potentially be useful as a technical standard for identifying what information needs to be available at the CU and what capabilities need to be on the UA and the CU (e.g. SC Light-UAS.2602 to Light-UAS.2615, Light-UAS.2700 to Light-UAS.2730, etc.). The standard was, however, not assessed against these requirements, as not recommended by AW-Drones; and

- is not as useful as a standard for the CU integration design documentation (i.e. SC Light-UAS.2600).

3.2.3 Recommended sections

This subsection provides the list of recommended sections, subsections, paragraphs, or combination thereof of ASTM F3002-14a that may be used as a basis for a MoC for the requirements or a part thereof as identified in the detailed technical assessment.

ASTM F3002-14a			
Requirement	**Related SAIL Integrity / assurance**	**Recommended section(s), subsection(s), paragraph(s), or combination thereof**	**Additional relevant information**
Light-UAS.2575(a)	SAIL III to VI (Medium & High risk)	10.1 10.2 10.4	While these individual subsections provide only partial coverage of the requirement, their combination is deemed to provide full coverage.
Light-UAS.2600	SAIL III to VI (Medium & High risk)	5	This section provides only partial coverage of the requirement, addressing it on a high level; the standalone utility of this section is deemed low.

3.2.4 Non-recommended sections

This subsection provides the list of elements of ASTM F3002-14a that need to be tailored and/or complemented before being proposed as a MoC for the requirements or a part thereof as identified in the detailed technical assessment.

ASTM F3002-14a			
Section, subsection, or paragraph to be tailored / complemented	**Title / subject**	**Requirement and SAIL**	**Required tailoring / complementing**
N/A			

3.3 ASTM F3003-14

3.3.1 Introduction

The objective of this section is to present the outcome of the preliminary high-level assessment and subsequent detailed technical assessment of *ASTM F3003-14. Standard Specification for Quality Assurance of a Small Unmanned Aircraft System (sUAS)* conducted in accordance with the criteria and methodology developed by SHEPHERD to evaluate the standard's suitability in fulfilling the following requirements:

- SORA v2.5 OSOs:
  - OSO#02 Integrity & Assurance, SAIL III to VI – Medium (M) & High (H).
- EASA SC Light-UAS – Medium & High Risk provisions:
  - Light-UAS.2300.

It identifies and substantiates the list of recommended sections, subsections, paragraphs, or combination thereof of ASTM F3003-14 that have been deemed suitable and, hence, may be used as a basis for a means of compliance (MoC) for the requirements or a part thereof. In the same manner, it also lists and provides clear justification for the elements of the standard that have been found not technically adequate and, thus, need to be tailored and/or complemented before being proposed as a MoC.

3.3.2 General remarks

ASTM F3003-14 establishes the quality assurance requirements for the design, manufacture, and production of small unmanned aircraft systems (sUAS).

This standard does not address the following requirements:

- OSO#02 Integrity; and
- Light-UAS.2300.

ASTM F2909-19 is a useful standard but should not be used in the current version as a standalone AMC for the assessed requirements. It does not cover:

- training of personnel for inspection and/or maintenance;
- maintenance items to be covered; and
- record-keeping of personnel qualifications and authorisations;

While ASTM F3003-14 has been withdrawn by ASTM, WK82742 is anticipated to incorporate some of its key elements into a New Practice to support UAS manufacturers in obtaining Production Approval in concert with Type Certification for UAS.

For further details on the rationale for the sections that have been considered as 'N/A' being too high-level requirements or similar to the requirements, as well as the rationale for the recommended sections, refer to the detailed technical assessment.

3.3.3 Recommended sections

This subsection provides the list of recommended sections, subsections, paragraphs, or combination thereof of ASTM F3003-14 that may be used as a basis for a MoC for the requirements or a part thereof as identified in the detailed technical assessment.

ASTM F3003-14			
Requirement	**Related SAIL Integrity / assurance**	**Recommended section(s), subsection(s), paragraph(s), or combination thereof**	**Additional relevant information**
OSO#02	Assurance SAIL III & IV – Low (L) & Medium (M)	5 (except 5.6) 6 7 8 9	– Quality Assurance Program (QAP) developed in accordance with this standard assures the verification of the declared manufacturing- and design-related in-service occurrence reporting procedures. Moreover, the Quality Assurance Manual (QAM) and Quality Assurance Record (QAR) provide evidence that the UAS has been manufactured in conformance with its design. – Subsection 5.6 is deemed disproportionate for Low (SAIL III) and Medium (SAIL IV) levels of robustness because audits are not required for these levels of robustness. – The combination of the recommended sections is deemed to provide full coverage.

3.3.4 Non-recommended sections

This subsection provides the list of elements of ASTM F3003-14 that need to be tailored and/or complemented before being proposed as a MoC for the requirements or a part thereof as identified in the detailed technical assessment.

ASTM F3003-14			
Section, subsection, or paragraph to be tailored / complemented	**Title / subject**	**Requirement and SAIL**	**Required tailoring / complementing**
5	Quality Assurance Program (QAP)	OSO#02 Assurance SAIL V & VI – High (H)	Programs/procedures related to process/product audits should be provided.
6	Engineering and Manufacture	OSO#02 Assurance SAIL V & VI – High (H)	Process and/or product audits related to engineering and manufacture should be addressed.
7	QA Inspections	OSO#02 Assurance SAIL V & VI – High (H)	How to perform process audits for Quality Assurance (QA) and Materials Review Board (MRB) inspections should be addressed.
8	Production Acceptance	OSO#02 Assurance SAIL V & VI – High (H)	Process audits for production acceptance should be addressed.
9	Assignment of QA Duties and Responsibilities	OSO#02 Assurance SAIL V & VI – High (H)	Duties and responsibilities of process/product audit personnel should be addressed.

3.4 ASTM F3005-14a

3.4.1 Introduction

The objective of this section is to present the outcome of the preliminary high-level assessment and subsequent detailed technical assessment of *ASTM F3005-14a. Standard Specification for Batteries for Use in Small Unmanned Aircraft Systems (sUAS)* conducted in accordance with the criteria and methodology developed by SHEPHERD to evaluate the standard's suitability in fulfilling the following requirements:

- EASA SC Light-UAS – Medium & High Risk provisions:
    - Light-UAS.2430.

It identifies and substantiates the list of recommended sections, subsections, paragraphs, or combination thereof of ASTM F3005-14a that have been deemed suitable and, hence, may be used as a basis for a means of compliance (MoC) for the requirements or a part thereof. In the same manner, it also lists and provides clear justification for the elements of the standard that have been found not technically adequate and, thus, need to be tailored and/or complemented before being proposed as a MoC.

3.4.2 General remarks

In terms of applicability, Section 4 of ASTM F3005-14a should be tailored in order to introduce the MoC based upon recommended sections. No specific rationale to limit the standard to UA of less than 25 kg has been identified (other than the remit of ASTM to deal with small UAS), nor any risk-based approach is apparent that would limit the SAIL applicability.

The detailed technical assessment is presented considering the various sections treated as a whole since the same remarks and conclusions have been reached; altogether, compliance with the criteria set forth in these sections should provide a reasonable assurance that the intent of the requirements of Light-UAS.2430(a)(1)&(b) in terms of safe functioning of supporting systems supplied by the batteries and in terms of their design and installation is met.

For further details on the rationale for the sections that have been considered as 'N/A' being too high-level requirements or similar to the requirements, as well as the rationale for the recommended sections, refer to the detailed technical assessment.

3.4.3 Recommended sections

This subsection provides the list of recommended sections, subsections, paragraphs, or combination thereof of ASTM F3005-14a that may be used as a basis for a MoC for the requirements or a part thereof as identified in the detailed technical assessment.

ASTM F3005-14a			
Requirement	**Related SAIL Integrity / assurance**	**Recommended section(s), subsection(s), paragraph(s), or combination thereof**	**Additional relevant information**
Light-UAS.2430	SAIL III to VI (Medium & High risk)	5 6 7 8	Light-UAS.2430(a)(2) is not addressed.

3.4.4 Non-recommended sections

This subsection provides the list of elements of ASTM F3005-14a that need to be tailored and/or complemented before being proposed as a MoC for the requirements or a part thereof as identified in the detailed technical assessment.

ASTM F3005-14a			
Section, subsection, or paragraph to be tailored / complemented	**Title / subject**	**Requirement and SAIL**	**Required tailoring / complementing**
4	Applicability	Light-UAS.2430 SAIL III to VI (Medium & High risk)	Refer to the general remark in Section 3.4.2.

3.5 ASTM F3178-16

3.5.1 Introduction

While AW-Drones identified *ASTM F3178-16. Operational Risk Assessment of Small Unmanned Aircraft Systems (sUAS)* as a potentially suitable candidate for showing compliance with OSO#01 – Medium (M) & High (H) integrity requirement regarding "*a method to identify, assess, and mitigate risks associated with flight operations [...] consistent with the nature and extent of the operations specified*", JARUS WG-SRM Annex E subgroup has recently agreed on updating this requirement following the external public consultation of draft SORA v2.5. The revised OSO#01 integrity requirement now places greater emphasis on the operator's responsibility to maintain a "*method to continuously evaluate whether the operator is operating according to the terms of the operational authorization and check whether the mitigations proposed as part of the operational authorization are still appropriate*".

In light of this evolving requirement, ASTM F3178-16 on operational risk assessment for UAS no longer aligns with the intent of OSO#01 requirements for a Medium (M) and High (H) levels of integrity.

However, it is recommended[1] for partially fulfilling provisions UAS.LUC.030(2)(e) and UAS.LUC.030(2)(g)(vi) of Part C of the Annex to IR (EU) 2019/947[2] for the obtention of a Light UAS operator Certificate (LUC), which is required under the EASA framework, following the publication of ED Decision 2023/012/R, for achieving compliance with OSO#01 – High (H) level of assurance.

3.5.2 Technical assessment

ASTM F3178-16 proposes a structured approach for assessing operational risks in the context of airworthiness and operations approval for UA below 55 lb (25 kg). Specifically, this standard guides applicants in understanding and documenting the expected operational environment, encompassing ground and airspace considerations, meteorological conditions, operational procedures, and system specifications, among others; identifying potential hazards associated with the intended operations; analysing the risk through a process that combines the likelihood of occurrence and the severity of consequences; and mitigating unacceptable levels of risk. Additionally, it offers a list of common failures to small UAS, some of which come with a detailed description of failure conditions and recommended mitigation practices.

While ASTM F3178-16 aligns with the fundamental principles of operational risk assessment in aviation, it falls short of the holistic / total, logically structured approach provided by SORA, specifically tailored by JARUS for UAS operations in the 'specific' category based on adequate, internationally agreed targets level of safety (TLOS) for both uninvolved people on the ground and other airspace users. As such, ASTM F3178-16 is not deemed a suitable alternative to SORA as acceptable means of compliance (AMC) with Article 11 of IR (EU) 2019/947. Indeed, F3178-16 lacks coverage of all provisions specified in Article 11 related to UAS operational risk assessment, including, inter alia, the definition of adequate operational safety objectives or the determination of the robustness of the necessary mitigation measures to meet the target level of safety.

However, despite the mentioned limitations, ASTM F3178-16 still offers valuable guidance for UAS operators. It can significantly contribute to enhancing their understanding of safety and risk management principles as a preliminary step for the formulation of appropriate procedures, practices, and policies for the identification, assessment, and mitigation of risks, which can complement or

[1] Only the sections identified as recommended.

[2] UAS.LUC.030(2)(g)(vi) reads as follows: "*The UAS operator shall [...] document all safety management system key processes for making personnel aware of their responsibilities [...], including safety risk management*".

support the SORA assessment from a more conventional safety risk management (SRM) perspective, as required by provisions UAS.LUC.030(2)(e) and UAS.LUC.030(2)(g)(vi) of Part C of the Annex to IR (EU) 2019/947 for the obtention of a LUC as a prerequisite to achieve compliance with OSO#01 – High (H) level of assurance under the EASA framework. Such key procedures, practices, and policies could be integrated into a broader SRM process within a comprehensive safety management system (SMS) adapted to the size of the organisation and the nature and extent of the intended operations.

ASTM F3178-16 does not provide any organisational guidance or requirements in terms of structure, post-holders, etc. Certain terms and concepts used are US-specific and may require adjustment to align with the European framework.

3.5.3 Recommended sections

The following table summarises the different sections of ASTM F3178-16 and identifies which of them are recommended for showing partial compliance with provisions UAS.LUC.030(2)(e) and UAS UAS.LUC.030(2)(g)(vi) of Part C of the Annex to IR (EU) 2019/947.

As stated in 3.5.2, a solid understanding of safety and risk management principles is essential for the development of appropriate procedures, practices, and policies aimed at identifying, assessing, and mitigating risks. This holds particularly true when such procedures are intended to be integrated into a broader SRM process within a comprehensive SMS, as mandated for the obtention of a LUC.

In this context, the table below provides clear guidance regarding the recommended sections of ASTM F3178-16 for acquiring knowledge on safety and risk management principles and those suitable for the subsequent development and implementation of the relevant risk identification, assessment, and mitigation procedures, practices, and policies.

ASTM F3178-16	
Section	**Content and relevance**
Introduction	High-level overview of the ASTM F3178-16 standard; introduction to the concept of 'operational risk assessment' ('ORA'). This section can be omitted.
1. Scope	Explanation of the scope, assumptions, and purpose of the standard. While F3178-16 self-limits its applicability to UAS below 55 lb (25 kg), it is deemed generally applicable to any UAS operated in the 'specific' category, with the caveat that the particularities of certain UAS systems / designs may require additional consideration. This section is recommended for gaining an overall understanding of both the standard and the safety and risk management principles. Certain terms and concepts used are US-specific and may require adjustment to align with the European framework.
2. Referenced Documents	Reference to SAE ARP4754A and ARP4761 standards, which are recommended for larger / higher energy UAS designs. These two standards are not part of SHEPHERD's scope. This section can be omitted.

ASTM F3178-16	
Section	**Content and relevance**
3. Terminology	Definition of relevant terms and units used throughout the standard. This section is recommended for gaining an overall understanding of both the standard and the safety and risk management principles, subject to the necessary terminology adaptations to the European framework. Certain terms and concepts used are US-specific and may require adjustment to align with the European framework.
4. Summary of Practice	A summary section with content similar to the Introduction. This section can be omitted.
5. Significance and Use	Explanation on the use of the F3178-16 standard as in Section 1 (Scope), complemented with the statement in subsection 5.2 that no ORA can eliminate all risks or uncertainty with regard to operations, but rather reduce it to an acceptable level. Subsection 5.2 is recommended for gaining understanding of the overarching safety and risk management principles. Certain terms and concepts used are US-specific and may require adjustment to align with the European framework.
6. Concept of Operations	Detailed guidance on the minimum elements of the system and aspects of intended operations that should be thoroughly described and documented. These should be considered generally covered by the SORA methodology, namely Annex A, with very few exceptions, such as the requirement for obtaining permission from landowners to operate from their land under point 6.3.4 or physical security under point 6.4.22. This section is recommended as a validation step for UAS operators that all relevant system and operational details are adequately documented and, hence, for the practical development and implementation of the relevant risk identification, assessment, and mitigation procedures, practices, and policies. Certain terms and concepts used are US-specific and may require adjustment to align with the European framework.
7. Operational Risk Assessment (ORA)	General explanation of safety hazard identification, analysis, mitigation, and documentation based on a well-documented ConOps. Recommendations for a hazard tracking system and a voluntary reporting system under points 7.2.3 and 7.2.4, both of which can be adapted to the size and needs of the organisation and complexity of the operation.

ASTM F3178-16	
Section	**Content and relevance**
	This section is recommended for the practical implementation of the relevant risk identification, assessment, and mitigation procedures, practices, and policies. Certain terms and concepts used are US-specific and may require adjustment to align with the European framework.
8. Common Operational Mitigations for sUAS	List of recommendations for operational mitigations, including training, operating procedures, go/no-go criteria, etc. These requirements should be considered covered by meeting OSO#08, OSO#09, OSO#20, and OSO#23. This section can be omitted.
9. Operation (Mission) System Configuration Management and Data Requirements	High-level description of configuration & change and data management requirements. Configuration management requirements can be considered covered by meeting updated OSO#01 – Medium (M) & High (H) and OSO#07. Although further detail and guidance are considered necessary for the establishment of the relevant procedures, practices, and policies, this section is recommended to complement Section 7. Certain terms and concepts used are US-specific and may require adjustment to align with the European framework.
10. Keywords	List of keywords used throughout the standard. This section can be omitted.
X1. Common Failures to sUAS by Category	List of examples of common failure to small UAS. These failures should be considered as addressed when meeting the relevant SORA OSOs (e.g., OSO#05 & OSO#10) and containment requirements. This section can be omitted.
X2. Examples of Hazard or Failure Identification and Mitigation Practices	List of examples of hazards / failure conditions with mitigation proposals. Same as for X1. This section can be omitted.

In conclusion, the combination of recommended sections 1, 3, 5.2, 6, 7, and 9 of ASTM F3178-16 provides partial coverage of provisions UAS.LUC.030(2)(e) and UAS.LUC.030(2)(g)(vi) of Part C of the Annex to IR (EU) 2019/947; additional guidance or best practices regarding the definition of risk probability and severity thresholds for the categorisation of risks as well as the establishment of acceptability levels are deemed necessary.

3.6 ASTM F3201-16

3.6.1 Introduction

The objective of this section is to present the outcome of the technical assessment of *ASTM F3201-16. Standard Practice for Ensuring Dependability of Software Used in Unmanned Aircraft Systems (UAS)* conducted to evaluate the standard's suitability in fulfilling the following requirements:

- SORA v2.5 OSOs:
  - OSO#05 Integrity, SAIL V & VI – High (H); and
  - OSOs#10+ Integrity, SAIL V & VI – High (H);
- SORA v2.5 Annex E section 4 requirements for the containment of the operation (Step #8);
- EASA SC Light-UAS – Medium & High Risk provisions:
  - Light-UAS.2510(a); and
  - Light-UAS.2511(b)(3).

ASTM F3201-16 proposes as a whole a methodology ("*that may be used by itself or in conjunction with other standards such as DO-178C*" – see section 4.3) to ensure that the software used on the UAS flight critical functions are dependable (e.g., safe and secure).

Consequently, it has been considered that, in this particular case, following the criteria and methodology developed by SHEPHERD to perform a section by section assessment is not appropriate; instead, a high-level technical assessment and subsequent recommendations are directly provided through this assessment report.

3.6.2 High-level technical assessment

The reference to software (SW) or airborne electronic hardware (AEH) development assurance processes to reduce the likelihood of development error(s) is bound to very specific wording both in EASA SC Light-UAS and JARUS SORA v2.5 released for external consultation.

The following table summarises the cases where the risk of development errors is mentioned both in EASA SC Light-UAS and JARUS SORA v2.5 released for external consultation, leading to the requirement to develop the software in accordance with an acceptable standard:

EASA SC Light-UAS	JARUS SORA v2.5 released for external consultation
Light-UAS.2511(b)(3) – Containment *When the risk associated with the adjacent areas on ground or adjacent airspace is significantly higher than the risk associated with the operational volume including the ground buffer:* ***software and airborne electronic hardware whose development error(s) could directly lead to operations outside the ground risk buffer*** *must be developed to a standard or methodology accepted by the Agency.*	SORA Annex E v2.5 section 4 requirements for the containment of the operation (Step #8) Integrity Criterion#4 – Medium (M) & High (H) ***Software (SW) and Airborne Electronic Hardware (AEH) whose development error(s) could directly lead to operations outside of the ground risk buffer*** *shall be developed to an industry standard or methodology recognized as adequate by the competent authority.*

EASA SC Light-UAS	JARUS SORA v2.5 released for external consultation
Note: *The use of the term 'directly' means that a development error in a software or an airborne electronic hardware would lead the UA outside the ground risk buffer without the possibility for another means to prevent the UA from exiting the operational volume.*	The note introduced in the EASA SC light-UAS to clarify the use of the term 'directly' does not exist in the JARUS document but the intent is the same.
No equivalent in SC Light-UAS.2510(a)	OSO#5 Integrity, SAIL V & VI – High (H) *Software (SW) and Airborne Electronic Hardware (AEH) whose development error(s) may cause or contribute to hazardous or catastrophic failure conditions are developed to an industry-standard or a methodology considered adequate by the competent authority and/or in accordance with means of compliance acceptable to that authority.*
No equivalent in SC Light-UAS.2510(a)	*Note:* *Development Assurance Levels (DALs) for SW/AEH may be derived from JARUS AMC RPAS.1309 Issue 2 Table 3 depending on the UAS class or an equivalent risk-based methodology acceptable to the competent authority.*
No equivalent in SC Light-UAS.2510(a)	OSOs#10+ Integrity, SAIL V & VI – High (H) *When operating over population density above 2,500 ppl/km2,* ***Software (SW) and Airborne Electronic Hardware (AEH) whose development error(s) could directly lead to a failure affecting the operation in such a way that it can be reasonably expected that a fatality will occur*** *are developed to a standard considered adequate by the competent authority and/or in accordance with means of compliance acceptable to that authority.*
No equivalent in SC Light-UAS.2510(a)	*Note:* *National Aviation Authorities (NAAs) may define the standards and/or the means of compliance they consider adequate. The SORA Annex E will be updated at a later point in time with a list of adequate standards based on the feedback provided by the NAAs.*

Therefore, there are no criteria contained in EASA SC Light-UAS or JARUS SORA v2.5 released for external consultation which would allow for an objective assessment of the ASTM F3201-16 standard. That said, the SHEPHERD consortium both reviewed the content of the standard versus current UAS industry practices and organised a discussion with the originator of this standard.

The following paragraphs summarise this assessment and discussion:

- Many small UAS (<55 lb) manufacturers are implementing software outside the traditional norms for aviation (e.g., DO-178C) and the initial objective of the standard was to propose a way to ensure that the software is dependable (e.g., safe and secure) for flight critical functions.

- ASTM F3201-16 was built upon reviewing existing guidance and documentation on the use of Software of Unknown Pedigree (SOUP) in other industries (e.g. medical industry) that have a need for safety-critical, safety-related, or secure software.

  NOTE: while ASTM F3201-16 addresses certain cyber-security aspects (e.g., guidance on identification of vulnerability, execution of penetration tests, etc.), they fall outside the scope of the requirements considered for this assessment.

- ASTM F3201-16 proposes several *Tiers* of requirements depending on the criticality of the functions:
  - Tier 1 requirements for functions whose functional failures are classified as 'minor';
  - Tier 2 requirements for functions whose functional failures are classified as 'major'; and
  - Tier 3 requirements for functions whose functional failures are classified as 'hazardous' or 'catastrophic'.

    NOTE: The definitions of the functional failure severities mentioned above refer to some sources (e.g. FAA Advisory Circular 23.1309) that are not aligned with the JARUS AMC.1309 definitions referred to in the SORA methodology.

- Considering the cases where the risk of development errors is mentioned both in EASA SC Light-UAS and JARUS SORA v2.5, only Tier 3 requirements would be applicable to SAIL V & VI operations.

- That said, while configuration control and problem reporting are part of these requirements, it is not understood why configuration control and problem reporting are not systematically requested for all tiers; ED-12C requests configuration control and problem reporting for DAL-A, -B, -C, and -D.

- In addition, while testing is part of the options proposed, there is not enough emphasis put on modern simulation means which are now generally used by the UAS industry (e.g. Monte Carlo simulations).

- While finalising the assessment of this standard, EASA and the FAA jointly published on 19th of December, 2023 a set of criteria for assessing potential alternate standards or publicly available methodologies used in other industry domains. This set of criteria has not been reviewed by the SHEPHERD consortium neither was it possible to assess the ASTM F3201-16 according to these criteria considering the timeline of this project; our recommendation is not to use the ASTM F3201-16 as an alternative to ED-12C for SAIL V & VI operations as long as the assessment of the standard against the EASA/FAA recommendations is not done.

  NOTE: SHEPHERD took the time to check EASA/FAA recommendations in terms of configuration control: "*[A/B/C/D] The process ensures that all the data needed to replicate the hardware/software item released for certification and production are under configuration control, including means to regenerate/verify.*" This supports the fifth bullet point in this list as well as the general recommendation expressed in the seventh bullet point.

- Ideally, the gap analysis of ASTM F3201-16 versus these new EASA/FAA recommendations will be performed by ASTM F38 committee, which will then be able to decide whether they may want to launch an update of the standard.

3.7 ASTM F3269-21

3.7.1 Introduction

The objective of this section is to present the outcome of the preliminary high-level assessment and subsequent detailed technical assessment of *ASTM F3269-21. Methods to Safely Bound Behavior of Aircraft Systems Containing Complex Functions Using Run-Time Assurance* conducted in accordance with the criteria and methodology developed by SHEPHERD to evaluate the standard's suitability in fulfilling the following requirements:

- SORA v2.5 OSOs:
  - OSO#05 Integrity & Assurance, SAIL III to VI – Low (L) to High (H); and
  - OSO#10+ Integrity & Assurance, SAIL I to VI – Low (L) to High (H).

- SORA v2.5 Annex E section 4 requirements for the containment of the operation (Step #8) Integrity & Assurance for all SAIL – Low (L) to High (H).

It identifies and substantiates the list of recommended sections, subsections, paragraphs, or combination thereof of ASTM F3269-21 that have been deemed suitable and, hence, may be used as a basis for a means of compliance (MoC) for the requirements or a part thereof. In the same manner, it also lists and provides clear justification for the elements of the standard that have been found not technically adequate and, thus, need to be tailored and/or complemented before being proposed as a MoC.

3.7.2 General remarks

ASTM F3269-21 is intended to be used as guidance material for creating a fault-tolerant architecture at the system level. It provides requirements and best practices for creating a run-time assurance (RTA) architecture for containing the behaviour of complex functions within predefined bounds. It cannot be applied in isolation as a MoC for the above-mentioned operational safety objectives. The standard assumes that a safety assessment has been conducted outside the scope of the document and the standard uses the results of this safety assessment as an input.

The standard does not address the following requirements:

- OSO#10+; and
- Step#8 Criterion#3.

No sections of ASTM F3269-21 can be fully recommended as MoC. While the detailed assessment 'Recommended' certain sections, this is only intended as 'Partially recommended' with the original verbiage retained for a standardised assessment within SHEPHERD.

For further details on the rationale for the sections that have been considered as 'N/A' being too high-level requirements or similar to the requirements, as well as the rationale for the recommended sections, refer to the detailed technical assessment.

3.7.3 Recommended sections

This subsection provides the list of recommended sections, subsections, paragraphs, or combination thereof of ASTM F3269-21 that may be used as a basis for a MoC for the requirements or a part thereof as identified in the detailed technical assessment.

ASTM F3269-21			
Requirement	**Related SAIL Integrity / assurance**	**Recommended section(s), subsection(s), paragraph(s), or combination thereof**	**Additional relevant information**
N/A			

3.7.4 Non-recommended sections

This subsection provides the list of elements of ASTM F3269-21 that need to be tailored and/or complemented before being proposed as a MoC for the requirements or a part thereof as identified in the detailed technical assessment.

ASTM F3269-21			
Section, subsection, or paragraph to be tailored / complemented	**Title / subject**	**Requirement and SAIL**	**Required tailoring / complementing**
5	RTA Functional Architecture	OSO#05 Integrity SAIL III & IV – Low (L) & Medium (M)	– For SAIL III operations, some aspects of the standard may be tailored to be less rigorous without compromising the integrity requirements. – For both SAIL III and IV operations, some tailoring is needed to account for the inclusion of the safety assessment and DAL allocation process as well as the consideration for design and installation appraisals in more detail to verify the implementation of the architecture at equipment level.
5	RTA Functional Architecture	Step#8 Integrity – L, M, H Criteria #1 & #2 Step#8 Assurance – L Criteria #1 & #2	The standard practice needs to be tailored to address requirements specific to the containment of the operation. However, principles of the standard allow for such tailoring. Therefore, it is recommended to use this standard as a basis for building more detailed means of compliance, but not directly as a means of compliance.

3.8 ASTM F3298-19

3.8.1 Introduction

The objective of this section is to present the outcome of the preliminary high-level assessment and subsequent detailed technical assessment of *ASTM F3298-19. Standard Specification for Design, Construction, and Verification of Lightweight Unmanned Aircraft Systems (UAS)* conducted in accordance with the criteria and methodology developed by SHEPHERD to evaluate the standard's suitability in fulfilling the following requirements:

- EASA SC Light-UAS – Medium & High Risk provisions:
    - Light-UAS.2529.

It identifies and substantiates the list of recommended sections, subsections, paragraphs, or combination thereof of ASTM F3298-19 that have been deemed suitable and, hence, may be used as a basis for a means of compliance (MoC) for the requirements or a part thereof. In the same manner, it also lists and provides clear justification for the elements of the standard that have been found not technically adequate and, thus, need to be tailored and/or complemented before being proposed as a MoC.

3.8.2 General remarks

Whilst ASTM F3298-19 states in its introduction that it covers "*lightweight (UAS) (not necessarily limited to UAs under 55 lb GTOW)*", it is considered that the UA weight is not a limiting factor and a MoC referring to the ASTM F3298-19 sections recommended in subsection 3.8.3 could be applied to UA with a MTOM of up to 600 kg in an analogous manner as EASA's SC-Light UAS requirements.

Most of the recommended sections do not fully cover the entire requirements but, when gathered, provide a better (not total) coverage.

The main topic that is currently missing relates to performance standards for the accuracy of the navigation system in time and space. ASTM-WK75923 is working on addressing these topics but has not been assessed in this project, since it has not been published yet.

Additionally, there is ongoing work in EUROCAE WG-105 SG4 for a MoC for SC Light-UAS.2529.

For further details on the rationale for the sections that have been considered as 'N/A' being too high-level requirements or similar to the requirements, as well as the rationale for the recommended sections, refer to the detailed technical assessment.

3.8.3 Recommended sections

This subsection provides the list of recommended sections, subsections, paragraphs, or combination thereof of ASTM F3298-19 that may be used as a basis for a MoC for the requirements or a part thereof as identified in the detailed technical assessment.

ASTM F3298-19			
Requirement	**Related SAIL Integrity / assurance**	**Recommended section(s), subsection(s), paragraph(s), or combination thereof**	**Additional relevant information**
Light-UAS.2529	SAIL III to VI (Medium & High risk)	10.2.1 10.2.2 10.2.3 10.2.4 10.2.5 A2.4.1.2	– Sections 10.2.1, 10.2.2 and A2.4.1.2 mainly address the information that needs to be available at the Control Station for the pilot to accurately control and monitor the UA. – Sections 10.2.3 to 10.2.5 give useful performance requirements for navigation systems. It needs to be determined whether these performance levels are adequate for the intended operation.

3.8.4 Non-recommended sections

This subsection provides the list of elements of ASTM F3298-19 that need to be tailored and/or complemented before being proposed as a MoC for the requirements or a part thereof as identified in the detailed technical assessment.

ASTM F3298-19			
Section, subsection, or paragraph to be tailored / complemented	**Title / subject**	**Requirement and SAIL**	**Required tailoring / complementing**
N/A			

3.9 ASTM F3364-19

3.9.1 Introduction

The objective of this subsection is to present the outcome of the preliminary high-level assessment and subsequent detailed technical assessment of *ASTM F3364-19. Standard Practice for Independent Audit Program for Unmanned Aircraft Operators* conducted in accordance with the criteria and methodology developed by SHEPHERD to evaluate the standard's suitability in fulfilling the following requirements:

- SORA v2.5 OSOs:
    - OSO#01 Assurance, SAIL III to VI – Medium (M) & High (H).

It identifies and substantiates the list of recommended sections, subsections, paragraphs, or combination thereof of ASTM F3364-19 that have been deemed suitable and, hence, may be used as a basis for a means of compliance (MoC) for the requirements or a part thereof. In the same manner, it also lists and provides clear justification for the elements of the standard that have been found not technically adequate and, thus, need to be tailored and/or complemented before being proposed as a MoC.

3.9.2 General remarks

ASTM F3364-19 establishes a minimum set of requirements for an Unmanned Aircraft Systems (UAS) Operator Independent Audit Program in compliance with ASTM F3365-19. Therefore, it is recommended only in combination with the F3365-19 standard. Although the scope of the assessment was limited to OSO#1, it is acknowledged that this standard can also be used to support certain tasks of the competent authority outlined in Article 18 of Commission Implementing Regulation (EU) 2019/947, specifically points (h) and (j).

After conducting this assessment, a new version of this standard, denoted as F3364-23, has been released by ASTM. However, it is important to note that the differences between versions -19 and -23 primarily pertain to editorial aspects. The recent version has been refined to conform to the updated ASTM template, particularly in terms of terminology and formatting. Consequently, even if the assessment was made on the -19 version, the conclusions remain consistent with the current -23.

For further details on the rationale for the sections that have been considered as 'N/A' being too high-level requirements or similar to the requirements, as well as the rationale for the recommended sections, refer to the detailed technical assessment.

3.9.3 Recommended sections

This subsection provides the list of recommended sections, subsections, paragraphs, or combination thereof of ASTM F3364-19 that may be used as a basis for a MoC for the requirements or a part thereof as identified in the detailed technical assessment.

ASTM F3364-19			
Requirement	**Related SAIL Integrity / assurance**	**Recommended section(s), subsection(s), paragraph(s), or combination thereof**	**Additional relevant information**
OSO#01	Assurance SAIL III – Medium (M)	5 6 7 8	– ASTM F3364-19 needs to be complemented with ASTM F3365-19. – The list of items to be assessed in section 5.1.2 needs to be tailored to consider EU applicable regulation. – The classification of findings is not provided.
OSO#01	Assurance SAIL IV to VI – High (H)	5 6 7 8	– ASTM F3364-19 needs to be complemented with ASTM F3365-19. – The list of items to be assessed in section 5.1.2 needs to be tailored to consider EU applicable regulation. – It does not define how often 'regular' audits need to be performed as required by OSO#1 for High robustness. – It does not cover the following part of the requirement: "T*he applicant holds an Organizational Operating Certificate or is/has a recognized flight test organization*". – The classification of findings is not provided.

3.9.4 Non-recommended sections

This subsection provides the list of elements of ASTM F3364-19 that need to be tailored and/or complemented before being proposed as a MoC for the requirements or a part thereof as identified in the detailed technical assessment.

ASTM F3364-19			
Section, subsection, or paragraph to be tailored / complemented	**Title / subject**	**Requirement and SAIL**	**Required tailoring / complementing**
N/A			

3.10 ASTM F3365-19

3.10.1 Introduction

The objective of this section is to present the outcome of the preliminary high-level assessment and subsequent detailed technical assessment of *ASTM F3365-19. Standard Practice for Compliance Audits to ASTM Standards on Unmanned Aircraft Systems* conducted in accordance with the criteria and methodology developed by SHEPHERD to evaluate the standard's suitability in fulfilling the following requirements:

- SORA v2.5 OSOs:
    - OSO#01 Assurance, SAIL III to VI – Medium (M) & High (H)

It identifies and substantiates the list of recommended sections, subsections, paragraphs, or combination thereof of ASTM F3365-19 that have been deemed suitable and, hence, may be used as a basis for a means of compliance (MoC) for the requirements or a part thereof. In the same manner, it also lists and provides clear justification for the elements of the standard that have been found not technically adequate and, thus, need to be tailored and/or complemented before being proposed as a MoC.

3.10.2 General remarks

ASTM F3365-19 establishes the minimum set of requirements for auditing programs, methods, and systems, the responsibilities for all parties involved, and qualifications for entities conducting audits against ASTM standards on Unmanned Aircraft Systems. However, its structure and content are not limited in any way to this scope and the practice could be well applied to the audits referred to in OSO#1. This standard is recommended only in combination with ASTM F3364-19, which provides additional details on how to conduct audits for UAS Operators.

Although the scope of the assessment was limited to OSO#1, it is acknowledged that this standard could be also used to support certain tasks of the competent authority outlined in Article 18 of Commission Implementing Regulation (EU) 2019/947, specifically points (h) and (j).

For further details on the rationale for the sections that have been considered as 'N/A' being too high-level requirements or similar to the requirements, as well as the rationale for the recommended sections, refer to the detailed technical assessment.

3.10.3 Recommended sections

This subsection provides the list of recommended sections, subsections, paragraphs, or combination thereof of ASTM F3365-19 that may be used as a basis for a MoC for the requirements or a part thereof as identified in the detailed technical assessment.

ASTM F3365-19			
Requirement	**Related SAIL Integrity / assurance**	**Recommended section(s), subsection(s), paragraph(s), or combination thereof**	**Additional relevant information**
OSO#01	Assurance SAIL III – Medium (M)	4 5 6 7 8 9 10 11 12	– ASTM F3365-19 needs to be complemented with ASTM F3364-19. – Need to remove the reference to ASTM standards in the scope and title as the process is considered applicable in general. – The combination of the two standards can provide useful guidance to establish the minimum requirements for audit processes but are not exhaustive.
OSO#01	Assurance SAIL IV to VI – High (H)	4 5 6 7 8 9 10 11 12	– ASTM F3365-19 needs to be complemented with ASTM F3364-19. – Need to remove the reference to ASTM standards in the scope and title as the process is considered applicable in general. – It does not cover the following part of the requirement: "*The applicant holds an Organizational Operating Certificate or is/has a recognized flight test organization*".

			– In general, the combination of the two standards can provide useful guidance to establish the minimum requirements for audit processes but are not exhaustive.

3.10.4 Non-recommended sections

This subsection provides the list of elements of ASTM F3365-19 that need to be tailored and/or complemented before being proposed as a MoC for the requirements or a part thereof as identified in the detailed technical assessment.

ASTM F3365-19			
Section, subsection, or paragraph to be tailored / complemented	**Title / subject**	**Requirement and SAIL**	**Required tailoring / complementing**
N/A			

3.11 ASTM F3367-21a

3.11.1 Introduction

The objective of this section is to present the outcome of the preliminary high-level assessment and subsequent detailed technical assessment of *ASTM F3367-21a. Standard Practice for Simplified Methods for Addressing High-Intensity Radiated Fields (HIRF) and Indirect Effects of Lightning on Aircraft* conducted in accordance with the criteria and methodology developed by SHEPHERD to evaluate the standard's suitability in fulfilling the following requirements:

- SORA v2.5 OSOs:
  - OSO#24 Integrity, SAIL III to VI – Medium (M) & High (H).
- EASA SC Light-UAS – Medium & High Risk provisions:
  - Light-UAS.2515; and
  - Light-UAS.2520.

It identifies and substantiates the list of recommended sections, subsections, paragraphs, or combination thereof of ASTM F3367-21a that have been deemed suitable and, hence, may be used as a basis for a means of compliance (MoC) for the requirements or a part thereof. In the same manner, it also lists and provides clear justification for the elements of the standard that have been found not technically adequate and, thus, need to be tailored and/or complemented before being proposed as a MoC.

3.11.2 General remarks

As known, UA weights, configurations and applications may be extremely different from each other and, for most of them, meeting Lightning Protection and HIRF Protection requirements would be much penalising in terms of weight and performance, if not impossible.

It is likely that the majority of UAS operators would prefer to choose the path of operational procedures and limitations to avoid these threats, as per EASA SC Light-UAS.2515 and Light-UAS.2520, showing and ensuring that the exposure to HIRF and Lightning is unlikely.

Furthermore, as stated in the Appendix to the assessed standard, ASTM F3367-21a has been derived from the FAA policy on HIRF/Lightning for "*low end Part 23*" manned (fixed-wing) aircraft, which is likely to be extensively revisited in case of Unmanned Aircraft Systems (different UA configurations and applications) that would nevertheless choose to comply with some form of HIRF / Lightning Protection requirements that would have to be more generic or established on a case by case.

The above remarks explain why most of the sections of the ASTM F3367-21a could not be recommended.

NOTE: A separate evaluation against the two EASA SC Light-UAS requirements dealing with the same topics as ASTM F3367-21a –Light-UAS.2515 ("*Electrical and electronic system lightning protection*") and Light-UAS.2520 ("*High-Intensity Radiated Fields (HIRF) Protection*")– is not presented in the detailed assessment after it became obvious that the same conclusions as with OSO#24 would be drawn.

For further details on the rationale for the sections that have been considered as 'N/A' being too high-level requirements or similar to the requirements, as well as the rationale for the recommended sections, refer to the detailed technical assessment.

3.11.3 Recommended sections

This subsection provides the list of recommended sections, subsections, paragraphs, or combination thereof of ASTM F3367-21a that may be used as a basis for a MoC for the requirements or a part thereof as identified in the detailed technical assessment.

ASTM F3367-21a			
Requirement	**Related AMC & GM**	**Recommended section(s), subsection(s), paragraph(s), or combination thereof**	**Additional relevant information**
OSO#24 Light-UAS.2515 Light-UAS.2520	Integrity (OSO#24) SAIL III to VI – Medium (M) & High (H)	5.1.3 & 5.1.4	– Subsections 5.1.3.1 to 5.1.3.3 are contingent upon UA configuration and technology. – Partial coverage.

3.11.4 Non-recommended sections

This subsection provides the list of elements of ASTM F3367-21a that need to be tailored and/or complemented before being proposed as a MoC for the requirements or a part thereof as identified in the detailed technical assessment.

ASTM F3367-21a			
Section, subsection, or paragraph to be tailored / complemented	**Title / subject**	**Requirement and SAIL**	**Required tailoring / complementing**
4	Overview Flowchart	OSO#24 (Integrity) Light-UAS.2515 Light-UAS.2520 SAIL III to VI – Medium (M) & High (H)	Any MoC may keep the intent of the chart to identify the various steps of the HIRF/IEL assessment in the case of UAS but would need to be adapted.
5.1	Minimum Design Requirements	OSO#24 (Integrity) Light-UAS.2515 Light-UAS.2520 SAIL III to VI – Medium (M) & High (H)	If deviations from any proposed design recommendations (e.g. tailored 5.1.3 and 5.1.4 – see above subsection 3.11.3) are desired, opening the door for operational procedures and limitations should be offered as per the SORA and EASA SC Light-UAS approach.
5.1.2	High Certification Level versus Low Certification Level	OSO#24 (Integrity) Light-UAS.2515 Light-UAS.2520 SAIL III to VI – Medium (M) & High (H)	This section refers to (manned) aeroplane certification levels as defined in CS23.2005 which are not relevant to UAS. In possibly tailoring this requirement, the concept of SAIL could be introduced to vary the level of HIRF to be applied.
6	Determine the Aeroplane Assessment Level	OSO#24 (Integrity) Light-UAS.2515 Light-UAS.2520	– This section refers to (manned) aeroplane certification levels as defined in CS23.2005 which are not relevant to UAS. In possibly

ASTM F3367-21a			
Section, subsection, or paragraph to be tailored / complemented	**Title / subject**	**Requirement and SAIL**	**Required tailoring / complementing**
		SAIL III to VI – Medium (M) & High (H)	tailoring this requirement, the concept of SAIL could be introduced to vary the level of HIRF/Lightning to be applied. – It also does not address the possibility of electrical engines.
7	HIRF and IEL System Safety Analysis	OSO#24 (Integrity) Light-UAS.2515 Light-UAS.2520 SAIL III to VI – Medium (M) & High (H)	In line with the approach of SC Light-UAS.2520 and Light-UAS.2515; however, UAS System Safety Assessment criteria and definitions should be used instead.
8	HIRF Compliance	OSO#24 (Integrity) Light-UAS.2515 Light-UAS.2520 SAIL III to VI – Medium (M) & High (H)	Directly related to section 7, which is not recommended.
9	IEL Compliance	OSO#24 (Integrity) Light-UAS.2515 Light-UAS.2520 SAIL III to VI – Medium (M) & High (H)	Directly related to section 7, which is not recommended.
10	Test methods	OSO#24 (Integrity) Light-UAS.2515 Light-UAS.2520 SAIL III to VI – Medium (M) & High (H)	Directly related to sections 7, 8, and 9, which are not recommended.

ASTM F3367-21a			
Section, subsection, or paragraph to be tailored / complemented	**Title / subject**	**Requirement and SAIL**	**Required tailoring / complementing**
Appendix	Background Information	OSO#24 (Integrity) Light-UAS.2515 Light-UAS.2520 SAIL III to VI – Medium (M) & High (H)	It captures the rationale from the FAA policy on HIRF/Lightning for 'low end Part 23' manned aircraft, which is likely to be extensively revisited in case of Unmanned Aircraft Systems (different UA configurations and applications).

3.12 ASTM F3389/F3389M-21

3.12.1 Introduction

The objective of this section is to present the outcome of the technical assessment of ASTM F3389/F3389M-21 conducted to evaluate the standard's suitability in fulfilling the following requirements:

- SORA Annex B v2.5 mitigation means:
  - M2 Integrity, Medium (M) & High (H)

		LEVEL of INTEGRITY	
		Medium (M)	**High (H)**
M2 – Effects of UA impact dynamics are reduced	*Criterion #1 (Technical design)*	• *Effects of impact dynamics and immediate post impact hazards[1], critical area or the combination of these results are reduced such that the risk to population is reduced by an approximate 1 order of magnitude (90%)[2,3].* • *When applicable, in case of malfunctions, failures or any combinations thereof that may lead to a crash, the UAS contains all elements required for the activation of the mitigation[4].* • *When applicable, any failure or malfunction of the proposed mitigation itself (e.g., inadvertent activation) does not adversely affect the safety of the operation.*	*Same as Medium. In addition:* • *When applicable, the activation of the mitigation is automated[4, 5, 6].* • *The effects of impact dynamics and immediate post impact hazards[1], critical area or the combination of them are reduced such that the risk to the population is reduced by an approximate 2 orders of magnitude (99%)[2,3].*
	Comments	*[1] Examples of immediate post impact hazards include fires and release of high energy parts.* *[2] Latest research on UAS impacts estimate injuries using the Abbreviated Injury Scale (AIS) developed for automotive impact tests and test dummies. An impact that has a 30% chance of causing injury of AIS level 3 injury or greater is estimated to have a 10% probability of death. Note that the SORA methodology only considers fatalities. It does not provide guidance on the injury levels / thresholds beyond which an injury should be considered as*	

		LEVEL of INTEGRITY	
		Medium (M)	**High (H)**
		a fatality. Further Guidance on how to evaluate impact severity measurement may be found for example in Ranges of Injury Risk Associated with Impact from Unmanned Aircraft Systems DOI: 10.1007/s10439-017-1921-6, ASSURE UAS reports A14 and A4 on UAS Ground Collision Severity Evaluation. *[3] The reduction in risk detailed here is equivalent to a "System Risk Ratio" which requires that the combination of functional performance (i.e., the reduction in risk when the mitigation functions as intended) and reliability (i.e., the chance that the mitigation does not function as intended) combined meet the requirement.* *[4] Failures or malfunctions of the UAS or mitigation means should not prevent the safe functioning of either system independently, if applicable.* *[5] An automated activation may be required when reaction time is critical or the operator cannot determine the need for activation.* *[6] The applicant may nevertheless implement an additional manual activation function.*	
	Criterion #2 (Procedures)	*Any equipment used to reduce the effect of the UA impact dynamics are installed and maintained in accordance with UAS / mitigation designer instructions.*	
	Comments	*N/A*	
	Criterion #3 (Training)	*When use of the mitigation requires action from the remote crew, then appropriate training must be provided for the remote crew by the operator.* *The operator must ensure that the personnel responsible (internal or external) for the installation and maintenance of the mitigation measures are qualified for the task.*	
	Comments	*N/A*	

3.12.2 Technical assessment

JARUS SORA M2 ground risk mitigation is intended to reduce the effect of ground impact once the control of the operation is lost. This can be achieved by reducing the size of the expected critical area, reducing the probability of lethality of a UA impact (by leveraging reductions in characteristics such as energy, impulse, transfer energy dynamics, etc.), or a combination of both methods.

The scope of ASTM F3389/F3389M-21 is specific to the second case, assessing the reduction of the probability of lethality of a UA impact; more specifically, the standard proposes four methods for evaluating the potential for impact injury:

- a simple analytical method (Method A);
- a simplified test (Method B);
- a more rigorous test (Method C); and
- a test method normed to approximate energy transfer values (Method D)

with appropriate safety margins applied to each method to address uncertainty in each of the approaches.

For these reasons, ASTM F3389/F3389M-21 is only deemed worthy of being evaluated against the JARUS SORA v2.5 M2 Criterion#1 for Medium (M) and High (H) levels of integrity, i.e. "*Effects of impact dynamics and immediate post impact hazards, critical area, or the combination of these results are reduced such that the risk to population is reduced by an approximate 1 (resp. 2 for High) order(s) of magnitude (90% (resp. 99% for High)*".

Methods B and C are limited to 8 lb (3.6 kg) drones or lighter, or up to 55 lb (25 kg) if being tested at parachute speeds.

Considering the pass/fail criteria of ASTM F3389/F3389M-21:

- Method A: 73 J max impact kinetic energy (KE);
- Method B: Characterization of impact risk as a function of UA kinetic energy based on the calculation of skull fracture risk. Pass/fail criteria based on NAA-defined safe threshold value of kinetic energy[3] and operating envelope, including environmental condition, constraints put in place to meet that value during operations;
- Method C: Characterisation of impact risk as a function of UA kinetic energy, plus head and neck injury metrics. Pass/fail criteria based on NAA-defined safe threshold value of kinetic energy, head and neck injury metrics;
- Method D: Injury Risk (head and neck injury criteria) of UA impact are less than the same values for a rigid impactor at NAA-defined kinetic energy thresholds.

The method conservatively assumes the following:

- All impacts are assumed to be at the most probable worst case configuration;
- All impacts are assumed to be to the head, the expected most sensitive area of the human body;

[3] In the absence of a specific application threshold, the value G for skull fracture shall be the peak resultant head acceleration metrics shown in Chapter 5 of *Report for the FAA UAS Center of Excellence Task A14: UAS Ground Collision Severity Evaluation 2017-2019*, which corresponds to a 30% probability of an AIS3+ injury.

- Kinetic energy thresholds from the ASSURE Task 14 report, which are supposed to represent 30% probability of an AIS3+ injury (taken from the FAA Micro UAS ARC report), are deemed overly conservative by the ASSURE Task 14 report as test results in the ASSURE study are less than the severity predicted. ASSURE recommends reassessing the metrics for UAS.

Assessment of individual methods:

- Method A: A UA with a maximum impact kinetic energy value of 73 J will meet M2 Medium injury criteria as defined in EASA MOC Light-UAS.2512-01 (M2 MoC) in Type 2 Means iii, "*ensure a maximum impact energy of less than 175 J*". UA with kinetic energy values referenced in the ASSURE Task 14 report may be able to meet M2 High injury criteria as the ASSURE Task 14 report says this value is conservative and the kinetic energy value is 42% of the value in the M2 MoC and is less than the maximum transferred energy requirement of 80 J, but further analysis or research is deemed needed.

- Method B: A UA that has put in place operational limitations to meet the kinetic energy limits derived from the threshold values from the ASSURE Task 14 report for a skull impact that results in a 30% probability of AIS3+ injury will meet M2 Medium injury criteria as this matches the criteria defined in EASA MOC Light-UAS.2512-01 (M2 MoC) in Type 2 Means ii, "*demonstrate that an impact with a person in the most critical condition results at most in 30% probability of AIS3+ injuries*". UA with kinetic energy values referenced in the ASSURE Task 14 report may be able to meet M2 High injury criteria as the report uses a conservative approach, but verification is deemed needed. If desired it is recommended that EASA determine their own values to better align with M2 Medium and High requirements.

- Method C: The method does not define any threshold criteria in the standard and refers to the governing NAA metrics. EASA would have to define threshold criteria relating to M2 Medium and High requirements before applicants can use this method.

- Method D: The method does not define any energy level threshold for the rigid impactor and references needing to come to agreement with the governing NAA. EASA would have to define energy level thresholds for the rigid impactor relating to M2 Medium and High requirements before applicants can use this method.

3.12.3 Proposed areas of improvement

Map AIS3+ injury metrics to probability of lethality

Mapping the AIS3+ injury metric probabilities used in the standard to probability lethality will better align test results with NAA requirements and the JARUS SORA methodology (e.g. the standard considers situation 'safe' below AIS3 30%, when in fact it should be less than 10% lethal to be aligned with the JARUS methodology.)

Pass/fail criterion and safe kinetic energy thresholds

The ASSURE Task 14 report mentions that the values in the report are overly conservative and should be reassessed for UAS, but ASTM F3389/F3389M-21 references these values as is without providing that context, which results in overly conservative kinetic energy threshold values.

The SHEPHERD consortium would like to recommend that future versions of this ASTM standard determine if there are more appropriate KE and risk injury values that better represent the risk, not only for 30% probability of AIS3+ injury, but also for the JARUS SORA M2 requirements of 10% and 1% probabilities of lethality.

Allow a weighted averaging approach to risk

To reduce the conservatism of the impact risk assessment, propose a method that allows users to complete a weighted average approach to the impact assessment, including:

- weighted average on the human body to where the UA will impact;
- weighted average of the type of failure and resultant impact dynamics (angle, orientation and speed).

EASA has indicated that this may not be the standard accepted approach and would need to be discussed as a MOC at the project level. As such it would still be an improvement in the standard to offer a process for this calculation to get an industry consensus approach for operators and NAAs.

3.13 ASTM F3548-21

3.13.1 Conformance monitoring service

3.13.1.1 Introduction

The objective of this section is to present the outcome of the preliminary high-level assessment and subsequent detailed technical assessment of *ASTM F3548-21. Standard Specification for UAS Traffic Management (UTM) UAS Service Supplier (USS) Interoperability* conducted in accordance with the criteria and methodology developed by SHEPHERD to evaluate the standard's suitability in fulfilling the following requirements:

- U-space IR (EU) 2021/664 requirements:
    - Article 13 on the conformance monitoring service and its associated set of AMC & GM published by EASA under ED Decision 2022/022/R on 20 December 2022.

The following subsections summarise the assessment results and indicate the conformance monitoring service requirements that are:

- fully addressed;
- partially addressed; and
- not covered;

by ASTM F3548-21.

3.13.1.2 General remarks

Acknowledging the principles behind the F3548-21 standard, the ASTM compliance mapping incorporates the concept of capabilities, the detailed requirements of which are comprehensively enumerated in Section 10 of the standard. These encompass:

Capability	List of applicable requirements
Strategic conflict detection	10.6
Aggregate operational intent conformance monitoring	10.7
Conformance monitoring for situational awareness	10.8

Keeping this perspective in mind, the following two subsections present a compilation of the conformance monitoring service requirements that are addressed either in their entirety ('Full coverage') or partially ('Partial coverage'), as well as the relevant capabilities.

Generally speaking, the main remarks are listed hereafter:

- GM1(b)(1) to Article 13 is only partially covered as the standard covers identification and operator notification of situations where the UAS flight authorisation deviation thresholds are violated but not when the capabilities and performance requirements, the requirements for the use of the necessary U-space services, or the applicable operational conditions and airspace constraints are not complied with.

- GM2(a)&(b) to Article 13 and AMC1(d) to Article 13(1) are not covered as checking for compliance relative to all the attributes listed in Article 3, Annex IV, required under Article 6(1), terms and conditions are beyond the scope of the standard.
- GM1(b)(2) to Article 13 is not covered by the standard requirements; other air traffic is out of the scope of the standard.
- GM1(b)(4) to Article 13 is not covered by the standard requirements; the single CIS provider is out of the scope of the standard.
- GM1(b)(5) to Article 13 is not covered by the standard requirements; other relevant authorities are out of the scope of the standard.
- The standard does not include the information of non-conformance into the traffic information message, but it only communicates uncoordinated behaviour through off-nominal 4D volumes.
- AMC4 to Article 13(1) is only partially covered as the standard requirement states to send a notification within 5 seconds, 95 % of the time, in contraposition with the regulation requirement of 99 % of the time.
- AMC1 to Article 13(2) is not addressed; USSP – ATSP communications are out of scope of the standard.
- The other Article 13 and associated AMC & GM requirements are deemed fully covered by the standard.

For further details on the rationale for the recommended sections as well as for the conformance monitoring service requirements beyond the scope of the standard, refer to the detailed technical assessment.

3.13.1.3 Requirements fully addressed

This subsection provides the list of recommended sections, subsections, paragraphs, or combination thereof of ASTM F3548-21 that may be used as a basis for a MoC for the conformance monitoring service requirements or a part thereof as identified in the detailed technical assessment.

ASTM F3548-21					
Requirement		**Coverage**	**Capability(ies)[4]**	**Relevant standard provisions**	**Remarks**
Article 13	GM1(a) Art 13	Full	Conformance monitoring for situational awareness	4.2.10 4.2.12 5.6.1.1	
	GM1(c)(2) Art 13	Full	Conformance monitoring for situational awareness	5.2.6.5 5.6.3.4 5.6.5.1 5.6.1.1	
	GM1(c)(3) Art 13	Full	Conformance monitoring for situational awareness	5.6.1.2 5.6.1.10 5.6.2.8 5.2.6.5 5.6.3.4 5.6.5.1	
Article 13(1)	AMC1(b) Art 13(1)	Full	Conformance monitoring for situational awareness	5.6.2.2 5.6.2.3 4.4.4	

[4] If an applicant meets the necessary requirements to demonstrate this capability, the applicant will meet the given regulatory requirement; when multiple capabilities are specified, the applicant must meet the requirements for all listed capabilities.

ASTM F3548-21					
Requirement		**Coverage**	**Capability(ies)[4]**	**Relevant standard provisions**	**Remarks**
	GM2(c) Art 13 AMC1(c) Art 13(1)	Full	Conformance monitoring for situational awareness	5.6.5.1	
	AMC1 Art 13(1) (cont'd)	Full Conditional	Conformance monitoring for situational awareness	5.6.5.1 5.6.5.2	Full coverage if details of non-conformance only relates to off-nominal volumes
	AMC2 Art 13(1)	Full	Aggregate operational intent conformance monitoring	5.5.1.1 5.3.2.1 5.3.2.2	
	GM2 Art 13(1) AMC3(b) Art 13(1)	Full	Conformance monitoring for situational awareness	4.2.11 4.4.4.3 5.6.5.1	
	GM3 Art 13(1)	Full	Conformance monitoring for situational awareness	5.6.5.1 5.6.5.2 5.6.5.6	
Article 13(2)	GM1(b)(3) Art 13	Full	Conformance monitoring for situational awareness	5.6.1.1 5.6.1.8 5.6.5.6 5.6.5.7 Annex A3	OpenAPI specification in Annex A3 for acknowledgement

3.13.1.4 Requirements partially addressed

This subsection provides the list of elements of ASTM F3548-21 that need to be tailored and/or complemented before being proposed as a MoC for the conformance monitoring service requirements or a part thereof as identified in the detailed technical assessment.

ASTM F3548-21					
Requirement		**Coverage**	**Capability(ies)**	**Relevant standard provisions**	**Remarks**
Article 13	GM1(b)(1) Art 13	Partial	Conformance monitoring for situational awareness	5.6.1.1 5.2.6.5 5.6.3.4 5.6.5.1	Include the non-conformances mentioned in the regulation
	GM1(c)(1) Art 13	Partial	Conformance monitoring for situational awareness	5.6.2.7	Off-nominal 4D volumes information to be added in the traffic information message
Article 13(1)	AMC1(a) Art 13(1)	Partial	Conformance monitoring for situational awareness	4.3.1 5.6.2.1	The standard matches the UA with respect to its operational intent but does not include other attributes as mentioned in Annex IV to the regulation.
	AMC4 Art 13(1)	Partial	Conformance monitoring for situational awareness	5.6.3.4	ASTM F3548-21 requires a notification within 5 s, 95% of the time. The regulation sets 99%.
Article 13(2)	N/A	Partial	Conformance monitoring for situational awareness Strategic conflict detection	5.4.2.19 5.6.5.6	– The sections refer only to alerts to UAS operators and other USSPs offering services in the same airspace. – Interfaces USSPs-UAS operators and USSPs-ATSPs are not covered so visual/display acknowledgments are not addressed.

3.13.1.5 Requirements not covered

ASTM F3548-21		
Requirement		**Rationale**
Article 13	GM1(b)(2) Art 13	Crewed air traffic – beyond the standard's scope
	GM1(b)(4) Art 13	CISP integration requirement – beyond the standard's scope
	GM1(b)(5) Art 13	Other relevant authorities – beyond the standard's scope
Article 13(1)	GM2(a)(b) Art 13 AMC1(d) Art 13(1)	U-space airspace requirement verification – beyond the standard's scope
	AMC3(a) Art 13(1)	Beyond the standard's scope
	GM1 Art 13(1)	The standard detects non-conformances based on position reports by comparing ongoing position data for a UA in flight with the associated operational intent, but, as long as the UA is inside the OI, it is considered as in conformance – beyond the standard's scope
Article 13(2)	AMC1 Article 13(2)	Communication with ATSP – beyond the standard's scope

3.13.2 Dynamic airspace reconfiguration

3.13.2.1 Introduction

The objective of this section is to present the outcome of the preliminary high-level assessment and subsequent detailed technical assessment of *ASTM F3548-21. Standard Specification for UAS Traffic Management (UTM) UAS Service Supplier (USS) Interoperability* conducted in accordance with the criteria and methodology developed by SHEPHERD to evaluate the standard's suitability in fulfilling the following requirements:

- U-space IR (EU) 2021/664 requirements:
    - Article 4 on the dynamic airspace reconfiguration (DAR) and its associated set of AMC & GM published by EASA under ED Decision 2022/022/E on 20 December 2022, as well as ATS.TR.237 of IR (EU) 2021/665.

The following subsections summarise the assessment results and indicate the dynamic airspace reconfiguration requirements that are:

- fully addressed;
- partially addressed; and
- not covered;

by ASTM F3548-21.

3.13.2.2 General remarks

Acknowledging the principles behind the F3548-21 standard, the ASTM compliance mapping incorporates the concept of capabilities, the detailed requirements of which are comprehensively enumerated in Section 10 of the standard. These encompass:

Capability	List of applicable requirements
Constraint management	10.2
Constraint processing	10.2
Discovery and Synchronization Service (DSS)	10.12

Keeping this perspective in mind, the following two subsections present a compilation of the DAR requirements applicable only to USSPs that are addressed either in their entirety ('Full coverage') or partially ('Partial coverage'), as well as the relevant capabilities.

Generally speaking, the main remarks are listed hereafter:

- ASTM F3548-21 specifically addresses U-space service providers, leaving ATC units outside its scope; the standard does not provide coverage for USSP-ATC exchanges in controlled airspace. However, it may conditionally and partially support certain dynamic airspace reconfiguration requirements if airspace information is provided in the form of constraints. As such, ATC units and providers of common information services (CIS) would need to integrate into the USSP network, either assuming the 'constraint manager' role themselves or collaborating with a USSP fulfilling this function on their behalf.

- The assessment has been performed only for the DAR requirements which pertain to USSPs. The USSPs shall have the 'constraint processing' capability in order to ingest constraint information, where the time-to-exit information must be included in the constraint details within the 'geozone' field.

- If DAR information is shared using the constraint mechanism, ATC units will need to rely on the 'constraint management' and the 'discovery and synchronization service (DSS)' capabilities listed above in order for the USSPs to implement the DAR in alignment with the standard requirements.

- No standard section(s) have been found suitable for GM2(c) Article 4 - Segregation assurance, as the U-space airspace risk assessment is out of scope of the standard.

- The standard relies on the UAS operator to adhere to the regulatory requirements associated with the constraints; for this reason, the standard does not define protection buffers consistent with the UAS performance requirements (as defined in section 5.8.1.2).

- The acknowledgement of the stakeholders is ensured through the DSS; however, the standard has not demonstrated its applicability to ATC units for dynamic airspace reconfiguration purposes.

- GM1(a), GM1(b), GM1(c), GM1(e), GM1(h), GM1(i), ATS.TR.237(b) & GM2(a), ATS.TR.237(a) & GM2(b)(2), GM2(b)(1), AMC1(b), and AMC1(a) to Article 4 were not considered for the assessment as they are either background information or requirements not applicable to USSPs.

For further details on the rationale for the recommended sections as well as for the dynamic airspace reconfiguration requirements beyond the scope of the standard, refer to the detailed technical assessment.

3.13.2.3 Requirements fully addressed

No dynamic airspace reconfiguration requirements or a part thereof are fully addressed by ASTM F3548-21.

3.13.2.4 Requirements partially addressed

This subsection provides the list of elements of ASTM F3548-21 that need to be tailored and/or complemented before being proposed as a MoC for the dynamic airspace reconfiguration requirements or a part thereof as identified in the detailed technical assessment.

ASTM F3548-21					
Requirement		**Coverage**	**Capability(ies)[5]**	**Relevant standard provisions**	**Remarks**
Article 4	GM1(d) Art 4	Partial Conditional	Constraint management Constraint processing Discovery and synchronization service (DSS)	4.5.4 4.2.16 4.2.17 5.7.1.1 5.7.1.2 5.7.2.13 5.8.1.2 Annex A3	The standard states that USSPs do not prevent the creation or activation of operational intents that intersect airspace restrictions or limitations. The USSPs just provide awareness of relevant constraints to UAS personnel or the operator's automation system.
	GM1(f) Art 4 AMC2 Art 4	Partial Conditional	Constraint management Constraint processing Discovery and synchronization service (DSS)	4.2.16 4.2.17 4.5.1 4.5.2 4.5.4 5.7.2.13 5.8.2.4	Specifically, the ATC unit will need to use the constraint management capability to create a constraint with a future earliest 4D volume start time, and this will serve as both the preliminary alert (any USSPs with relevant subscriptions/operational intents will receive

[5] If an applicant meets the necessary requirements to demonstrate this capability, the applicant will meet the given regulatory requirement; when multiple capabilities are specified, the applicant must meet the requirements for all listed capabilities.

ASTM F3548-21					
Requirement		**Coverage**	**Capability(ies)[5]**	**Relevant standard provisions**	**Remarks**
				Annex A3	a notification) and publishing of the restriction and provision to UAS operators.
	GM1(g) Art 4	Partial Conditional	Constraint processing Discovery and synchronization service (DSS)	4.2.17 4.5.2 5.8.2.1 5.8.2.3 5.8.2.4 Annex A3	Specifically, if a USSP makes use of the constraint mechanism, the UAS operators will be notified through the mechanism of the flight authorisation service with the corresponding associated operational intent.

3.13.2.5 Requirements not covered

ASTM F3548-21		
Requirement		**Rationale**
Article 4	GM1(a) Art 4	Background information
	GM1(b) Art 4	Background information
	GM1(c) Art 4	Communication between USSPs and ATC – beyond the standard's scope
	GM1(e) Art 4	Communication between USSPs and ATC – beyond the standard's scope
	GM1(h) Art 4	ATC procedures – beyond the standard's scope
	GM1(i) Art 4	Communication between USSPs and ATC – beyond the standard's scope
	AMC1(a) Art 4	U-space airspace design – beyond the standard's scope
	AMC1(b) Art 4	U-space airspace design – beyond the standard's scope
	GM2(a) Art 4	Communication between USSPs and ATC – beyond the standard's scope
	GM2(b)(1) Art 4	U-space airspace design – beyond the standard's scope
	GM2(b)(2) Art 4	U-space airspace design – beyond the standard's scope
	GM2(c) Art 4	U-space airspace design – beyond the standard's scope
	GM3 Art 4	Communication between USSPs and ATC – beyond the standard's scope
	AMC3 Art 4	Communication between USSPs and ATC – beyond the standard's scope

3.13.3 UAS flight authorisation service

3.13.3.1 Introduction

The objective of this section is to present the outcome of the preliminary high-level assessment and subsequent detailed technical assessment of *ASTM F3548-21. Standard Specification for UAS Traffic Management (UTM) UAS Service Supplier (USS) Interoperability* conducted in accordance with the criteria and methodology developed by SHEPHERD to evaluate the standard's suitability in fulfilling the following requirements:

- U-space IR (EU) 2021/664 requirements:
    - Article 10 on the UAS flight authorisation service and its associated set of AMC & GM published by EASA under ED Decision 2022/022/R on 20 December 2022.

The following subsections summarise the assessment results and indicate the UAS flight authorisation service requirements that are:

- fully addressed;
- partially addressed; and
- not covered;

by ASTM F3548-21.

3.13.3.2 General remarks

EASA has already acknowledged the significance of the ASTM F3548-21 standard in relation to the UAS flight authorisation service by incorporating it into GM3 Article 10(5) – *Unjustified delay* and GM1 Article 10(6) – *Arrangements in case of conflicting UAS flight authorisation requests*.

However, recognising the value of the F3548-21 standard compliance mapping effort against Article 10 carried out by ASTM, in collaboration with active contributions from various SHEPHERD consortium members, SHEPHERD has deemed it meaningful for the benefit of the UAS and U-space industries to integrate its key outcomes into the SHEPHERD project scope. In this context, rather than a mere copy-and-paste approach, this integration consists in presenting the critical information in a manner that facilitates **EASA's seamless adoption of new or update of existing AMC & GM concerning Article 10 based on the ASTM F3548-21 standard**.

Acknowledging the principles behind the F3548-21 standard, the ASTM compliance mapping incorporates the concept of capabilities, the detailed requirements of which are comprehensively enumerated in Section 10 of the standard. These encompass:

Capability	List of applicable requirements
Strategic coordination	10.2
Constraint management	10.2
Constraint processing	10.2
Strategic conflict detection	10.6

Capability	List of applicable requirements
Conformance monitoring for situational awareness	10.8
Constraint management	10.9
Discovery and Synchronization Service (DSS)	10.12

Keeping this perspective in mind, the following two subsections present a compilation of the UAS flight authorisation service requirements that are addressed either in their entirety ('Full') or partially ('Partial') by one or more of the previous capabilities, clearly indicating the instances where full or partial coverage is contingent upon specific conditions ('Conditional'). Moreover, Section 5 outlines the regulatory and associated AMC & GM requirements that are not covered by ASTM F3548-21, detailing whether they extend beyond the scope of the standard or serve solely as background information.

In addition to Article 10 on UAS flight authorisation service, SHEPHERD has been tasked by EASA to perform a detailed technical assessment of this standard against the dynamic airspace reconfiguration (Article 4) and conformance monitoring service (Article 13) requirements. Refer to the individual assessments for further details.

As remarked in the dedicated DAR assessment, ASTM F3548-21 specifically addresses U-space service providers, leaving ATC units outside its scope; the standard does not provide coverage for USSP – ATC exchanges in controlled airspace. However, it may conditionally and partially support Article 10 and associated AMC & GM requirements related to checking flight authorizations requests against U-space airspace restrictions, temporary airspace limitations, and dynamic airspace reconfiguration if airspace information is provided in the form of constraints. Additionally, to share airspace information effectively using this standard ATC units (in controlled airspace) and CIS would need to integrate into the USSP network, either assuming the 'constraint manager' role themselves or collaborating with a USSP fulfilling this function on their behalf.

3.13.3.3 Requirements fully addressed

This subsection provides the list of recommended sections, subsections, paragraphs, or combination thereof of ASTM F3548-21 that may be used as a basis for a MoC for the UAS flight authorisation service requirements or a part thereof.

ASTM F3548-21					
Requirement		**Coverage**	**Capability(ies)[6]**	**Relevant standard provisions**	**Remarks**
Article 10	GM1(e) Art 10 | Priority rules enforcement	Full	Strategic conflict detection	5.4	
Article 10(1)	GM1(a) Art 10 | Individual UAS flight authorisations	Full	Strategic conflict detection	5.4.2.3 5.4.2.4 5.4.2.5 5.4.2.6 5.4.2.7 5.4.2.8 5.4.2.9 5.4.2.10	
	GM1(b) Art 10	Full	Strategic conflict detection	5.4	Covered by the generic use case outlined in Section 5.4, but there is no special handling of repeated operations.
	GM1(c) Art 10 | Information on overlapping with	Full Conditional	Constraint processing	4.2.17 5.8	Only if geo-awareness information is shared in the form of constraints.

[6] If an applicant meets the necessary requirements to demonstrate this capability, the applicant will meet the given regulatory requirement; when multiple capabilities are specified, the applicant must meet the requirements for all listed capabilities.

ASTM F3548-21					
Requirement		**Coverage**	**Capability(ies)[6]**	**Relevant standard provisions**	**Remarks**
	airspace restrictions				
	GM1(b) Art 10(6)	Full	Discovery & Synchronization Service (DSS)	A2.4.1.4	
Article 10(2)(a)	AMC1(b) Art 10(2)(a);(b)	Full Conditional	Strategic conflict detection	5.4	If, in accordance with AMC1(d) Article 3(4)(d), the capacity and density limits of the U-space airspace is set such that 4D flight volumes may not overlap, ASTM F3548-21 meets this AMC. On the contrary, if they are defined through other means (e.g., fixing a maximum number of simultaneous UAS operations), then this standard does not provide coverage for this AMC.
Annex IV	GM1(a)(3) Annex IV	Full	Strategic conflict detection	5.4.1.3	
	GM1(a)(5) Annex IV	Full	Strategic conflict detection	4.3	While ASTM F3548-21 does not manage the interface with the UAS operator, the data specification provided can support standardisation of acceptable formats to meet this requirement.
	GM1(b) Annex IV	Full	Strategic conflict detection	4.3	

ASTM F3548-21					
Requirement		**Coverage**	**Capability(ies)[6]**	**Relevant standard provisions**	**Remarks**
	GM1(b) Art 10(2)	Full	Strategic conflict detection	4.3 5.3.1.3	
	GM1(e) Art 10(2) | 4D trajectory description	Full	Strategic conflict detection	4.3	
Article 10(2)(b)	AMC1(g) Art 10(2)(a);(b) | first paragraph GM1(a) Art 10(2)	Full	Strategic conflict detection	5.4.2.3 5.4.2.4 5.4.2.7 5.4.2.8	
	GM1(c) Art 10(2)	Full	Strategic coordination	5.3.2.1 5.3.2.2 5.4 5.5.1.3	
Article 10(4)	GM1 Art 10(4)	Full	Strategic conflict detection	5.4.2.18	
Article 10(5)	AMC1(e) Art 10(5) GM1(d) Art 10(5)	Full	Strategic conflict detection	5.4.2.5 5.4.2.19	
	AMC1(f)(2) Art 10(5) | Cooperative, non-conforming drones	Full	Strategic conflict detection	5.4.2.5 5.4.2.9 5.4.2.19	
	GM3 Art 10(5)	Full	Strategic conflict detection	5.2.6.5	

ASTM F3548-21					
Requirement		**Coverage**	**Capability(ies)[6]**	**Relevant standard provisions**	**Remarks**
Article 10(6)	AMC1(a) Art 10(6) GM1(a) Art 10(6)	Full	Strategic coordination Discovery & Synchronization Service (DSS)	A2.3.2 A2.3.3 A2.5.2	
	AMC1(b) Art 10(6) GM1(e) Art 10 | Exchange of UAS flight authorisation requests	Full	Strategic coordination Discovery & Synchronization Service (DSS)	4.4.4.5 A2.3.2 A2.3.3	While ASTM F3548-21 does not have an equivalent state to 'withdrawn', the 'ended' state can be used here to fulfil the intent.
Article 10(7)	GM1(d) Art 10(2) | Restricted area warning	Full Conditional	Constraint processing	5.8.2.4	Only if dynamic airspace restrictions and limitations are distributed as constraints.
	AMC2 Art 10(2)(a);(b) | first paragraph	Full Conditional	Constraint processing	5.8.1.2 5.8.2.1	Only if Member States use constraints as the mechanism for distributing information on airspace restrictions.
	AMC1(a) Art 10(7)	Full Conditional	Constraint management	5.7.2.1 5.7.2.2 5.7.2.3 5.7.2.13	A CIS provider could be an authorised constraint provider that supplies the Constraint Management service with airspace restriction data.
	AMC1(b) Art 10(7)	Full Conditional	Constraint processing Strategic coordination	5.3.2.1 5.3.2.2 5.8.1.2 5.8.2.1	Only if Member States use constraints as the mechanism for distributing information on airspace restrictions.

ASTM F3548-21					
Requirement		**Coverage**	**Capability(ies)[6]**	**Relevant standard provisions**	**Remarks**
Article 10(8)	AMC1(a) Art 10(8)	Full	Strategic conflict detection	5.4.2.16 5.4.2.19	
	AMC1(b) Art 10(8)	Full	Strategic conflict detection	5.2.6.5	
	GM1 Art 10(8)	Full	Strategic conflict detection	5.4.1.3	
Article 10(9)	AMC1(a) Art 10(9) GM1(a) Art 10(9) GM1(b) Art 10(9)	Full	Strategic conflict detection	5.4.1.5 5.4.1.7 5.4.2.3 5.4.2.7 5.4.2.18 5.4.2.19 5.9.2.10 5.9.2.11	
	AMC1(b) Art 10(9)	Full	Strategic conflict detection	5.4.1.7	
Article 10(10)	GM1(a) Art 10(10)	Full Conditional	Constraint processing	5.8.2.3	Only if dynamic airspace restrictions and limitations are distributed as constraints.
	GM1(b) Art 10(10)	Full Conditional	Constraint processing	5.8.2.1 5.8.2.4	Only if dynamic airspace restrictions and limitations are distributed as constraints.
	AMC2 Art 4	Full Conditional	Constraint processing	5.8.2.4	Only if dynamic airspace restrictions and limitations are distributed as constraints.

ASTM F3548-21					
Requirement		**Coverage**	**Capability(ies)[6]**	**Relevant standard provisions**	**Remarks**
	GM1(f) Art 4 | from "*The ATC unit will then publish*" to "*newly published restriction*"	Full Conditional	Constraint processing	1.12.4 5.8.2.4	Only if dynamic airspace restrictions and limitations are distributed as constraints.
	GM1(g) Art 4 | first sentence	Full Conditional	Constraint processing	1.12.4 5.8.2.4	Only if dynamic airspace restrictions and limitations are distributed as constraints.
	GM2(a) Art 10(10)	Full	Strategic conflict detection	5.4.2.4 5.4.2.6 5.4.2.8 5.4.2.10	
	GM2(c) Art 10(10) | up to the last sentence	Full	Strategic conflict detection	4.4.4.5	
	GM2(c) Art 10(10) | last sentence	Full Conditional	Conformance monitoring for situational awareness	4.2.11 4.4.4.3 5.6.5.1	Conditional if the conformance monitoring service is required.
	GM2(d) Art 10(10)	Full	Strategic conflict detection	4.4.4.5	While ASTM F3548-21 does not have an equivalent state to 'withdrawn', the 'ended' state can be used here to fulfil the intent.

3.13.3.4 Requirements partially addressed

This subsection provides the list of elements of ASTM F3548-21 that need to be tailored and/or complemented before being proposed as a MoC for the UAS flight authorisation service requirements or a part thereof.

ASTM F3548-21					
Requirement		**Coverage**	**Capability(ies)**	**Relevant standard provisions**	**Remarks**
Article 10(1)	AMC1(b) Art 10(1)	Partial	Strategic conflict detection	5.9.2.11	ASTM F3548-21 only logs those UAS flight authorisation requests that are rejected due to conflicts.
Article 10(2)(c)	AMC1 Art 10(2)(c) GM1 Art 10(2)(c)	Partial	Strategic conflict detection	5.4 5.9	ASTM F3548-21 provides reasons for rejection when it is related to conflicts with other operational intents. Note: the most likely expected reason for rejection is expected to be related to priority.
Article 10(5)	GM1(a) Art 10(5)	Partial Conditional	Constraint processing	5.8.2.1	If U-space airspace information is provided in the form of constraints, ASTM F3548-21 can provide the information to the UAS operator but cannot reject the flight authorisation.
	AMC1(c) Art 10(5)	Partial Conditional	Constraint processing	5.8.2.4	If U-space airspace information is provided in the form of constraints, ASTM F3548-21 can provide the information to the UAS operator but cannot reject the flight authorisation.
	AMC1(f) Art 10(5) | last paragraph	Partial	Strategic conflict detection	5.4.2.18	ASTM F3548-21 provides reasons for rejection when rejection is related to conflicts with other operational intents.

ASTM F3548-21					
Requirement		**Coverage**	**Capability(ies)**	**Relevant standard provisions**	**Remarks**
					It allows the USSP to have awareness of conflicts to be able to support planning of alternatives.
Article 10(7)	AMC1(e) Art 10(2)(a);(b)	Partial Conditional	Constraint processing	5.8.2.4	If U-space airspace information is provided in the form of constraints, ASTM F3548-21 can provide the information to the UAS operator but cannot reject the flight authorisation.
	AMC1(f) Art 10(2)(a);(b) GM(1)(e) Art 10(2) | No-fly zone deconfliction GM1(d) Art 10(2) | No-fly zone deconfliction	Partial Conditional	Constraint processing	5.8.2.4	If U-space airspace information is provided in the form of constraints, ASTM F3548-21 can provide the information to the UAS operator but cannot reject the flight authorisation.
	GM1(a) Art 10(7)	Partial Conditional	Constraint processing	5.8.2.4	If U-space airspace information is provided in the form of constraints, ASTM F3548-21 can provide the information to the UAS operator but cannot reject the flight authorisation.
Article 10(10)	GM1(f) Art 4 | UAS flight authorisation cancelation or amendment	Partial Conditional	Constraint processing	5.8.2.4	If U-space airspace information is provided in the form of constraints, ASTM F3548-21 can provide the information to the UAS operator but cannot reject the flight authorisation.

ASTM F3548-21					
Requirement		**Coverage**	**Capability(ies)**	**Relevant standard provisions**	**Remarks**
	GM2(b) Art 10(10) | New dynamic airspace restriction / limitation	Partial Conditional	Constraint processing	5.8.2.4	If U-space airspace information is provided in the form of constraints, ASTM F3548-21 can provide the information to the UAS operator but cannot reject the flight authorisation.
	GM2(b) Art 10(10) | UAS flight authorisation change acknowledgement request	Partial	Strategic conflict detection	5.2.6.5	F3548-21 provides user notification but does not request acknowledgment.

3.13.3.5 Requirements not covered

ASTM F3548-21		
Requirement		**Rationale**
Article 10	GM1(f) Art 10	Background information
Article 10(1)	GM1(c) Art 10	Background information
	AMC1(a)(1) Art 10	No interoperability requirement – beyond standard's scope
	AMC1(a)(2) Art 10	No interoperability requirement – beyond standard's scope
	AMC1(a)(3) Art 10	The operational intent ID in the API specification may be set to match the unique authorisation number but this is not required by the standard. If the USSP uses the operational intent ID as the unique authorisation number, the standard supports this AMC through Section 5.9 on Logging.
	AMC2 Art 10	No interoperability requirement – beyond standard's scope
	GM2 Art 10(5)	No interoperability requirement – beyond standard's scope
	AMC1(c) Art 10(7) GM1(b) Art 10(7)	No interoperability requirement – beyond standard's scope
	GM1(c) Art 10(7)	UAS operator requirement – beyond standard's scope
	GM1 Art 10(1)	No interoperability requirement – beyond standard's scope
Article 10(2)(a)	AMC1(a) Art 10(2)(a);(b)	No interoperability requirement – beyond standard's scope
	AMC1(c) Art 10(2)(a);(b)	No interoperability requirement – beyond standard's scope
	AMC1(d) Art 10(2)(a);(b)	No interoperability requirement – beyond standard's scope
Annex IV	GM1(a)(1) Annex IV	No interoperability requirement – beyond standard's scope
	GM1(a)(2a) Annex IV	No interoperability requirement – beyond standard's scope
	GM1(a)(2b) Annex IV	No interoperability requirement – beyond standard's scope

ASTM F3548-21		
Requirement		**Rationale**
	GM1(a)(4a) Annex IV	No interoperability requirement – beyond standard's scope
	GM1(a)(4b) Annex IV	No interoperability requirement – beyond standard's scope
	GM1(a)(4c) Annex IV	No interoperability requirement – beyond standard's scope
	GM1(c) Annex IV	Background information
	GM1(a)(6) Annex IV	No interoperability requirement – beyond standard's scope
	GM1(a)(7) Annex IV	No interoperability requirement – beyond standard's scope
	GM1(a)(8) Annex IV	No interoperability requirement – beyond standard's scope
	GM1(a)(9) Annex IV	No interoperability requirement – beyond standard's scope
	GM1(a)(10a) Annex IV	No interoperability requirement – beyond standard's scope
	GM1(a)(10b) Annex IV	No interoperability requirement – beyond standard's scope
Article 10(2)(b)	AMC1(g) Art 10(2)(a);(b) | second paragraph	ASTM F3548-21 does not require strategic coordination for off-nominal 4D volumes – beyond standard's scope
	GM1(f) Art 10(2)	Background information
Article 10(2)(c)	GM1(a) Art 10	Background information
	GM1(b) Art 10(2)(c)	Background information
Article 10(2)(d)	GM1(c) Art 10	Background information
	GM1 Art 10(2)(d)	Background information
Article 10(3)	AMC1 Art 10(3)	No interoperability requirement – beyond standard's scope
	GM1 Art 10(3)	No interoperability requirement – beyond standard's scope
Article 10(5)	GM1(d) Art 10	Background information / No interoperability requirement

ASTM F3548-21		
Requirement		**Rationale**
	GM1(b) Art 10(5)	Background information
	GM1(c) Art 10(5)	No interoperability requirement – beyond standard's scope
	AMC1(a) Art 10(5)	No interoperability requirement – beyond standard's scope
	AMC1(b) Art 10(5) GM2 Art 10(5)	No interoperability requirement – beyond standard's scope
	AMC1(d) Art 10(5)	No interoperability requirement – beyond standard's scope
	AMC1(f)(1) Art 10(5) GM1(d) Art 10(5)	Crewed air traffic – beyond standard's scope
	AMC1(f)(2) Art 10(5) | Non-cooperative drones	Non-cooperative drones – beyond standard's scope
	AMC1(f)(3) Art 10(5)	Crewed air traffic – beyond standard's scope
	GM1(e) Art 10(5)	ASTM F3548-21 does not include a time-out period for operational intent activation – beyond standard's scope
Article 10(7)	AMC2 Art 10(2)(a);(b) | second paragraph	No interoperability requirement – beyond standard's scope
Article 10(8)	AMC1 Art 10(8)	Background information
Article 10(9)	AMC1(c) Art 10(9)	No interoperability requirement – beyond standard's scope
Article 10(10)	AMC1(a) Art 10(10)	Crewed air traffic – beyond standard's scope
	AMC1(b) Art 10(10)	Crewed air traffic – beyond standard's scope
	GM1(f) Art 4 | DAR initiation by ATC unit	Background information
	AMC3 Art 4	ATC notification – beyond standard's scope
	GM1(g) Art 4	ATC notification – beyond standard's scope
	GM1(i) Art 4	Background information

ASTM F3548-21		
Requirement		**Rationale**
	GM2(b) Art 10(10) | manned aircraft traffic	Crewed air traffic – beyond standard's scope
	GM2(b) Art 10(10) | non-cooperative drones	Non-cooperative drones – beyond standard's scope
Article 10(11)	AMC1(a) Art 10(11)	No interoperability requirement – beyond standard's scope
	AMC1(b) Art 10(11) GM1(a) Art 10(11)	No interoperability requirement – beyond standard's scope
	AMC1(c) Art 10(11)	No interoperability requirement – beyond standard's scope
	GM1(b) Art 10(11)	No interoperability requirement – beyond standard's scope
	GM1(c) Art 10(11)	No interoperability requirement – beyond standard's scope
	GM1(d) Art 10(11)	No interoperability requirement – beyond standard's scope

3.14 ASTM F3600-22

3.14.1 Introduction

The objective of this section is to present the outcome of the preliminary high-level assessment and subsequent detailed technical assessment of *ASTM F3600-22. Standard Guide for Unmanned Aircraft System (UAS) Maintenance Technician Qualification* conducted in accordance with the criteria and methodology developed by SHEPHERD to evaluate the standard's suitability in fulfilling the following requirements:

- SORA v2.5 OSOs:
    - OSO#03 Integrity & Assurance, SAIL I to VI – Low (L) to High (H)

It identifies and substantiates the list of recommended sections, subsections, paragraphs, or combination thereof of ASTM F3600-22 that have been deemed suitable and, hence, may be used as a basis for a means of compliance (MoC) for the requirements or a part thereof. In the same manner, it also lists and provides clear justification for the elements of the standard that have been found not technically adequate and, thus, need to be tailored and/or complemented before being proposed as a MoC.

3.14.2 General remarks

ASTM F3600-22 is intended to be used for the assessment of competencies of qualified individuals who wish to certify as a UAS maintenance technician through a certification program.

This standard does not address OSO#03 Assurance Criterion#1. Consequently, ASTM F3600-22 has been analysed against the following requirements:

- OSO#03 Integrity; and
- OSO#03 Assurance Criterion#2.

The result of the assessment is that the recommended sections, as outlined in subsection 3.14.3 below, provide very low coverage of the retained OSO#03 requirements and, even if Tables 2 to 5 might be useful as an initial reference basis for maintenance technicians qualification in relation to the authorisation process required, their adoption would require considerable supplementary work for completeness.

Table 1 of the standard is not recommended to be adopted under the EASA framework because it provides a UAS classification system for technicians training that is not in line with the applicable EU regulatory framework.

For further details on the rationale for the sections that have been considered as 'N/A' being too high-level requirements or similar to the requirements, as well as the rationale for the recommended sections, refer to the detailed technical assessment.

3.14.3 Recommended sections

This subsection provides the list of recommended sections, subsections, paragraphs, or combination thereof of ASTM F3600-22 that may be used as a basis for a MoC for the requirements or a part thereof as identified in the detailed technical assessment.

ASTM F3600-22			
Requirement	**Related AMC & GM**	**Recommended section(s), subsection(s), paragraph(s), or combination thereof**	**Additional relevant information**
OSO#03	Integrity SAIL I to VI – Low (L) to High (H)	4 5	– These sections only partially address the following requirement: "*The maintenance staff is competent*", because complete training syllabi and recurrent training for maintenance technicians are not covered. – The adoption of these sections would require considerable supplementary work for full coverage.
OSO#03	Assurance SAIL I to VI – Low (L) to High (H)	4 5	– The classification system to train technicians on the knowledge necessary to maintain the UAS is addressed through a UAS classification system (Table 1) that is not in line with the EU regulatory framework. Three different levels of competence in the exam items are provided in Table 5. – These sections provide very low coverage of the requirements, even if Tables 2 to 5 are useful for an initial reference basis for maintenance technician qualification in relation to the authorisation process required. The adoption of these sections would require considerable supplementary work for full coverage.

3.14.4 Non-recommended sections

This subsection provides the list of elements of ASTM F3600-22 that need to be tailored and/or complemented before being proposed as a MoC for the requirements or a part thereof as identified in the detailed technical assessment.

ASTM F3600-22			
Section, subsection, or paragraph to be tailored / complemented	**Title / subject**	**Requirement**	**Required tailoring / complementing**
N/A			

3.15 C3 link spectrum & technology standards mapping

3.15.1 Introduction

The objective of this section is to present the outcome of the C3 link spectrum & technology standards mapping conducted by SHEPHERD to evaluate their relevance and effectiveness in fulfilling the following requirements:

- SORA v2.5 OSOs:
  - OSO#06, SAIL II to VI – Low (L) to High (H);
- EASA SC Light-UAS – Medium & High Risk provisions:
  - Light-UAS.2715;
  - Light-UAS.2720; and
  - Light-UAS.2730.

The mapping provides a comprehensive overview of available standards, accompanied by a concise summary of their content and, where relevant, an insightful analysis of the comparative differences.

3.15.2 General remarks

The evaluation of the various C3 link spectrum & technology standards within scope of the project was done in deviation from the SHEPHERD methodology. This decision stemmed from the acknowledgement that the suitability of C3 link spectrum & technology heavily depends on the intended ConOps. Consequently, it was determined that a detailed technical analysis would be more effectively carried out by UAS designers and/or manufacturers during the system's design phase. Meanwhile, SHEPHERD concentrated on compiling a comprehensive list of available standards, offering a concise overview of their content and, where relevant, providing an analysis of the comparative differences.

3.15.3 Evaluated standards

3.15.3.1 AW-Drones

Organisation	Standard	Title	Year
ASTM	F3002-14	Standard Specification for Design of the Command and Control System for Small Unmanned Aircraft Systems (sUAS)	2014
ASTM	F3298-19	Standard Specification for Design, Construction, and Verification of Lightweight Unmanned Aircraft Systems (UAS)	2019
ISO	ISO 21384-2:2021	Unmanned Aircraft Systems - Part 2: UAS components	2021
EUROCAE	ED-266	Guidance on Spectrum Access, Use, and Management for UAS	2020
IEEE	IEEE 802.15.3c-2009	Bluetooth technology	2009
IEEE	IEEE 802.11-2020	WIFI technology (2.4 GHz + 5 GHz Band)	2020
IEEE	IEEE 802.22-2017	Standard for Wireless regional area network (WRAN)	2017

3.15.3.2 Other

Organisation	Standard	Title	Year
CEN & ASD-STAN	prEN 4709-001:2021	Aerospace series – Unmanned Aircraft Systems – Part 001: Product requirements and verification.	2021

3.15.4 Standards not considered

3.15.4.1 Not yet published

Organisation	Standard	Title	Year
EUROCAE	ED-265	Minimum Operational Performance Standard for RPAS Command and Control Data Link (C-Band Satellite)	Draft – not yet published
EUROCAE	ED-400	Minimum Operational Performance Standard for UAS Communications by Cellular Networks	Draft – not yet published

3.15.4.2 Not fit for purpose

Organisation	Standard	Title	Year
RTCA	DO-362A	Command and Control (C2) Data Link Minimum Operational Performance Standards (MOPS) (Terrestrial)	2020

3.15.5 High-level assessment outcome

The assessment underscores that the viability of a C2 / C3 link spectrum & technology is highly tied to the specific ConOps it is meant to support. Furthermore, relevant standards for promising C3 link technologies such as satellite or cellular networks were not available at the time the evaluation was performed. However, the following conclusions could be drawn from the high-level assessment:

Standard	Relevance for OSO#06	Relevance for associated requirements
ASTM F3002-14	Compliance with ASTM F3002-14a leads to compliance with the link monitoring requirement. It does not, however, give precise design or performance criteria for the link itself.	SC Light-UAS.2720 Compliance with ASTM F3002-14a provides full coverage with Light-UAS.2720(a).
ASTM F3298-19	Compliance with ASTM F3298-19 will lead to partial compliance with the performance requirement.	N/A
ISO 21384-2:2021	ISO 21384-2:2021 does not provide enough technical details to be considered as a potential MoC.	N/A
EUROCAE ED-266	ED-266 is deemed extremely useful guidance through the complex landscape of spectrum access, use, and management for unmanned aircraft systems. It must be seen as a guidance and not as a technical standard.	SC Light-UAS.2715 Useful information on spectrum access management.
IEEE 802.15.3c-2009	N/A – technology deemed impractical due to limited range.	N/A
IEEE 802.11-2020	N/A – agreement with the ED-266 conclusion that WiFi is, in most cases, not a suitable technology for the reasons stated under '*Summary*'.	N/A
IEEE 802.22-2017	WRAN as a means for C3 could be a viable option for certain operations. Where this is the case, IEEE 802.22-2017 should be consulted for the design of the C3 system.	SC Light-UAS.2715 (a) IEEE 802.22-2017 provides nominal performance specifications for the operation modes. Its adequacy needs to be determined by the manufacturer / operator. Adequate performance targets should be defined. (b) IEEE 802.22 provides guidance for message correct sequencing and identifying.

Standard	Relevance for OSO#06	Relevance for associated requirements
		SC Light-UAS.2730 (a) IEEE 802.22-2017 addresses link security (b) IEEE 802.22-2017 addresses authentication

3.15.6 Additional information

3.15.6.1 EASA's proposed MoC OSO#06 – SAIL III

While not directly related to the SHEPHERD project, it is worth noting that EASA, on December 18, 2023, released for public consultation the SAIL III OSO#06 MoC, which proposed means to "*determine that the C2 performance is adequate to safely carry out the intended operation*" and guidance on how to "*provide evidence that the remote pilot has means to continuously monitor the C2 performance and ensure that minimum performances continue to be achieved*", as well as additional test guidelines.

3.15.6.2 Other potentially useful standards that were not assessed

Organisation		Title	Status
JARUS	WG5	White paper – Use of mobile networks to support UAS operations	Published
ACJA (GUTMA - GSMA)	WG1	Aviation coordination with 3GPP	Under development
ACJA (GUTMA - GSMA)	WG2	Network Coverage Service Definition v1.0	Published but superseded by the document below
ACJA (GUTMA - GSMA)	WG2	Interface for Data Exchange between MNOs and the UAS Ecosystem (v2.0)	Published
ACJA (GUTMA - GSMA)	WG2	Reference Method for assessing Cellular C2 Link Performance and RF Environment Characterization for UAS	Published
ACJA (GUTMA - GSMA)	WG3	LTE Aerial Profile version 1.00	Published
ACJA (GUTMA - GSMA)	WG4	MOPS / MASPS for cellular C2	Under development

3.16 IEC 62133-2:2017 + AMD1:2021

3.16.1 Introduction

The objective of this section is to present the outcome of the preliminary high-level assessment and subsequent detailed technical assessment of *IEC 62133-2:2017 + AMD1:2021. Secondary cells and batteries containing alkaline or other non-acid electrolytes – Safety requirements for portable sealed secondary cells, and for batteries made from them, for use in portable applications – Part 2: Lithium systems* conducted in accordance with the criteria and methodology developed by SHEPHERD to evaluate the standard's suitability in fulfilling the following requirements:

- EASA SC Light-UAS – Medium & High Risk provisions:
    - Light-UAS.2430.

It identifies and substantiates the list of recommended sections, subsections, paragraphs, or combination thereof of IEC 62133-2:2017 + AMD1:2021 that have been deemed suitable and, hence, may be used as a basis for a means of compliance (MoC) for the requirements or a part thereof. In the same manner, it also lists and provides clear justification for the elements of the standard that have been found not technically adequate and, thus, need to be tailored and/or complemented before being proposed as a MoC.

3.16.2 General remarks

The detailed technical assessment is presented considering the various sections treated as a whole (except Annex A) since the same remarks and conclusions have been reached.

One has to keep in mind that this standard is specific to off-the-shelf batteries and not directly related to the risk-based approach of the UAS regulations.

Considering the complexity and amount of required testing, it has been found that this standard would be more suitable to high risk (SAIL V & VI) operations than to medium risk (SAIL III & IV) operations.

For further details on the rationale for the sections that have been considered as 'N/A' being too high-level requirements or similar to the requirements, as well as the rationale for the recommended sections, refer to the detailed technical assessment.

3.16.3 Recommended sections

This subsection provides the list of recommended sections, subsections, paragraphs, or combination thereof of IEC 62133-2:2017 + AMD1:2021 that may be used as a basis for a MoC for the requirements or a part thereof as identified in the detailed technical assessment.

As stated in 3.16.2 above, the various sections have been handled as a whole since the same remarks and conclusions have been reached; altogether, compliance with the criteria set forth in the sections outlined below should provide reasonable assurance that the intent of the requirements of Light-UAS.2430(a)(1)&(b) in terms of safe functioning of supporting systems supplied by the batteries and in terms of their design and installation is met.

IEC 62133-2:2017 + AMD1:2021			
Requirement	**Related AMC & GM**	**Recommended section(s), subsection(s), paragraph(s), or combination thereof**	**Additional relevant information**
Light-UAS.2430(a)(1)&(b)	SAIL V & VI (High risk)	4 5 6 7 8 9 10	Light-UAS.2430(a)(2) is not addressed.
Light-UAS.2430(b)(4)	SAIL V & VI (High risk)	Annex A	Exclusively addressing Light-UAS.2430(b)(4)

3.16.4 Non-recommended sections

This subsection provides the list of elements of IEC 62133-2:2017 + AMD1:2021 that need to be tailored and/or complemented before being proposed as a MoC for the requirements or a part thereof as identified in the detailed technical assessment.

IEC 62133-2:2017 + AMD1:2021			
Section, subsection, or paragraph to be tailored / complemented	**Title / subject**	**Requirement**	**Required tailoring / complementing**
N/A			

As indicated in subsection 3.16.2, the standard has been recommended for Light-UAS.2430, except point Light-UAS.2430(a)(2), for SAIL V & VI only. Alternative MoC would need to be established to more suitably address SAIL III & IV and associated range of UAS applications.

3.17 ISO 21384-2:2021

3.17.1 Introduction

The objective of this section is to present the outcome of the preliminary high-level assessment and subsequent detailed technical assessment of *ISO 21384-2:2021. Unmanned aircraft systems – Part 2: UAS components* conducted in accordance with the criteria and methodology developed by SHEPHERD to evaluate the standard's suitability in fulfilling the following requirements:

- SORA v2.5 OSOs:
  - OSO#06 Integrity, SAIL I to VI – Low (L) to High (H); and
  - OSO#13 Integrity, SAIL I to VI – Low (L) to High (H).

- EASA SC Light-UAS – Medium & High Risk provisions:
  - Light-UAS.2250(c); and
  - Light-UAS.2430.

It identifies and substantiates the list of recommended sections, subsections, paragraphs, or combination thereof of ISO 21384-2:2021 that have been deemed suitable and, hence, may be used as a basis for a means of compliance (MoC) for the requirements or a part thereof. In the same manner, it also lists and provides clear justification for the elements of the standard that have been found not technically adequate and, thus, need to be tailored and/or complemented before being proposed as a MoC.

3.17.2 General remarks

ISO 21384-2:2021 proposes a number of requirements for the design and manufacture of uncrewed aircraft systems (UAS), including the uncrewed aircraft (UA), remote pilot station (RPS), datalinks, payloads, and associated support equipment.

The following requirements are not addressed by ISO 21384-2:2021, as outlined in the preliminary high-level assessment:

- OSO#06 Integrity, SAIL I to VI – Low (L) to High (H); and
- OSO#13 Integrity, SAIL I to VI – Low (L) to High (H).

For further details on the rationale for the sections that have been considered as 'N/A' being too high-level requirements or similar to the requirements, as well as the rationale for the recommended sections, refer to the detailed technical assessment.

3.17.3 Recommended sections

This subsection provides the list of recommended sections, subsections, paragraphs, or combination thereof of ISO 21384-2:2021 that may be used as a basis for a MoC for the requirements or a part thereof as identified in the detailed technical assessment.

ISO 21384-2:2021			
Requirement	**Related SAIL Integrity / assurance**	**Recommended section(s), subsection(s), paragraph(s), or combination thereof**	**Additional relevant information**
Light-UAS.2250(c)	SAIL III to VI (Medium & High risk)	6.1 6.5	– Partial coverage; clarifications / appropriate interpretations should be added regarding the expression "*having an important bearing on safety in operations*" used in Light-UAS.2250(c) to identify which design and parts the recommended subsection of ISO 21284-2 should be applied to. NOTE: In the framework of the 'specific' category of UAS operations, when the operational authorisation is based upon compliance with AMC1 to Article 11 (i.e. the SORA OSOs), OSO#04 is classified as 'Not Required' (i.e. not required to show compliance to the competent authority) for SAIL III, meaning that such a SC Light-UAS design requirement may also not be required to be demonstrated to the competent authority.
Light-UAS.2430	SAIL III to VI (Medium & High risk)	9.1	– Partial coverage; Section 9.1 does not address Light-UAS.2430(a)(2) related to Remote Crew information and Light-UAS.2430(b)(4) related to minimising hazard during ground handling.

ISO 21384-2:2021			
Requirement	**Related SAIL Integrity / assurance**	**Recommended section(s), subsection(s), paragraph(s), or combination thereof**	**Additional relevant information**
			– With regard to IEC 62133-2:2017+AMD1:2021, refer to the separate SHEPHERD's assessment. Alternative standards should also be allowed in a future MoC. – See previous note regarding SAIL III applicability. – Note also that Light-UAS.2430(b)(1) requires design considerations for the battery storage that are not explicitly addressed in Section 9.1 (especially probable failures should not affect essential systems which would require additional MoC / guidance on how to ensure this).
Light-UAS.2529	SAIL III to VI (Medium & High risk)	10.2.3 10.5.1 10.5.2 10.5.3 10.5.4 10.5.5 10.6.1 10.6.2 10.6.3	Partial coverage; the recommended sections offer valuable insights into diverse navigation technologies and sensors. However, a crucial aspect missing is the inclusion of performance requirements, particularly the accuracy of these systems. Other standards such as the ASTM WK75923 would be a beneficial addition.

3.17.4 Non-recommended sections

This subsection provides the list of elements of ISO 21384-2:2021 that need to be tailored and/or complemented before being proposed as a MoC for the requirements or a part thereof as identified in the detailed technical assessment.

ISO 21384-2:2021			
Section, subsection, or paragraph to be tailored / complemented	**Title / subject**	**Requirement and SAIL**	**Required tailoring / complementing**
10.3	Flight control actuators	Light-UAS.2250 SAIL III to VI (Medium & High risk)	Provision 10.3(a) provides sound criteria for flight control actuators (which have an important bearing on safety). However, this section is deemed more appropriate for showing compliance with Light-UAS.2300 EMI criteria covered under other SC Light-UAS requirement(s) (e.g. Subpart F)
11.2	Antenna design	Light-UAS.2250(c) SAIL III to VI (Medium & High risk)	Provisions 11.2.(a),(b)&(c) constitute also sound criteria specifically for Antenna Design but are not related to Light-UAS.2250(c). RPS alerting requirements in provision 11.2(d) are not directly related to Light-UAS.2250(c).

3.18 ISO 21384-3:2023

3.18.1 Introduction

The objective of this section is to present the outcome of the preliminary high-level assessment and subsequent detailed technical assessment of *ISO 21384-3:2023. Unmanned aircraft systems – Part 3: Operational procedures* conducted in accordance with the criteria and methodology developed by SHEPHERD to evaluate the standard's suitability in fulfilling the following requirements:

- SORA v2.5 OSOs:
  - OSO#01 Integrity & Assurance, SAIL II to VI – Low (L) to High (H);
  - OSO#07 Integrity, SAIL I to VI – Low (L) to High (H);
  - OSOs#08+ Integrity & Assurance, SAIL I to VI – Low (L) to High (H);
  - OSO#13 Integrity & Assurance, SAIL I to VI – Low (L) to High (H);
  - OSO#19 Integrity & Assurance Criterion#1, SAIL IV to VI – Medium (M) & High (H); and
  - OSO#23 Integrity & Assurance Criterion#2, SAIL III & IV – Medium (M).

It identifies and substantiates the list of recommended sections, subsections, paragraphs, or combination thereof of ISO 21384-3:2023 that have been deemed suitable and, hence, may be used as a basis for a means of compliance (MoC) for the requirements or a part thereof. In the same manner, it also lists and provides clear justification for the elements of the standard that have been found not technically adequate and, thus, need to be tailored and/or complemented before being proposed as a MoC.

3.18.2 General remarks

ISO 21384-3:2023 proposes a number of requirements for UAS operators at the organisational and procedural levels. However, the majority of these requirements are presented at the same level as existing regulatory and AMC & GM provisions, making them not suitable as new compliance means. Further guidance, criteria, or best practices would be needed to serve that purpose.

With the above in mind, and in accordance with the preliminary high-level assessment, the following requirements are not covered by this standard:

- OSO#01 Assurance;
- OSO#07 Integrity & Assurance;
- OSOs#08+ Integrity Criterion#2;
- OSOs#08+ Assurance Criteria#1&#2;
- OSO#13 Integrity;
- OSO#19 Integrity & Assurance Criterion#1; and
- OSO#23 Integrity & Assurance Criterion#2.

For further details on the rationale for the sections that have been considered as 'N/A' being too high-level requirements or similar to the requirements, as well as the rationale for the recommended sections, refer to the detailed technical assessment.

3.18.3 Recommended sections

This subsection provides the list of recommended sections, subsections, paragraphs, or combination thereof of ISO 21384-3:2023 that may be used as a basis for a MoC for the requirements or a part thereof as identified in the detailed technical assessment.

ISO 21384-3:2023			
Requirement	**Related SAIL Integrity / assurance**	**Recommended section(s), subsection(s), paragraph(s), or combination thereof**	**Additional relevant information**
OSO#01	Integrity SAIL IV to VI – High (H)	5.1 5.3.4	– 5.1 introduces the need for an SMS and an ISMS, required to obtain a LUC as per AMC1(f)(i) UAS.LUC.010(2)(a) and associated AMC & GM – 5.3.4 defines the duties and responsibilities for the SECO / security manager in the same manner as AMC1(b) UAS.LUC.030(2) does for the safety manager. – The combination of these two sections provides very low coverage.
OSOs#08+	Integrity Criterion#1 SAIL I to VI – Low (L) to High (H)	9.3.1	– 9.3.1 only for pre-flight inspection (procedure). – It provides very low coverage.
OSO#13	Assurance SAIL I to VI – Low (L) to High (H)	9.5.3.1 9.5.3.2 9.5.3.3 9.5.3.6 9.5.3.7 9.5.3.8	– Only for C2 link communication service. – Efforts are needed to integrate the proposed provisions into an SLA or a similar official commitment. – Adaptations to the particular UAS operator – C2CSP case are deemed necessary. – The combination of these six sections do not provide full coverage.

3.18.4 Non-recommended sections

This subsection provides the list of elements of ISO 21384-3:2023 that need to be tailored and/or complemented before being proposed as a MoC for the requirements or a part thereof as identified in the detailed technical assessment.

ISO 21384-3:2023			
Section, subsection, or paragraph to be tailored / complemented	**Title / subject**	**Requirement and SAIL**	**Required tailoring / complementing**
5.1	Safety and security – General	OSO#01 Integrity SAIL II – Low (L)	The implementation of an SMS or ISMS is not proportionate to SAIL II operators.
		OSO#01 Integrity SAIL III – Medium (M)	The implementation of an SMS or ISMS is not proportionate to SAIL III operators.
5.3.4	Tasks of the Security Officer (SECO)	OSO#01 Integrity SAIL II – Low (L)	A SECO or security manager is only required to obtain a LUC, as per AMC1(f)(i) UAS.LUC.010(2), which is not deemed proportionate to SAIL II operators.
		OSO#01 Integrity SAIL III – Medium (M)	A SECO or security manager is only required to obtain a LUC, as per AMC1(f)(i) UAS.LUC.010(2), which is not deemed proportionate to SAIL III operators.
9.2	Operational plan – Flight planning	OSOs #08+ Integrity SAIL I to VI – Low (L) to High (H)	– No clear distinction is made between operational planning and flight planning. – No guidance, criteria, or best practices are provided.

3.19 ISO 23629-7:2021

3.19.1 Introduction

The objective of this section is to present the outcome of the preliminary high-level assessment and subsequent detailed technical assessment of *ISO 23629-7:2021. UAS Traffic Management (UTM) Part 7 – Data Model for Spatial Data* conducted in accordance with the criteria and methodology developed by SHEPHERD to evaluate the standard's suitability in fulfilling the following requirements:

- U-space IR (EU) 2021/664 requirements:
    - Article 9 on the geo-awareness service and its associated set of AMC & GM published by EASA under ED Decision 2022/022/E on 20 December 2022.

The following subsections summarise the assessment results and indicate the geo-awareness service requirements that are:

- fully addressed;
- partially addressed; and
- not covered;

by ISO 23629-7:2021.

3.19.2 General remarks

No standard sections, subsections, or paragraphs of this standard have been found suitable for showing full compliance with:

- GM1(c) Article 9 – General; the standard does not address the use of the geo-awareness service by the UAS flight authorisation service for the identification of overlaps of UAS flight authorisation requests with the relevant operational and airspace restrictions; and

- AMC1 Article 9(1) – Information, GM1 Article 9(2) – Timeliness, and AMC1 Article 9(2) – Timeliness; the standard does not address the timeliness of the geo-awareness service information. Therefore, ISO 23629-7:2021 cannot provide full coverage of Article 9(2).

It is recommended that:

- the definition of certain attributes contained in Section 4.4.2 – *Attributes of airspace* are reviewed and amended as necessary to ensure compatibility with ED-269 and ED-318 standards; and

- Section 4.3.3 – *Attributes of temporal obstacle* is reviewed and amended as necessary to specify that not all short-term obstacles trigger airspace restrictions relevant for the geo-awareness service.

While Annex A does not contain requirements, it is deemed helpful to understand the examples provided in relation to the recommended standard sections.

For further details on the rationale for the recommended sections as well as for the geo-awareness service requirements beyond the scope of the standard, refer to the detailed technical assessment.

3.19.3 Requirements fully addressed

No ISO 23629-7:2021 standard sections, subsections, or paragraphs have been found suitable for showing full compliance with the geo-awareness service requirements or a part thereof.

3.19.4 Requirements partially addressed

This subsection provides the list of elements of ISO 23629-7:2021 that need to be tailored and/or complemented before being proposed as a MoC for the geo-awareness service requirements or a part thereof as identified in the detailed technical assessment.

ISO 23629-7:2021				
Requirement		**Coverage**	**Relevant standard provisions**	**Remarks**
Article 9	GM1(b) Art 9	Partial	1	Level of accuracy and performance requirements are not addressed
Article 9(1)(a)	N/A	Partial Conditional	4.2.2 4.2.3 4.3.2 4.3.3 4.4.2 4.4.4	<u>Section 4.2.2</u> – The characteristics of the takeoff and landing area(s) are not considered part of the geo-awareness information for which USSPs must be certified under the geo-awareness service (i.e., outside of the scope of the current U-space regulation). They should be rather associated with general geospatial data, where some of the attributes proposed may not be deemed necessary (e.g., geoid undulation at elevation, magnetic declination, resources). <u>Section 4.2.3</u> – The general characteristics of land should be rather seen as general geospatial data, where some of the attributes proposed may not be deemed necessary (e.g. geoid undulation at elevation, magnetic declination). <u>Sections 4.3.2 & 4.3.3</u> – Conditional coverage; only for (static and temporal) obstacles triggering operational or airspace restrictions; otherwise, they should be rather

				associated with general geospatial data, outside of the scope of the current U-space regulation. – Static and temporal obstacle data should be merged under a single package. – 'Type of height' should be updated to 'height reference' to avoid ambiguity. <u>Section 4.4.2</u> – 'Type of height' should be modified to 'height reference' to avoid ambiguity; – 'Administrator' entity should be clearly defined; – 'UTM services' should be understood as the 6 U-space services (4+2) laid down in the U-space Regulation; – Compatibility with ED-269 and ED-318 standards should be ensured. <u>Section 4.4.4</u> – The proposed CNS attributes are not considered part of the geo-awareness information for which USSPs must be certified under the geo-awareness service.
Article 9(1)(c)	N/A	Partial Conditional	4.3.3	– Conditional coverage; only for temporal obstacles triggering temporary operational or airspace restrictions; otherwise, they should be rather associated with general geospatial data, outside of the scope of the current U-space regulation. – 'Type of height' should be updated to 'height reference' to avoid ambiguity.
Article 9(2)	GM2 Art 9(2)	Partial	All	– 'Identifier' attribute might include the version number; – ‘Generate time' attribute can be referenced to the time of update.

3.19.5 Requirements not covered

ISO 23629-7:2021		
Requirement		**Rationale**
Article 9	GM1(a) Art 9	Background information
	GM1(c) Art 9	Flight authorisation service interaction – beyond standard's scope
Article 9(1)(b)	N/A	Section 4.4.2 of the standard is not recommended
Article 9(1)	AMC1 Art 9(1)	Timeliness – beyond standard's scope
Article 9(2)	AMC1 Art 9(1)	Timeliness – beyond standard's scope
	GM1 Art 9(1)	Timeliness – beyond standard's scope

3.20 RTCA DO-366A

3.20.1 Introduction

The objective of this section is to present the outcome of the technical assessment of *RTCA DO-366A. Minimum Operational Performance Standards (MOPS) for Air-to-Air Radar for Traffic Surveillance* conducted to evaluate the standard's suitability in fulfilling the following requirements:

- SORA Tactical Mitigation Performance Requirements (TMPRs) ARC-d, as per Annex D.

3.20.2 General remarks

The DO-366 MOPS for Air-to-Air Radar (ATAR) for Traffic Surveillance is the companion MOPS of DO-365 and DO-365A; its latest version, DO-366A, being companion to DO-365B and later revisions. DO-366A has been written by RTCA SC-228 as a mini-MOPS containing requirements related to air-to-air radars to complement DO-365B. Consequently, it can be considered as a system meeting RTCA SC-228 requirements, as required per SORA Annex D, though only usable with a DO-365 equipment. For this reason, this standard has not been subject to a detailed assessment.

As noted in the SHEPHERD's P1 assessment deliverable '*DO-365A & UAS DAA standards Mapping*', the corresponding TSO-C212A is currently in work. Regarding usage in Europe, the air-to-air radar described in DO-366A needs to use appropriate and authorised spectrum, as defined by a future EASA ETSO or by local authorities.

3.20.3 Recommended sections

All sections are recommended, although only in support of a DO-365 compliant system and as long as the ConOps fits DO-398 (DAA OSED), as explained in the following subsection.

3.20.4 Sections to be tailored / complemented

DO-366A describes a high-power air-to-air radar (ATAR) to answer a concept of operations focused on medium to large sized fixed wing aircraft (DO-398). This standard will need tailoring before being applied to small UAS and rotorcraft. Additionally, considering performances of current technologies, it is expected that such ATAR will behave poorly at low altitude.

The next revision of the standard (DO-366B) is planned to include requirements for a low size, weight and power (SWaP) class of ATAR. This revision will be developed jointly by RTCA SC-228 and EUROCAE WG-105 (timeline still to be defined).

Regarding evaluations of DAA systems, those targeting low SWaP platforms and uniquely based on DO-366A ATAR as non-cooperative sensors will need to be carefully evaluated considering that this type of sensor might not be a realistic representation of what a low SWaP platform can equip and considering its performances at low altitude.

3.21 RTCA DO-386

3.21.1 Introduction

The objective of this section is to present the outcome of the preliminary high-level assessment and subsequent detailed technical assessment of *RTCA DO-386. Vol I Minimum Operational Performance Standards for Airborne Collision Avoidance System Xu (ACAS Xu)* conducted in accordance with the criteria and methodology developed by SHEPHERD to evaluate the standard's suitability in fulfilling the following requirements:

- SORA tactical mitigation performance requirements (TMPRs) – ARC-d, as per Annex D.

It identifies and substantiates the list of recommended sections, subsections, paragraphs, or combination thereof of RTCA DO-386 that have been deemed suitable and, hence, may be used as a basis for a means of compliance (MoC) for the requirements or a part thereof. In the same manner, it also lists and provides clear justification for the elements of the standard that have been found not technically adequate and, thus, need to be tailored and/or complemented before being proposed as a MoC.

3.21.2 General remarks

As indicated in SORA Annex D, requirements from SC-228 DAA MOPS (DO-365) can be considered as the requirements for DAA in ARC-d. For this reason, the DO-386 standard is evaluated in comparison to DO-365.

A detailed comparison '*Requirements Management and Justification Matrix (RMJM)*' has been performed by RTCA SC-147 between DO-386 and DO-365A, available upon request to RTCA. However, the RMJM is not used in this work since the focus of SHEPHERD is on DO-365B.

A high-level comparison, between DO-386 and DO-365B, is included in Annex K of the latter, though it only covers the STM (surveillance module) and TRM (alerting and decision module); this is due to the fact that sensors, C2 link, command execution, and display are considered as out of the scope of DO-386.

Consequently, SHEPHERD's assessment is split into two parts: first, an assessment based on DO-365B Annex K for the STM (surveillance module) and TRM (alerting and decision module); secondly, an assessment of the remaining items.

The DO-365B Annex K splits the STM and TRM requirements into three different categories:

- Category 1 requirements are coming from DO-386 and pushed into DO-365B as requirements specific to the DAA class 3 (ACAS Xu).
- Category 2 requirements are defined in DO-386 and meet the intent or supersede the requirements from DO-365B. Explanations justifying the differences and how they meet DO-365B requirements form the bulk of Annex K (K.1 to K.24).
- Category 3 are requirements where DO-386 does not comply with DO-365B. Exemptions have been agreed on between the working groups from both documents (respectively SC-147 and SC-228). The agreements are detailed in Annex K.25, K.26, K.27.

Since Category 1 and Category 2 requirements already meet the DO-365B, no further assessment is provided for them. To help the reader, the table listing them is included in subsection 3.21.3 below.

The Annex K assessment is focused on Category 3 requirements that do not comply with DO-365B. To help the reader, the table listing them is included in subsection 3.21.4 below.

The remaining items have been assessed in the SHEPHERD's detailed assessment and the outcomes have been added to the related tables.

NOTES

- The introductory sections, titles without associated text and more generally sections unrelated to DO-365 requirements, or sections directly referring to an external standard, have been excluded from the detailed assessment, as indicated in the preliminary assessment. Additionally, Vol II of this standard has not been assessed since it is exclusively composed of the Julia code implementing the Vol I requirements along with its associated documentation.

- ACAS Xu will be included in TSO-C211a (Detect and Avoid Systems). This TSO is in 'section review' at the FAA (publication planned in 2022/23). The EU Validation is on-going in SESAR PJ13 Erica. As stated in DO-365B Annex K.2, the standards are written such that manufacturers of ACAS Xu will only have to prove compliance with DO-386.

- Regarding a possible ETSO, the system must first be validated using European data. However, the lack of low-level data for the European airspace calls first for an initiative to gather the appropriate data, and build an encounter model. Additionally, this standard needs to be used in conjunction with DO-366A, with the additional limitations described in the corresponding assessment (low altitude performance, spectrum limitations).

3.21.3 Recommended sections

The majority of the DO-386 standard may be considered as providing acceptable means of compliance with the requirements laid out by DO-365B. This paragraph provides the list of corresponding sections of DO-386.

The first columns list the requirements as expressed in the SORA, coming from DO-365B. The second column details the recommended section from DO-386. The thirds column indicates cases where ACAS Xu requirements are more conservative than the DO-365B ones. This applies to surveillance outlier detection, traffic position validation, and alert timings (category 2 requirements).

RTCA DO-386				
Requirements from DO-365B	**Recommended sections from DO-386**	**Requirement category**	**Additional relevant information**	**Assessment source**
2.2.1.3	2.2.3.12(.9) 2.2.3.12(.10.1) 2.2.5.3(.1) 2.2.5.5	N/A	SORA TMPR Detect	SHEPHERD
2.2.1.5	2.2.4 2.2.4.6(.4.2)	N/A	SORA TMPR Detect	SHEPHERD
2.2.2.1.1	As per DO-365B Annex K.2	2	DO-386 §2.2.3.12 §2.2.7	DO-365B Annex K
2.2.2.1.2	As per DO-365B Annex K.3	2	DO-386 §2.2.3.12.10.1 §2.2.5.5.14	DO-365B Annex K
2.2.2.1.3	As per DO-365B Annex K.4	2	N/A	DO-365B Annex K
2.2.2.1.4	As per DO-365B Annex K.5	2	N/A	DO-365B Annex K

RTCA DO-386				
Requirements from DO-365B	**Recommended sections from DO-386**	**Requirement category**	**Additional relevant information**	**Assessment source**
2.2.2.1.6	As per DO-365B Annex K.6	2	DO-386 §2.2.7	DO-365B Annex K
2.2.2.2.1	As per DO-365B Annex K.7	1	DO-386 §2.2.3.2.3 §2.2.5.1.4	DO-365B Annex K
2.2.2.2.1.1	2.2.3.12(.9) 2.2.5.1(.2) 2.2.5.1(.3) 2.2.5.1(.5) 2.2.5.3(.1) 2.2.5.4 2.2.5.5	N/A	SORA TMPR Detect	SHEPHERD
2.2.2.2.1.2	2.2.3.12(.9) 2.2.5.1(.5) 2.2.5.3(.1) 2.2.5.5	N/A	SORA TMPR Detect	SHEPHERD
2.2.2.2.1.3	2.2.3.12(.9) 2.2.5.3(.1) 2.2.5.5	N/A	SORA TMPR Detect	SHEPHERD
2.2.2.2.1.4	2.2.5.6	N/A	SORA TMPR Decide	SHEPHERD
2.2.2.2.1.5	2.2.5.1(.2) 2.2.5.3(.1)	N/A	SORA TMPR Detect	SHEPHERD

RTCA DO-386				
Requirements from DO-365B	**Recommended sections from DO-386**	**Requirement category**	**Additional relevant information**	**Assessment source**
	2.2.5.5			
2.2.2.2.1.8	As per DO-365B Annex K.8	2	N/A	DO-365B Annex K
2.2.2.2.1.11	As per DO-365B Annex K.9	2	N/A	DO-365B Annex K
2.2.2.2.1.13	As per DO-365B Annex K.10	2	N/A	DO-365B Annex K
2.2.2.2.1.15	2.2.5.6	N/A	SORA TMPR Decide	SHEPHERD
2.2.2.2.1.16	As per DO-365B Annex K.11	2	N/A	DO-365B Annex K
2.2.2.2.1.18	2.2.5.2	N/A	SORA TMPR Decide	SHEPHERD
2.2.2.2.1.19	2.2.5.1(.3) 2.2.5.3(.1) 2.2.5.5	N/A	SORA TMPR Detect	SHEPHERD
	2.2.3.12(.9) 2.2.5.6(.1.3) 2.2.6	N/A	SORA TMPR Feedback Loop	SHEPHERD
2.2.2.2.2	As per DO-365B Annex K.12	2	DO-386 §2.2.7	DO-365B Annex K

RTCA DO-386				
Requirements from DO-365B	**Recommended sections from DO-386**	**Requirement category**	**Additional relevant information**	**Assessment source**
2.2.2.2.4	2.2.3.12(.5)	N/A	SORA TMPR Robustness	SHEPHERD
2.2.2.2.5	2.2.5.1(.3) 2.2.5.3(.1) 2.2.5.5	N/A	SORA TMPR Detect	SHEPHERD
2.2.3	As per DO-365B Annex K.13	2	DO-386 §2.2.5.1.4	DO-365B Annex K
2.2.4.1	2.2.3.8(.3.2.3.1.2) 2.2.4.6 2.2.3.12	N/A	SORA TMPR Decide	SHEPHERD
2.2.4.3.5.2	2.2.5.6 2.2.5.2	N/A	SORA TMPR Decide	SHEPHERD
2.2.4.3.5.3	As per DO-365B Annex K.14	2	N/A	DO-365B Annex K
2.2.4.3.5.4	2.2.5.6 2.2.5.3	N/A	SORA TMPR Decide	SHEPHERD
2.2.4.3.6.1	As per DO-365B Annex K.13.4	2	N/A	DO-365B Annex K
2.2.4.3.6.1	As per DO-365B Annex K.14	2	N/A	DO-365B Annex K
2.2.4.3.6.1.3	As per DO-365B Annex K.14	2	N/A	DO-365B Annex K

RTCA DO-386				
Requirements from DO-365B	**Recommended sections from DO-386**	**Requirement category**	**Additional relevant information**	**Assessment source**
2.2.4.3.7	As per DO-365B Annex K.14	2	N/A	DO-365B Annex K
2.2.4.4	As per DO-365B Annex K.15	2	N/A	DO-365B Annex K
2.2.4.4.1.1.1.3	As per DO-365B Annex K.16	1	DO-386 §2.2.5	DO-365B Annex K
2.2.4.4.3.1.2.1	2.2.5.1(.2)	N/A	SORA TMPR Decide	SHEPHERD
2.2.4.4.3.1.3.1	2.2.5.1(.2)	N/A	SORA TMPR Decide	SHEPHERD
2.2.4.4.1.2	As per DO-365B Annex K.17	2	N/A	DO-365B Annex K
2.2.4.4.3.1	As per DO-365B Annex K.14	2	N/A	DO-365B Annex K
2.2.4.4.3.1.1.1	As per DO-365B Annex K.18	2	N/A	DO-365B Annex K
2.2.4.4.3.2	As per DO-365B Annex K.19	2	N/A	DO-365B Annex K
2.2.4.5	As per DO-365B Annex K.20 (with subsections)	2	N/A	DO-365B Annex K
2.2.5.6.2.3.2.8	As per DO-365B Annex K.21	1	N/A	DO-365B Annex K

RTCA DO-386				
Requirements from DO-365B	**Recommended sections from DO-386**	**Requirement category**	**Additional relevant information**	**Assessment source**
2.2.5.7.1	As per DO-365B Annex K.22	1	N/A	DO-365B Annex K
2.2.5.7.4	As per DO-365B Annex K.23	1	N/A	DO-365B Annex K
2.2.5.12.2.2	As per DO-365B Annex K.24	1	N/A	DO-365B Annex K
2.2.7	2.2.3.12(.3)	N/A	SORA TMPR Execute	SHEPHERD
2.2.8	2.2.7 2.2.7.1	N/A	SORA TMPR Robustness	SHEPHERD
2.2.9	2.2.5.6(.5) 2.2.7.2 2.2.7.3	N/A	SORA TMPR Robustness	SHEPHERD

3.21.4 Sections having agreed exemptions

This subsection provides the list of elements of RTCA DO-386 that need to be tailored and/or complemented before being proposed as a MoC for the requirements or a part thereof as identified in the detailed technical assessment.

RTCA DO-386			
Requirements from DO-365B	**Subject**	**Accepted deviations from DO-386**	**Additional relevant information**
2.2.4.3.6.1	En Route DWC Alerts	As per DO-365B Annex K.25	Test vectors failures classified into four categories depending on the cause: – Category A, due to DO-365B using well-clear volume, while ACAS Xu directly estimates collision risk; – Category B, encounter close to alert boundaries – passing or failing is susceptible to noise applied; – Category C, test vector uses a randomization seed yielding noise that is on the margins of the expected distribution; and – Category D, non-altitude reporting intruders above 15,500 ft considered invalid (inherited from TCAS). The categories are detailed in DO-365B, Annex K.25.2. From DO-365 K.25.1: "*Taking into account the above described justification categories and agreements between SC-147 and SC-228, ACAS Xu is considered to be fully compliant with the En Route DWC alerting requirements outlined in DO-365B.*"
2.2.4.4.1.1.1	Corrective Manoeuvre Guidance En Route and Non-Cooperative	As per DO-365B Annex K.26	Alerting hysteresis can lead to an alert being held while the guidance no longer warrants an alert for up to 4 s. Though requirement 583 does not allow for a buffer, an associated note marks as acceptable to have up to 5 s buffer.

RTCA DO-386			
Requirements from DO-365B	**Subject**	**Accepted deviations from DO-386**	**Additional relevant information**
2.2.4.4.3.1.4	Special Cases Unvalidated ADS-B Only	As per DO-365B Annex K.27	DO-365 forbids using unvalidated ADS-B for corrective alerts and guidance to avoid band saturation. However, ACAS Xu has prescriptive algorithms to prevent saturation. Thus, ACAS Xu can provide corrective guidance against unvalidated ADS-B intruders and does not need to comply with requirement 581.

ANNEX

3.22 ANALYSIS OF IEC 61508 AS AN ALTERNATIVE TO DO-178C

Summary

This document presents a comprehensive comparison of DO-178C and IEC 61508 standards. While not part of the original scope of SHEPHERD, this thorough comparison, outlining their respective approaches to safety-critical systems in aviation and various other industries, was presented to and reviewed by EASA in the framework of the project, resulting in its annexation to this final deliverable.

While DO-178C is specifically tailored to airborne systems and equipment software, IEC 61508 is a generic standard applicable to electrical, electronic and programmable electronic safety-related systems across different industries.

The analysis reveals that although both standards share similarities in software planning, development approaches and definition requirements, they differ either in their safety or hazard classification systems. The DO-178C's Design Assurance Levels (DALs) focus on the consequences of software failure, whereas the IEC 61508's Safety Integrity Levels (SILs) concentrate on the risk reduction provided by safety functions.

The document further explores the potential application of the IEC 61508 principles in the aviation industry, particularly in the context of Uncrewed Aerial Vehicles (UAVs) and Uncrewed Traffic Management (UTM) systems. By integrating the IEC 61508 principles into the existing DO-178C process, the aviation industry can benefit from a more comprehensive and flexible approach to safety management, addressing the unique challenges posed by UAVs and UTM systems.

Key recommendations for integrating IEC 61508 principles into the aviation industry's DO-178C process include tailoring IEC 61508 requirements, establishing a comprehensive safety lifecycle model, implementing adapted IEC 61508 requirements, and incorporating hazard and risk analysis methodologies.

The adoption of IEC 61508 principles in the aviation industry, with an initial focus on UAVs and UTM systems, can significantly enhance the systematic management of safety-related activities in the design, development and maintenance of aviation systems. This integration will ultimately contribute to increased safety and reliability in the rapidly evolving world of autonomous flight and air traffic management.

General scope and purpose

As software continues to play an increasingly crucial role in transportation systems, the need for safety standards and software development systems has become more important than ever. However, with the diversity of transportation systems and the varying levels of safety requirements, choosing the right safety standard can be challenging.

IEC61508 is a safety standard that can be applied to any transportation system, including ground-based systems, and it provides a comprehensive framework to ensure high levels of safety in software development. This paper evaluates both the DO-178C and IEC61508 (Part 3) safety development standards and provides a high-level comparison between the two. While not part of the original scope of SHEPHERD, this detailed comparison was presented to and reviewed by EASA in the framework of the project, resulting in its annexation to this final deliverable. The aim is to help transportation system stakeholders make an informed decision about which safety standard is the most appropriate for their specific needs.

This section seeks to explain and provide a comprehensive overview of the overarching themes of the discussion and clarify the intentions and goals behind the comparison of these two safety standards.

The beginning of the analysis highlights the importance of safety standards in software development for transportation systems, underlining the increased reliance on software and the significant role it plays in safety-critical systems. It also explains why the choice of safety standard can significantly influence the overall safety, reliability, and performance of these systems.

The section further delineates the reasons behind the selection of the two specific standards: DO-178C and IEC61508. It sets the context by discussing how these standards are generally applied in the industry and the types of transportation systems they are commonly associated with.

The key purpose of this chapter is to establish a basis for the subsequent detailed comparison of the two standards, explaining that this examination aims to assist stakeholders in making an informed decision about which standard best aligns with their specific needs. Additionally, the comparison will be carried out in a comprehensive manner, covering all aspects of the safety development process from hazard identification and classification to software design, implementation, verification, and documentation.

The last section confirms that the comparison will not only highlight the differences between DO-178C and IEC61508, but will also explore areas where the principles of the IEC61508 can supplement the requirements of DO-178C, potentially contributing to an enhanced safety approach in the transportation industry.

Bridging the gap: IEC 61508's role as a universal standard in avionics software assurance

In the evolving landscape of avionics software development and certification, the quest for a universal standard that ensures the highest levels of safety and reliability across both airborne and ground-based systems is paramount. The DO-178 and DO-278A standards have long stood as bastions of safety assurance within their respective domains. However, the International Electrotechnical Commission's (IEC) 61508 standard emerges as a compelling unifier, offering a comprehensive framework that can serve as an equivalent to both DO-178 for airborne systems and DO-278A for ground-based systems. This chapter explores the foundations, similarities, and extensions of IEC 61508 that justify its position as an effective equivalent standard, focusing on its adaptability, comprehensive approach to safety lifecycle, and risk management processes.

Compatibility with DO-178 and DO-278A

DO-178, titled "Software Considerations in Airborne Systems and Equipment Certification," and DO-278A, its counterpart for ground-based systems, focus on ensuring that software performs its intended function with a high degree of confidence and without introducing unacceptable risks. Both standards emphasise a process-oriented approach to software development and verification, aimed at achieving and evidencing software reliability and safety.

IEC 61508 mirrors these concerns but brings a broader perspective, focusing on the entire system's safety lifecycle. It addresses not only software but also the interaction between software and hardware components. This holistic view makes IEC 61508 uniquely equipped to serve as an equivalent framework, ensuring that all aspects of system safety are considered, whether for airborne (DO-178) or ground-based (DO-278A) systems.

Advantages of IEC 61508 as a unifying standard

The adaptability of IEC 61508 to different industries and technologies stands as one of its primary advantages. This flexibility makes it particularly suitable for the avionics sector, where rapid technological advancements are common. The standard's emphasis on a safety lifecycle approach encourages continuous improvement and adaptation to emerging risks and technologies, ensuring ongoing relevance and effectiveness.

Furthermore, IEC 61508's risk management process, which includes rigorous hazard analysis and risk assessment, aligns with the safety-critical nature of avionics software. By adopting a quantitative approach to safety integrity levels (SILs), IEC 61508 provides a clear, measurable framework for assessing and mitigating risks, facilitating a structured comparison to the assurance levels defined in DO-178 and DO-278A.

Overcoming challenges in adoption

While IEC 61508 presents a compelling case for its equivalence to DO-178 and DO-278A, challenges in adoption remain, primarily related to the avionics industry's regulatory environment and the specific requirements of airborne and ground-based systems. Bridging these standards requires careful mapping of IEC 61508's safety lifecycle phases and SILs to the specific processes and objectives outlined in DO-178 and DO-278A.

Moreover, regulatory acceptance plays a crucial role. Achieving industry and regulatory bodies' endorsement of IEC 61508 as an equivalent standard for avionics software assurance necessitates a detailed comparative analysis, demonstrating that compliance with IEC 61508 meets or exceeds the safety assurance levels prescribed by DO-178 and DO-278A.

The universal applicability and comprehensive approach of IEC 61508 position it as a viable equivalent to both DO-178 and DO-278A. Its flexibility, coupled with a rigorous safety lifecycle and risk management process, aligns with the critical safety requirements of avionics software, whether airborne or ground-based. By embracing IEC 61508, the industry can move towards a more unified and adaptable framework for software safety assurance, fostering innovation while maintaining the highest safety standards. The journey towards

universal acceptance and implementation will require collaboration, detailed analysis, and regulatory support, but the benefits of a unified safety standard in the avionics domain are clear and compelling.

Overview of the two standards

The aviation industry has long since adopted standards that incorporate safety planning and safety-specific process development into their software development cycle — starting with the adoption of DO-178C in the 1980s. Similarly, the automotive industry has recently started adopting IEC 61508 as a safety-driven development system that incorporates safety design into the software development process for high-volume production vehicles.

The use of software in vehicular transportation over the last thirty years has shown the necessity of safety-oriented development standards due to the ever-increasing complexity of these systems with millions of lines of code and autonomous systems, which are being deployed in transportation systems. Highly complex software and electronic systems used in transportation, whether aviation, civilian or military, all have a direct impact on the everyday safety of our communities.

DO-178C (Software Considerations in Airborne Systems and Equipment Certification) and IEC 61508 (Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems) are two separate standards used in different industries for ensuring the safety of software and systems. DO-178C is primarily used in the aviation industry, while IEC 61508 is a more generic standard applicable across various industries like automotive, energy (atomic power plants) and railway.

While both standards address safety, they use different terminology and classification systems. DO-178C uses Design Assurance Levels (DALs), whereas IEC 61508 uses Safety Integrity Levels (SILs). Comparing these two standards directly is not straightforward, as they were developed for different contexts and applications. However, a rough mapping between the two can be provided to give an idea of their relative safety levels.

DO-178C DALs

DAL A: Catastrophic failure — most stringent
DAL B: Hazardous-severe failure
DAL C: Major failure
DAL D: Minor failure
DAL E: No effect — least stringent

IEC 61508 SILs

SIL 1: Lowest level of safety integrity
SIL 2: Moderate level of safety integrity
SIL 3: High level of safety integrity
SIL 4: Highest level of safety integrity

Rough mapping

DO-178C DAL A <-> IEC 61508 SIL 4
DO-178C DAL B <-> IEC 61508 SIL 3
DO-178C DAL C <-> IEC 61508 SIL 2
DO-178C DAL D <-> IEC 61508 SIL 1
DO-178C DAL E <-> No direct equivalent in IEC 61508

Even though the standards in DO-178C and IEC 61508 were developed for different contexts and applications, it is still valuable to create a "rough mapping" between the two for several reasons:

Safety integrity comparison: Both standards aim to ensure safety in the operation of complex systems. Hence, mapping between DO-178C's Design Assurance Levels (DALs) and IEC 61508's Safety Integrity Levels (SILs) can provide a comparative scale for understanding safety measures across industries. For example, a system developed to DO-178C DAL A has a similar degree of safety assurance as one developed to IEC 61508 SIL 4. This

comparison becomes particularly useful when attempting to transfer or utilise practices from one domain to another.

Harmonisation and knowledge transfer: Given the global nature of many industries today, there is often significant value in being able to understand and relate different safety standards. Having a rough mapping between these standards aids in harmonising safety concepts, facilitating knowledge transfer and reducing misunderstandings that may occur due to the different terminology used.

Leveraging best practices: By understanding the parallels between the DALs and SILs, it's possible to leverage best practices from one standard to another, resulting in a more robust safety culture and potentially more efficient processes.

Cross-industry applications: For companies and projects that straddle different industry sectors, it's not uncommon to encounter both DO-178C and IEC 61508. The mapping between the standards can guide the decision-making process for cross-industry applications.

Regulatory and compliance requirements: Compliance requirements for a product or system might be specified in terms of either a DO-178C's DAL or an IEC 61508's SIL. Having a rough translation between these provides a useful starting point when these requirements need to be moved from one context to another.

It is important to note, however, that while this rough mapping provides an initial point of comparison, it should not replace careful and comprehensive consideration of the specific requirements and guidelines outlined in each standard. The safety integrity needs for any given system should always be evaluated in the full context of its intended use and operating environment.

Adoption of industry function safety software and hardware to aviation processes

The aviation industry is characterised by stringent safety requirements used to ensure the highest level of safety for passengers, crew and the environment. This chapter discusses the adoption of the IEC 61508 standard (a generic standard for electrical, electronic and programmable electronic safety-related systems) to the aviation's DO-178C-related processes. This adoption aims to enhance safety and reliability in the aviation industry by leveraging the principles and best practices from IEC 61508.

IEC 61508 and DO-178C: A comparative overview

IEC 61508 is a comprehensive standard that covers various aspects of safety-related systems, including hardware, software and the overall safety lifecycle. It is applicable to a wide range of industries and sectors, with a focus on functional safety. The DO-178C process, on the other hand, is specific to the aviation industry and primarily focuses on software development for airborne systems.

Despite their different scopes, there are several common elements between the IEC 61508 and the DO-178C process. Both standards emphasise risk-based safety approaches, safety integrity levels and the importance of safety lifecycle management. By adopting IEC 61508 principles and practices to the DO-178C process, the aviation industry can benefit from a more holistic and robust safety management system.

Analysis of the similarities and differences between IEC 61508 and DO-178C processes

- Risk-based safety approach: Both IEC 61508 and DO-178C processes emphasise a risk-based approach to safety management. They identify, assess and mitigate risks to achieve acceptable safety levels in their respective industries.
- Safety integrity levels: Both standards use similar concepts of safety integrity levels (SILs, in IEC 61508) or DALs (Design Assurance Levels, in DO-178C) to categorise the safety requirements based on the severity of potential consequences. This classification helps determine the rigour and extent of safety-related activities for each safety level.
- Safety lifecycle management: Both IEC 61508 and DO-178C processes promote the use of safety lifecycle models as a framework for systematically managing safety-related activities. These models cover all aspects of safety management, from initial concept and design to decommissioning and disposal.
- Verification and validation: Both standards emphasise the importance of verification and validation activities to ensure that safety requirements are met and the safety-related systems perform their intended functions.
- Documentation: Comprehensive documentation of safety-related activities, including design, analysis, testing and maintenance, is required by both IEC 61508 and DO-178C processes to demonstrate compliance and traceability.

Differences between IEC 61508 and DO-178C processes

- Scope: IEC 61508 is a generic standard applicable to a wide range of industries and sectors, whereas the DO-178C process is specific to the aviation industry and focuses primarily on software development for airborne systems.
- Focus on hardware: The IEC 61508 process covers both hardware and software aspects of safety-related systems, while the DO-178C process concentrates on the software-related elements, with the DO-254 addressing hardware development in the aviation industry.

- Level of detail: The IEC 61508 process provides a more detailed and comprehensive set of requirements and guidance for safety management, whereas the DO-178C process is less prescriptive and leaves more room for interpretation and tailoring to specific projects.

Areas where IEC 61508 principles can complement existing DO-178C requirements

- Hardware safety: IEC 61508's focus on hardware safety can provide valuable insights for the aviation industry to ensure that safety-related hardware is designed, developed and maintained with the same rigour as software.
- Systematic safety lifecycle model: While both standards promote safety lifecycle management, IEC 61508 provides a more comprehensive framework that can be adapted to the aviation industry to streamline safety-related activities and enhance consistency.
- Techniques and measures: IEC 61508 Part 7 provides an overview of techniques and measures to ensure functional safety. These techniques can be applied to the aviation industry to further enhance safety practices and risk management.
- Security considerations: IEC 61508 requires the consideration of malevolent and unauthorised actions during hazard and risk analyses, which can be beneficial for the aviation industry to ensure a more comprehensive risk assessment and enhance the overall security of safety-related systems.

Mapping between IEC 61508 and DO-178C standards

- Risk-based safety approach:
    - IEC 61508: Functional safety and risk reduction based on SILs
    - DO-178C: Software safety assurance and risk reduction based on DALs
- Safety integrity levels:
    - IEC 61508: Safety Integrity Levels (SIL 1-4)
    - DO-178C: Design Assurance Levels (DAL A-E)
- Safety lifecycle management:
    - IEC 61508: Overall safety lifecycle model
    - DO-178C: Software development and certification lifecycle
- Verification and validation:
    - IEC 61508: Verification and validation of safety-related systems (hardware and software)
    - DO-178C: Verification and validation of safety-related software
- Documentation:
    - IEC 61508: Documentation throughout the safety lifecycle
    - DO-178C: Documentation for software development, verification and validation

Adapting IEC 61508 to the DO-178C process

To adopt IEC 61508 to the aviation processes in DO-178C, the following steps are recommended:

- Analyse the similarities and differences between the IEC 61508 and DO-178C processes, identifying areas where the IEC 61508 principles can complement the existing DO-178C requirements.

- Establish a comprehensive safety lifecycle model for the aviation industry, incorporating IEC 61508 principles to enhance the systematic management of safety-related activities in the design, development and maintenance of aviation systems.
- Implement the adapted IEC 61508 requirements in the DO-178C process, ensuring that the aviation industry follows a consistent, risk-based approach to safety management.
- Provide training and resources to aviation industry stakeholders to ensure a smooth transition and successful implementation of the adapted IEC 61508 principles in the DO-178C process.

Benefits of adopting IEC 61508 in the Aviation DO-178C process

By adopting IEC 61508 in the aviation industry's DO-178C process, the industry can benefit from:

- A more comprehensive and robust safety management system that covers both hardware and software aspects of safety-related systems.
- Enhanced functional safety, ensuring that safety-related systems perform their intended functions in the event of failures or malfunctions.
- Improved risk management through the application of safety integrity levels and risk-based approaches to safety assessment.
- A consistent and systematic safety lifecycle model that streamlines safety-related activities and provides a clear framework for continuous improvement.
- The ability to leverage best practices and knowledge from a wide range of industries and sectors, promoting innovation and continuous improvement in aviation safety.

Safety lifecycle model for the aviation industry, incorporating the principles of the IEC 61508

A comprehensive safety lifecycle model for the aviation industry, incorporating IEC 61508 principles, can be structured into the following phases:

Concept phase:

1. Identify the system's scope and boundaries.
2. Perform a preliminary hazard and risk analysis.
3. Define the safety objectives and high-level safety requirements.
4. Determine the Design Assurance Levels (DALs) or the Safety Integrity Levels (SILs).

System requirements and design phase:

1. Develop a system architecture and allocate relevant safety requirements.
2. Specify hardware and software requirements for safety-related systems.
3. Perform a detailed hazard and risk analysis that considers both hardware and software aspects.
4. Design safety-related functions and allocate safety integrity levels.

Hardware development phase (IEC 61508 principles & DO-254 guidance):

1. Develop hardware components based on allocated requirements.
2. Perform related hardware verification and validation activities.
3. Assess hardware compliance with safety integrity levels and reliability requirements.

Software development phase (DO-178C process):

1. Develop software components based on allocated requirements.
2. Perform software verification and validation activities.
3. Assess software compliance with Design Assurance Levels.

System integration and testing phase:

1. Integrate hardware and software components into the overall system.
2. Perform system-level verification and validation activities.
3. Verify that relevant safety requirements are met and safety-related functions perform as intended.

Certification and deployment phase:

1. Compile necessary documentation for certification.
2. Obtain certification from the relevant aviation regulatory authorities.
3. Deploy the system into operational environments.

Operation and maintenance phase:

1. Monitor system performance, reliability and safety during operation.
2. Perform regular maintenance, updates and upgrades as necessary.
3. Investigate and address any safety incidents or issues that may arise.

Decommissioning and disposal phase:

1. Assess the end-of-life impact on safety and environmental factors.
2. Remove safety-related systems from operation.
3. Dispose of system components in an environmentally responsible manner.

By establishing a comprehensive safety lifecycle model incorporating IEC 61508 principles, the aviation industry can enhance the systematic management of safety-related activities. This approach ensures that safety is considered at every stage of the design, development and maintenance of aviation software and hardware systems, ultimately leading to improved safety, reliability and robustness.

Software planning

The following is a comparison of software planning in both standards, including the required artefacts and development approaches:

Software planning artefacts

DO-178C	IEC 61508
• Plan for Software Aspects of Certification (PSAC) • Software Development Plan (SDP) • Software Verification Plan (SVP) • Software Configuration Management Plan (SCMP) • Software Quality Assurance Plan (SQAP) • Software Requirements Standards • Software Design Standards • Software Code Standards • Software Test Standards	• Safety Plan • Software Requirements Specification (SRS) • software Design Specification (SDS) • Software Test Plan • Software Configuration Management Plan • Software Quality Assurance Plan • Software Verification and Validation Plan • Software Integration and Test Plan

Table 1. Software planning artefacts

Software development approach

DO-178C	IEC 61508
• *Top-down approach* DO-178C emphasises a top-down approach, where the software development process starts with high-level requirements, followed by detailed design, coding and testing. • *Traceability* DO-178C requires traceability between software requirements, design, code and test cases to ensure that all requirements are implemented and verified. • *Verification and validation* Verification activities are performed to confirm that the software conforms to its requirements, while validation activities	• *Top-down and bottom-up approaches* IEC 61508 supports both top-down and bottom-up development approaches, depending on the complexity of the system and the requirements of the specific industry. • *Traceability* IEC 61508 also requires traceability between safety requirements, design, implementation and verification activities to ensure that safety functions are correctly implemented. • *Verification and validation* Similar to DO-178C, IEC 61508 emphasises verification and validation activities to demonstrate that the software meets its

ensure that the software meets the intended operational needs. ● *Structured development* DO-178C promotes a structured development process, with specific objectives and activities for each phase of the software lifecycle.	safety requirements and performs as intended in the target environment. ● *Safety lifecycle model* IEC 61508 follows a safety lifecycle model that covers all phases of the software development process, from initial concept and hazard analysis to decommissioning and disposal.

Table 2. Software development approach

Comparison

Both DO-178C and IEC 61508 place significant emphasis on planning, traceability and verification/validation activities.

While there are similarities in the software planning process, artefacts and development approaches between DO-178C and IEC 61508, the key differences lie in the level of prescription and specificity to the respective industries.

Safety and requirements definition

The following is a comparison of safety and requirements definitions in both standards, with a focus on the evaluation of safety or hazard classification:

Safety or hazard classification

DO-178C	IEC 61508
DO-178C classifies the safety of airborne software systems using Design Assurance Levels (DALs). There are five DAL levels, from A to E, with A being the most critical and E being the least critical. The assignment of DALs is based on the failure condition classification of the software: ● Level A (Catastrophic): Failure may cause multiple fatalities or loss of the aircraft. ● Level B (Hazardous): Failure may cause a large reduction in safety margins or serious injury to a small number of occupants. ● Level C (Major): Failure may cause significant reduction in safety margins, discomfort to occupants or physical distress to a small number of occupants. ● Level D (Minor): Failure may cause a slight reduction in safety margins or slight discomfort to occupants. ● Level E (No Effect): Failure has no effect on safety or the functioning of the aircraft.	IEC 61508 classifies the safety of electrical/electronic/programmable electronic safety-related systems using Safety Integrity Levels (SILs). There are four SIL levels, from 1 to 4, with SIL 1 being the least critical and SIL 4 being the most critical. The assignment of SILs is based on the risk reduction required for each safety function: ● SIL 1: Provides a low level of risk reduction (typically a risk reduction factor of 10). ● SIL 2: Provides a medium level of risk reduction (typically a risk reduction factor of 100). ● SIL 3: Provides a high level of risk reduction (typically a risk reduction factor of 1,000). ● SIL 4: Provides the highest level of risk reduction (typically a risk reduction factor of 10,000).

Table 3. Safety or hazard classification

Comparison

While both DO-178C and IEC 61508 have safety or hazard classification systems, their approaches differ:

- DO-178C focuses on the consequences of software failure, classifying the severity of failure conditions into five DALs, each with its own set of objectives and activities.
- IEC 61508, on the other hand, focuses on risk reduction provided by safety functions, assigning SILs based on the level of risk reduction needed to achieve a tolerable risk.

Requirements definition

DO-178C

Requirements in DO-178C are expressed as high-level requirements and low-level requirements. High-level requirements describe the overall functionality of the software and its intended behaviour, while low-level requirements provide detailed information on inputs, outputs and internal functions.

IEC 61508

IEC 61508 defines safety requirements as part of the safety requirements specification, which includes functional safety requirements and safety integrity requirements. Functional safety requirements describe the safety functions that must be performed by the system, while safety integrity requirements establish the required level of performance for each safety function.

While both DO-178C and IEC 61508 have safety or hazard classification systems, their approaches and focuses are different, with DO-178C emphasising failure condition consequences and IEC 61508 targeting the risk reduction provided by safety functions. The way requirements are defined in both standards is also distinct, with DO-178C focusing on high-level and low-level requirements, and IEC 61508 defining functional safety requirements and safety integrity requirements.

Hazard classification

Both standards require the classification of hazards and the assignment of safety integrity levels based on the severity and likelihood of potential hazards. This chapter compares the hazard classification process in both standards, outlining similarities and differences.

Hazard identification

Both DO-178C and IEC 61508 require the identification of potential hazards early in the development process. While DO-178C focuses on airborne systems and equipment, IEC 61508 has a broader scope, covering the functional safety of electrical, electronic and programmable electronic systems.

DO-178C

DO-178C uses a qualitative approach to identify hazards, requiring the analysis of system requirements, functions and potential failure conditions. This process involves the assessment of single-event, multiple-event and common-cause failure conditions, with the objective of identifying all potential failure conditions that could affect safety.

IEC 61508

IEC 61508 employs a more systematic hazard and risk analysis process, involving techniques such as fault tree analysis, event tree analyses and failure modes and effects analyses. These methods help identify hazards, their potential causes and their consequences on the overall safety of the system.

Hazard classification and severity

Both DO-178C and IEC 61508 classify hazards according to their severity, but they use different terminologies and scales.

DO-178C

The DO-178C categorises potential failure conditions into five levels of severity, from 'No Effect' to 'Catastrophic.' These levels are defined as follows:

- *Catastrophic*: Failure conditions that can result in multiple fatalities or the loss of an aircraft.
- *Hazardous*: Failure conditions that can result in a large reduction in safety margins, serious injury or fatalities.
- *Major*: Failure conditions that can reduce safety margins, cause discomfort to occupants or result in a significant increase in crew workload.
- *Minor*: Failure conditions that have a slight effect on safety or cause some inconvenience to occupants.
- *No Effect*: Failure conditions that have no impact on safety.

IEC 61508

IEC 61508 classifies hazards into four Safety Integrity Levels (SILs), which represent the risk reduction required to achieve an acceptable level of safety. SILs range from SIL 1 (lowest) to SIL 4 (highest). The classification is based on three factors: the consequence of a hazard, the likelihood of its occurrence and the exposure time.

Assigning Safety Integrity Levels (SILs) and Software Levels (SLs)

Both DO-178C and IEC 61508 assign specific safety integrity levels (SILs) and software levels (SLs) based on the hazard classification.

DO-178C: Software levels (SLs)

DO-178C assigns software levels (A to E) corresponding to the severity of failure conditions. These levels dictate the rigour of software development, verification and validation activities.

IEC 61508: Safety Integrity Levels (SILs)

IEC 61508 assigns SILs based on the risk analysis, with each SIL corresponding to a specific range of risk reduction. The assigned SIL determines the rigour of the development process and the required performance of the safety functions.

DO-178C and IEC 61508, though designed for different industries, share a common objective of ensuring the safety of critical systems. They both involve hazard identification, classification and the assignment of safety integrity levels or software levels, albeit with different methodologies and terminologies. By understanding the differences and similarities between these standards, developers can effectively tailor their processes to meet the specific requirements and rigour necessary for the development and verification of safety-critical systems in their respective industries.

Software architecture, design and implementation

This chapter compares the approaches to software architecture, design and implementation in both standards, highlighting their similarities and differences.

Software architecture

Software architecture is a critical aspect of both DO-178C and IEC 61508 as it provides the foundation for the development of safe and reliable systems. The standards have different emphases but still share some common principles.

DO-178C

DO-178C requires a hierarchical decomposition of the software system into components or modules, with the clear identification of interfaces and data flow. The architecture should support the allocation of system-level requirements to software components and promote modularity, traceability and the separation of concerns.

IEC 61508

The IEC 61508 focuses on the architecture of safety-related systems, emphasising the segregation of safety functions from non-safety functions. This standard recommends the use of architectural patterns, such as diverse redundancy and fault tolerance, to achieve the required level of safety integrity. Additionally, IEC 61508 requires the definition of safety-related software and hardware components, along with their interactions and dependencies.

Software design

Both DO-178C and IEC 61508 emphasise a structured and systematic approach to software design, ensuring that the system is developed to meet its requirements and safety objectives.

DO-178C

DO-178C prescribes a top-down design approach, where high-level requirements are changed into lower-level requirements, ultimately resulting in detailed software design. The design process should ensure that the software components are well-structured, modular and have well-defined interfaces. This approach facilitates traceability, maintainability and ease of verification.

IEC 61508

IEC 61508 also recommends a structured design approach, with an emphasis on the identification and allocation of safety functions to software components. The standard requires the use of formal methods, such as state-transition diagrams, Petri nets or formal logic, for the design of safety-critical components. This ensures a higher degree of rigour and correctness in the design process.

Software implementation

Both DO-178C and IEC 61508 place great importance on the quality of software implementation, as it directly impacts the safety and reliability of the system.

DO-178C

DO-178C prescribes the use of coding standards and guidelines, as well as the selection of appropriate programming languages, to ensure the consistency, readability and maintainability of the software. The standard also emphasises the importance of traceability between source code and design artefacts, ensuring that the implementation adheres to the design specifications.

IEC 61508

IEC 61508 also emphasises the use of coding standards and guidelines and requires the selection of appropriate programming languages and tools based on the system's safety requirements. In addition, IEC 61508 recommends the use of formal methods and static analysis tools for verifying the correctness and safety of the software implementation.

Unit verification and integration level

Development verification is an essential aspect of ensuring that the software in safety-critical systems performs as intended. Both DO-178C and IEC 61508 emphasise the importance of verification at multiple levels, including unit and integration testing. This chapter compares the verification processes at the unit and integration levels for both standards, with the goal of highlighting their similarities and differences.

Unit level verification

Unit level verification involves verifying the correctness and compliance of individual software components or modules.

DO-178C

DO-178C emphasises the importance of verifying that the source code outputs meet the software requirements and standards.

This includes:

- Ensuring that the code adheres to coding standards and guidelines.
- Verifying the traceability between source code and design artefacts.
- Performing unit testing to verify the functionality of individual software components.

IEC 61508

IEC 61508 also focuses on the verification of individual software components.

This includes:

- Ensuring that the code adheres to coding standards and guidelines.
- Verifying the correct allocation of safety functions to software components.
- Performing unit testing, with an emphasis on the correct implementation of safety functions.

Integration level verification

Integration level verification involves verifying the correctness and compliance of the software system as a whole, including the interactions between individual software components.

DO-178C

DO-178C requires the following steps for integration level verification:

- Verifying that the software functionality meets the system requirements.
- Verifying that the software design and architecture meet the software requirements and standards.
- Performing integration testing to evaluate the correct interactions between software components and validate the system's overall functionality and safety.

IEC 61508

IEC 61508 also emphasises integration level verification and requires the following steps:

- Verifying that the safety functions are correctly integrated into the system.

- Evaluating the correct interactions between safety-related and non-safety-related components.
- Performing integration testing with a focus on safety function performance and fault tolerance.

Both DO-178C and IEC 61508 stress the importance of verification at the unit and integration levels to ensure that the software performs as intended and meets safety requirements. While there are differences in the specifics of the verification processes, the overall goals are similar: to ensure that individual software components function correctly, and that the system as a whole operates safely and reliably.

Artefacts and governing bodies

When properly followed, both DO-178C and IEC 61508 produce artefacts that can be reviewed by governing bodies as part of a larger certification process. The FAA, for instance, requires the use of DO-178C for developing airborne software but does not guarantee certification based on the process alone. This chapter compares the artefacts and governing bodies associated with DO-178C and IEC 61508, highlighting their similarities and differences.

Artefacts

Both DO-178C and IEC 61508 require the generation of various artefacts throughout the development and verification process. These artefacts serve as evidence that the development process has been followed and that the safety requirements have been met.

DO-178C

Some common artefacts produced during the development process according to DO-178C include:

- System and software requirements documents
- Software design documents and architecture diagrams
- Source code and coding standards
- Unit and integration test plans, procedures and results
- Traceability matrices
- Configuration management and problem reporting records

IEC 61508

IEC 61508 also requires the generation of several artefacts during the development process, such as:

- Hazard and risk analysis reports
- Safety requirements specifications
- Safety-related system and software design documents
- Source code and coding standards
- Unit and integration test plans, procedures and results
- Traceability matrices
- Configuration management and problem reporting records

Governing Bodies

Different industries have specific governing bodies responsible for overseeing the certification process and ensuring compliance with the respective standards.

DO-178C

In the aerospace industry, various governing bodies oversee the certification process, depending on the region. Some examples include:

- Federal Aviation Administration (FAA) in the United States
- European Union Aviation Safety Agency (EASA) in Europe
- National Civil Aviation Agency (ANAC) in Brazil

These governing bodies review the artefacts produced during the development process as part of the larger certification process for the whole aircraft.

IEC 61508

For IEC 61508, governing bodies vary depending on the industry sector and region. Examples of governing bodies include:

- **TC 65 (Industrial-process measurement, control and automation)**: This technical committee and its subcommittees are directly involved in the development and maintenance of IEC 61508, among other standards related to automation and control.
- **Working Groups and Maintenance Teams**: Specific working groups and maintenance teams under the relevant technical committees are established to focus on the continuous development, revision, and clarification of the standards.
- **IEC National Committees**: Each IEC member country's national committee contributes to the review, voting, and implementation of the standard within their country. They can also propose changes or updates to the standard.

These organisations may have additional sector-specific standards derived from IEC 61508, such as ISO 26262 for automotive applications.

Both DO-178C and IEC 61508 emphasise the importance of generating artefacts throughout the development process, which serve as evidence of compliance with the respective standards. While the specific artefacts and governing bodies differ between the standards, they share the common goal of ensuring the safety and reliability of critical systems.

Support tools

Support tools play a vital role in the development and verification of safety-critical systems, ensuring consistency, repeatability and efficiency in the process. Both DO-178C and IEC 61508 require the evaluation and certification of supporting tools and processes to guarantee their reliability and known outputs. This chapter compares the support tools used in DO-178C and IEC 61508 and highlights their similarities and differences.

Support tools in DO-178C

DO-178C defines several categories of support tools, such as development tools, verification tools and configuration management tools. These tools need to be evaluated and certified for repeatability and known outputs. Some common support tools used in DO-178C include:

- Integrated development environments (IDEs)
- Compilers and code generators
- Static and dynamic analysis tools
- Unit testing and integration testing tools
- Configuration management tools
- Traceability tools
- Problem reporting tools

Support tools in IEC 61508

IEC 61508 also emphasises the importance of support tools in the development process, with a focus on ensuring the correctness, reliability, and safety of the system. Similar to DO-178C, IEC 61508 requires the evaluation and certification of these tools. Some common support tools used in IEC 61508 include:

- Integrated development environments (IDEs)
- Compilers and code generators
- Formal methods and static analysis tools
- Unit testing and integration testing tools
- Configuration management tools
- Traceability tools
- Problem reporting tools

Qualification and certification of support tools

Both DO-178C and IEC 61508 require that the support tools used in the development process be evaluated and qualified, ensuring their repeatability and known outputs.

DO-178C

DO-178C outlines the tool qualification process, which involves creating a Tool Qualification Plan (TQP) that describes the tool's intended use, the evaluation of the tool's outputs and the necessary activities for tool qualification.

IEC 61508

IEC 61508 also requires a tool qualification process, which may involve creating a TQP or equivalent documentation that describes the tool's intended use, the evaluation of the tool's outputs and the necessary activities for tool qualification.

Extra considerations for IEC 61508 from the AMC & GM for U-space regulations

Certification data and evidence [GM7 Article 15]

U-space regulations, along with its accompanying acceptable means of compliance (AMC) and guidance material (GM), sets forth guidelines for the safe and secure integration of uncrewed aircraft systems (UAS) into European airspaces. This chapter explores the consideration of IEC 61508, a functional safety standard, from the perspective of certification data and evidence as described in the AMC & GM for U-space regulations.

Concept of operations (ConOps)

When incorporating IEC 61508 into the development of U-space services, a clear ConOps should be established. This includes defining the overall system architecture, the interactions between the components and the safety functions required to ensure reliable operation.

Compliance matrix

A compliance matrix should be developed to demonstrate how the system adheres to the U-space Regulation (EU) 2021/664, the related AMC & GM, and applicable industry standards, including the IEC 61508.

Engineering processes and procedures

The engineering processes and procedures must follow the IEC 61508 guidelines, including the use of software assurance techniques, risk reduction measures, and the application of safety integrity levels (SILs).

Engineering and design documentation

Detailed engineering and design documentation must be provided to demonstrate the proper implementation of the IEC 61508 principles in the development of U-space services.

Safety assessment

A comprehensive safety assessment, compliant with IEC 61508, should be conducted to evaluate the risks associated with the U-space services and determine appropriate risk reduction measures.

Security risk assessment

A security risk assessment must be performed to identify potential threats to the U-space services and to ensure the system's resilience against cyber-attacks.

Operational procedures and instructions

Operational procedures and instructions should be developed for stakeholders such as U-space Service Providers (USSPs) and UAS operators, outlining the safe and secure use of U-space services while adhering to the principles set out in IEC 61508.

Analyses and tests

System analyses and tests should be conducted following the IEC 61508 guidelines, including the validation of safety functions, fault detection mechanisms and system performance under various operating conditions.

Records

Maintain records of reviews, configurations, changes, statements of work and quality control measures in compliance with the requirements set out in IEC 61508.

Residual defects and limitations

Identify and document any residual defects and limitations associated with U-space services, ensuring that they do not compromise safety or security as defined in IEC 61508.

By considering IEC 61508 from the perspective of certification data and evidence as described in the AMC & GM for U-space regulations, developers can ensure that U-space services are developed and operated in a safe, reliable and secure manner. Incorporating the principles and guidelines defined in IEC 61508 into the development process helps ensure compliance with U-space regulations and contributes to the overall safety and security of UAS operations in European airspaces.

Concept of operations (ConOps) — Content

U-space regulations aim to provide a framework for the safe and efficient management of uncrewed aircraft systems (UAS) operations in the European Union. The acceptable means of compliance (AMC) and guidance material (GM) for U-space regulations outline the expectations for the concept of operations (ConOps) content. In this chapter, we will explore how the IEC 61508, a widely recognised functional safety standard, can be considered in the context of developing a ConOps for U-space services.

Aligning the IEC 61508 with U-space-related elements in the ConOps

IEC 61508 can be used as a basis for addressing various aspects of a ConOps for U-space services to ensure the safe and reliable operation of a UAS. Here are some examples of how the IEC 61508 can be considered in the context of the AMC & GM for U-space regulations.

Infrastructure availability and continuity [GM8 Article 15(1) (5)]

IEC 61508 can help define the safety requirements and risk mitigation measures for the infrastructure supporting U-space services. This includes the availability and continuity of service provisions, as well as redundancy and fault tolerance considerations.

Operational capacity and scalability [GM8 Article 15(1) (5)]

The safety lifecycle approach of IEC 61508 can be applied to evaluate the operational capacity and scalability of a U-space system. This involves analysing the system's ability to support simultaneous operations and its potential for growth.

Third-party arrangements and subcontracted activities [GM8 Article 15(1) (6)]

IEC 61508 can provide guidance on managing safety-related activities involving third parties or subcontractors. This includes ensuring that safety requirements are properly communicated and met by all parties involved in the U-space system's development and operation.

Functional System Description and Targeted Level of Integrity or Reliability [GM8 Article 15(1) (8) & (9)]

The ConOps should describe the functional system of the U-space service provider, including its architecture, components and interfaces. IEC 61508 can help define the targeted level of integrity or reliability for the functional system, ensuring that it meets the required safety objectives.

Cybersecurity measures [GM8 Article 15(1) (10)]

IEC 61508 can be used as a basis for addressing cybersecurity risks in the U-space system. This includes implementing technical measures such as authentication, encryption and secure communication protocols to protect against potential threats.

Previous certification/approval experience [GM8 Article 15(1) (11)]

Experience with IEC 61508 certification or approval can be beneficial when developing a U-space ConOps. It demonstrates the applicant's familiarity with functional safety principles and the ability to apply them to a U-space system.

Assumptions on U-space performance requirements [GM8 Article 15(1) (13)]

IEC 61508 can provide guidance on defining assumptions related to U-space performance requirements. This includes identifying safety-related performance requirements, such as response times, data accuracy and system availability, based on the risk analysis and safety objectives.

IEC 61508 can be considered as a valuable resource when developing a ConOps for U-space services. By aligning the functional safety principles of IEC 61508 with the expectations outlined in the AMC & GM for U-space regulations, applicants can ensure the safety and reliability of their U-space systems while addressing the unique challenges associated with uncrewed aircraft operations.

Software assurance

This chapter discusses the application of IEC 61508, a widely used functional safety standard, from the perspective of software assurance in the context of U-space regulations.

Documented software assurance process

IEC 61508 provides a systematic framework for developing safety-related systems, including software assurance processes. When applying IEC 61508 in the context of U-space regulations, the applicant should consider the following aspects:

Development error identification, correction and mitigation

IEC 61508 emphasises the importance of identifying, correcting and mitigating development errors, such as mistakes in requirement determination, design or implementation. By following the structured process outlined in IEC 61508, applicants can minimise potential residual defects in software implementation.

Software behaviour in the specified context

The IEC 61508 requires the software to behave as intended in the specified context. This aligns with U-space performance requirements, ensuring that the software operates safely and effectively in the context of U-space services.

Additional feature implementation

The applicant should demonstrate that the implementation of potential additional features, except those required for ensuring the safe provision of services, does not interfere with the safe provision of the required services. This can be achieved by adhering to the IEC 61508's principles of modular design and separation of concerns.

Credit taken from simulated environments and automated activities

When software assurance relies on simulated environments and/or automated activities, the IEC 61508 can be used to address the U-space requirements, as follows:

Scope and credit identification

Applicants should identify the scope and credit taken from simulated environments and automated activities, substantiating their relevance to U-space performance requirements. IEC 61508 provides guidance on the use of simulations and automated verification techniques as part of the overall safety lifecycle.

Simulated or automated environment trustworthiness

IEC 61508 can be used to demonstrate that the simulated or automated environments are representative of, or sufficiently close to, real operational conditions and can be trusted to produce evidence of their proper behaviour and products. The standard provides a structured approach to validating the correctness and reliability of the simulated or automated environments, ensuring their relevance to the context of U-space.

IEC 61508 can be a valuable reference for addressing the software assurance requirements outlined in the AMC & GM for U-space regulations. By adhering to the principles and processes defined in IEC 61508, applicants can establish a documented software assurance process that satisfies the U-space performance requirements, ensuring the safe and efficient provision of U-space services.

Information security assurance

When considering the IEC 61508 from the information security assurance perspective, it's important to focus on the AMC & GM guidance for U-space regulations.

Security risk assessment and mitigation

The applicant should follow a continued risk-based approach to assess the provision of services against potential information security threats and vulnerabilities that could affect the confidentiality, availability and integrity of the services. Key steps in this process include:

Identifying and assessing risks

Assess the potential threats and vulnerabilities affecting the components of functional systems, such as hardware, software, interfaces with other U-space airspace stakeholders, e-conspicuity or Network R-ID receivers.

Mitigating risks

Develop and implement necessary mitigation measures to ensure that no identifiable vulnerabilities exist or that they cannot be exploited to create a hazard or generate a failure resulting in an unsafe condition.

Demonstrating the effectiveness of mitigation measures

Provide evidence of the effectiveness and robustness of the mitigation measures through security-oriented robustness testing, inspection/analysis, refutation/penetration testing or a combination of these, as agreed upon with the competent authority.

Developing instructions for continued protection

Create instructions for physical and operational security procedures, auditing and monitoring the security effectiveness to ensure continued and effective protection of the provision of services.

Sharing mitigation measures with stakeholders

When mitigation measures rely on operational security measures to be fulfilled by a third party (e.g. UAS operator, USSP), they should be properly documented and shared with the relevant stakeholders.

Dynamically reassessing vulnerabilities and threat levels

Continuously reassess potential new vulnerabilities and threat levels not foreseen during previous security risk assessments. If an unacceptable threat is identified, notify the relevant stakeholders and the competent authority in a timely manner of the need and means to mitigate the new risk.

IEC 61508 considerations in information security assurance

The IEC 61508 standard can be applied to U-space systems to ensure the safety and reliability of functional systems. Although IEC 61508 is not primarily focused on information security, it can provide guidance on systematic design, development and validation of safety-critical systems. The principles of IEC 61508 can be adapted to complement the information security assurance process outlined in the AMC & GM for U-space regulations.

The AMC & GM for U-space regulations emphasises the importance of information security assurance in the provision of U-space services. Although IEC 61508 is not primarily focused on information security, its principles can be adapted to complement and support the risk-based approach outlined in the AMC & GM. By considering IEC 61508 in the context of information security assurance, developers and operators can ensure the safety, reliability and security of U-space systems and services.

Software assurance processes

This chapter will discuss the alignment of IEC 61508 software assurance processes with the key elements of the AMC & GM for U-space regulations.

Software requirements

IEC 61508 emphasises the importance of clear, complete and correct software requirements, ensuring that they align with system-level requirements and satisfy the specified services and safety support requirements. This is consistent with the expectations set out in the AMC & GM for software requirements, which include specifications for functional behaviour in nominal and degraded modes, timing performance, capacity, accuracy, resource usage, robustness and overload tolerance.

Software implementation

In accordance with IEC 61508, software implementation should not introduce any functions that could adversely affect the service specifications or cause undesirable behaviour that may impair safe service provisions. This aligns with the expectations laid out in the AMC & GM for U-space regulations.

Traceability

IEC 61508 requires comprehensive traceability for all software requirements, ensuring that they are linked to the specification of services, safety support requirements and verification activities. This is in line with the AMC & GM's expectations for traceability throughout the software development process.

Verification and validation

IEC 61508 specifies rigorous verification and validation processes, including testing and analyses to demonstrate that the implemented software complies with its requirements. This is consistent with the expectations for software verification in the AMC & GM, which includes verifying the software requirements in a representative environment, robustness testing, interface verification and producing traceable results.

Configuration management and quality control

IEC 61508 emphasises the importance of configuration management and quality control throughout the software life cycle. This is consistent with the expectations for software assurance processes in the AMC & GM, which include configuration identification, problem reporting and corrective action management.

Independence and impartiality

IEC 61508 requires software quality control activities to be performed independently from the software development team, ensuring impartiality in the assessment of conformance with the established processes and

procedures. This aligns with the expectations for software quality control in the AMC & GM for U-space regulations.

The software assurance processes outlined in the IEC 61508 align well with the key elements of the AMC & GM for U-space regulations. By following the IEC 61508 standard, developers can ensure that their software meets the safety and performance requirements set forth by the AMC & GM. It is important to note that the specific application of IEC 61508 in the context of U-space regulations may require further adaptation and tailoring to fully satisfy regulatory requirements.

Software assurance — use of existing industry standards

While applicants are responsible for defining software assurance processes within their organisation, existing industry standards can provide valuable guidance material to support these efforts. In this chapter, we will explore how IEC 61508 can be considered from the perspective of the AMC & GM for U-space regulations, focusing on the key software engineering principles and associated software life cycle data.

IEC 61508 and key software engineering principles

IEC 61508 is an international standard for functional safety in electrical, electronic and programmable electronic systems. It addresses several key software engineering principles that align with the AMC & GM for U-space regulation, such as:

Software specification (requirements and design information)

IEC 61508 provides guidance on specifying safety requirements and design information for safety-related systems. This includes hazard and risk analysis, safety requirements specification and safety-related system and software design.

Software verification

The standard emphasises the importance of software verification, including formal methods, static and dynamic analysis and unit and integration testing.

Traceability (between items)

IEC 61508 requires traceability between safety requirements, design information, implementation and verification evidence.

Configuration and change management

The standard addresses configuration and change management, ensuring that changes to safety-related systems are controlled and documented.

Quality assurance

IEC 61508 requires quality assurance processes, such as audits, reviews and assessments, to ensure that the software life cycle processes are carried out correctly.

Guidance material in IEC 61508 for software assurance

IEC 61508 provides guidance material that can be considered for software assurance in the context of the AMC & GM for U-space regulations:

Objectives of the software life cycle processes

The standard defines objectives for each phase of the software life cycle, ensuring that safety requirements are met throughout the development process.

Activities to meet objectives

IEC 61508 describes activities for meeting the objectives of the software life cycle processes, such as requirements elicitation, design, implementation, verification and validation.

Description of the evidence, in the form of software life cycle data

The standard provides guidance on the documentation and evidence required to demonstrate that the objectives of the software life cycle processes have been met.

Particular aspects (e.g., previously developed or COTS software)

IEC 61508 addresses specific aspects, such as the integration of previously developed or commercial off-the-shelf (COTS) software and associated safety considerations.

IEC 61508 offers valuable guidance material for software assurance in the context of the AMC & GM for U-space regulations. By considering the key software engineering principles and associated software life cycle data outlined in the standard, applicants can establish a robust software assurance process that ensures the safety and reliability of their systems.

Security risk assessment

The Acceptable Means of Compliance (AMC) and Guidance Material (GM) for U-space regulations outline a security risk assessment process that can be mapped to the IEC 61508's safety lifecycle. This chapter discusses the consideration of IEC 61508 from the AMC & GM for U-space regulations, focusing on a security risk assessment perspective.

IEC 61508 and U-space regulations for a security risk assessment process

IEC 61508 provides a framework for ensuring functional safety in the development of safety-critical systems. The security risk assessment process outlined in the AMC & GM for U-space regulations can be considered an extension of the IEC 61508's safety lifecycle, focusing on the cybersecurity aspects.

Determination of the operational environment

Both IEC 61508 and the U-space regulations require defining the operational environment of a functional system. This involves identifying the system boundaries, its interaction with external systems, and the context in which it operates.

Identification of digital interfaces and assets

The IEC 61508 emphasises the identification of safety-related components and systems, while U-space regulations focus on identifying digital interfaces and assets that contribute to or sustain cybersecurity. This step aligns with the concept of identifying safety functions in IEC 61508.

Identification of attack paths

In the context of cybersecurity, identifying attack paths is a crucial step in assessing the security risks associated with a system. This process can be related to the hazard analysis performed in the IEC 61508, where potential failure modes and risks are identified.

Assessment of consequences and severity

Both IEC 61508 and the U-space regulations require assessing the consequences and severity of potential risks. While IEC 61508 focuses on safety risks, U-space regulations consider the impact of cybersecurity threats, such as denial-of-service (DoS) attacks, on the affected items.

Evaluation of potentiality for successful exploits

U-space regulations emphasise evaluating the potentiality of successful exploits, considering the typical security attributes: confidentiality, availability and integrity. This step can be mapped to the risk assessment process provided in IEC 61508, where the likelihood and consequences of hazardous events are evaluated.

Iterative approach to achieve acceptable residual risk

Both IEC 61508 and the U-space regulations advocate for an iterative approach to converge on an acceptable level of residual risk. This involves evaluating the severities in conjunction with the potential for attack, determining the acceptability of the outcome, identifying mitigation means to reach an acceptable level of safety and evaluating the effectiveness of the mitigation means with respect to the level of risk.

The security risk assessment process outlined in the AMC & GM for the U-space regulations can be mapped to the IEC 61508's safety lifecycle, highlighting the similarities between the two standards. By considering IEC 61508 from the regulatory perspective of U-space, developers can effectively apply safety and security concepts to ensure the safe and secure operation of unmanned aircraft systems in the European Union.

Conclusion

Throughout this comparison of DO-178C and IEC 61508 alongside the analysis of IEC 61508 from the perspective of the AMC & GM from U-space regulations, this report has detailed various aspects of both standards, their similarities, differences and practical applications in real-life software processes. This concluding will summarise the key findings and insights gained from this comparison and analysis.

Similarities and differences between DO-178C and IEC 61508

DO-178C and IEC 61508 are both well-established standards for ensuring the safety and reliability of safety-critical systems in their respective industries, with DO-178C focusing on airborne systems and IEC 61508 on electrical, electronic and programmable electronic safety-related systems. While both standards share similarities in terms of their systematic approach to safety, their objectives and the importance of support tools differ in the specific techniques, methods and requirements they outline for the development and verification of safety-critical systems.

Analysis of IEC 61508 from the perspective of U-space AMC & GM

U-space regulations aim to provide a safe and efficient environment for uncrewed aircraft systems operations in the European Union. The security risk assessment process outlined in the AMC & GM for U-space regulations can be directly mapped and drawn in parallel to the IEC 61508 safety lifecycle. This mapping demonstrates that IEC 61508 can serve as a foundation for U-space regulations, providing a structured and systematic approach to ensure the functional safety and cybersecurity of uncrewed aircraft systems.

Final thoughts

Both DO-178C and IEC 61508 serve as critical benchmarks in the development and validation of safety-critical systems within their respective sectors. By comprehending the commonalities, disparities and practical uses of these standards, developers are empowered to efficiently utilise the right techniques and methodologies for assuring safety and dependability.

Moreover, examining IEC 61508 through the lens of the AMC & GM in U-space regulations underscores the potential of this standard to transcend industrial domains. Importantly, the IEC 61508 standard could potentially be utilised as a comprehensive compliance solution for U-space AMC & GM requirements. It emphasises the necessity to consider functional safety and cybersecurity collectively and holistically in the development of safety-critical systems.

BIBLIOGRAPHY

European Union Aviation Safety Agency (EASA), Easy Access Rules for Unmanned Aircraft Systems – Revision from September 2022, September 2022.

European Union Aviation Safety Agency (EASA), Special Condition (SC) for Light-UAS - Medium Risk 01, December 2020.

European Union Aviation Safety Agency (EASA), Special Condition (SC) for Light-UAS - High Risk 01, December 2021.

European Commission, Commission Implementing Regulation (EU) 2021/664 on a regulatory framework for the U-space, April 2021.

European Union Aviation Safety Agency (EASA), Acceptable Means of Compliance and Guidance Material to Regulation (EU) 2021/664 on a regulatory framework for the U-space – Issue 1, December 2022.

Project reports

SHEPHERD, D1.1-D1.2 Industry standards assessment criteria and work methodology, September 2022.

SHEPHERD, D2.1-D3.1 Identification of satisfactory industry standards and justification for not acceptable industry standards (Part 1), April 2023.

European Union Aviation Safety Agency

Konrad-Adenauer-Ufer 3
50668 Cologne
Germany

Mail EASA.research@easa.europa.eu
Web www.easa.europa.eu

An Agency of the European Union