ZERO DEBRIS APPROACH AND SOFTWARE DESIGN CONSIDERATIONS

SOFTWARE PRODUCT ASSURANCE CONFERENCE 2025
22-25 September | ESA ESTEC | The Netherlands

Thales Alenia Space Italia
Gianluca Caruso
Alessandro Marini
Sante Candia

Date:
Ref:
Template: 83230347-COM-TAS-EN-012

INTRODUCTION

/// The number of man-made objects in Earth's orbit keeps growing due to space activities. This increase has accelerated recently because the space sector is evolving quickly.

/// It is crucial to minimize the impact of space operations in the orbital environment to reduce collision risks and ensure safety during re-entry.

/// Current space debris mitigation and standards are not addressing Software properly.

/// **The aim of this work is to explore these standards from a software perspective and assess their potential impacts on software products criticality classification and software products design, development and validation.**

Date:
Ref:
Template: 83230347-COM-TAS-EN-012

TABLE OF CONTENTS

RECALL ON ECSS-Q-ST-40C REV.1 - SAFETY

Space debris mitigation requirements are concerned with safety (they are recalled in the ECSS-Q-ST-40C Rev. 1)

Safety-related space debris requirements/policy are not subject to tailoring.

Final consequence of debris fallout due to uncontrolled spacecraft re-entry could include environment detrimental effect and loss of life.

e.g. Category A SW is designed and validated to mitigate the Catastrophic Safety consequences ; Loss of Life, Severe detrimental environmental effects,..

Category B is designed and validated to mitigate the Dependability effect “Loss of mission” but also the “Major Safety effects” and “Major detrimental environmental effects”.

Table 6-1: Severity categories

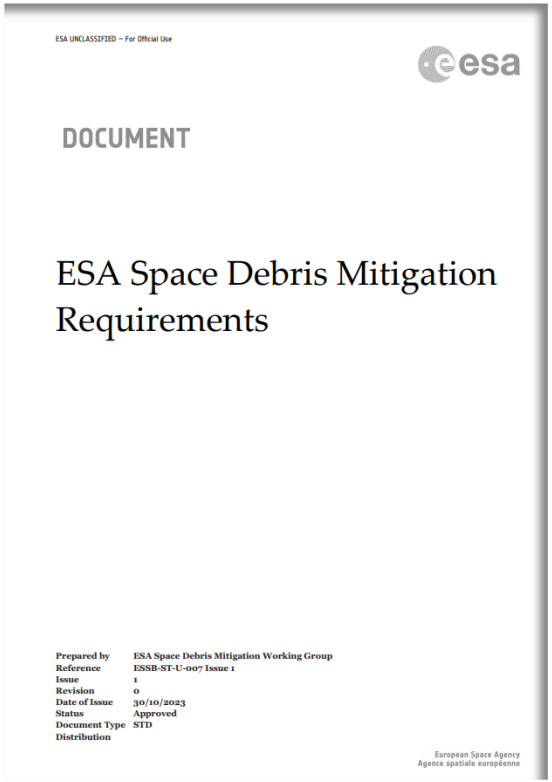
Name	Level	Type of consequences	
		Dependability	Safety
Catastrophic	1	Failure propagation (Only for lower than system level analysis) (Refer to ECSS-Q-ST-30 requirement 5.3.2.c)	• Loss of life, life-threatening or permanently disabling injury or occupational illness • Loss of system • Loss of an interfacing manned flight system • Loss of launch site facilities • Severe detrimental environmental effects
Critical	2	Loss of mission	• Temporarily disabling but not life-threatening injury, or temporary occupational illness • Major damage to an interfacing flight system • Major damage to ground facilities • Major damage to public or private property • Major detrimental environmental effects
Major	3	Major mission degradation	---
Minor or Negligible	4	Minor mission degradation or any other effect	---

Table 6-3: Criticality category assignment for software products vs. function criticality

Function criticality	Criticality category to be assigned to a software product
I	Criticality category A if the software product is the sole means to implement the function
	Criticality category B if, in addition, at least one of the following compensating provisions is available, meeting the requirements defined in clause 6.5.6.3: - A hardware implementation - A software implementation; this software implementation shall be classified as criticality A - An operational procedure
II	Criticality category B if the software product is the sole means to implement the function
	Criticality category C if, in addition, at least one of the following compensating provisions is available, meeting the requirements defined in clause 6.5.6.3: - A hardware implementation - A software implementation; this software implementation shall be classified as criticality B - An operational procedure
NOTE: It should be noted that a too high level/incomplete functional decomposition, poorly accounting for safety and dependability aspects, could lead to a unnecessarily conservative software category classification.	

Date:
Ref:
Template: 83230347-COM-TAS-EN-012

ESA SPACE DEBRIS MITIGATION REQUIREMENTS


ESA UNCLASSIFIED – For Official Use

esa

DOCUMENT

ESA Space Debris Mitigation Requirements

Prepared by	ESA Space Debris Mitigation Working Group
Reference	ESSB-ST-U-007 Issue 1
Issue	1
Revision	0
Date of Issue	30/10/2023
Status	Approved
Document Type	STD
Distribution	

European Space Agency
Agence spatiale européenne

The ESA Space Debris Mitigation standard specifies design and operational measures through to the space object end of life to:

- Prevent space debris release and proliferation
- Control system break-up risk
- Control collision risk
- Control system failure risk
- Improve orbital clearance
- Assure safe re-entry
- Minimise impact on astronomy

ESA SPACE DEBRIS MITIGATION REQUIREMENTS

Are there possible implication on Software for the following functions?

5.3 “Avoiding break-up in Earth orbit

- avoidance maneuvers capability
- autonomous passivation, as a future development

5.4 “Disposal” : Probability of successful disposal above 0,9 through to end of life

- Identification of all subsystems or components to accomplish any disposal maneuvers.
- Autonomous disposal, as a future development
- Health monitoring and prognostic approaches (on ground and/or on board), including AI approaches, as a future development

5.5 “Re-entry”

- Identification of the system functions that contribute to the controlled re-entry, if planned.

some examples

Date:
Ref:
Template: 83230347-COM-TAS-EN-012

FRENCH LAW « SPACE DEBRIS MITIGATION REQUIREMENTS »

Order of 28 June 2024 amending the Order of 31 March 2011 on the technical regulation pursuant to Decree No 2009-643 of 9 June 2009 concerning authorisations granted pursuant to Law No 2008-518 of 3 June 2008 on space operations

NOR: ECOI2413938A
ELI: https://www.legifrance.gouv.fr/eli/arrete/2024/6/28/ECOI2413938A/jo/texte
Official Journal of the French Republic No 0152 of 29 June 2024
Text No 13

Article 38-2 Validation of procedures

The procedures for controlling the space object shall be tested and validated by the operator prior to launch, with the exception of degraded cases nor requiring an immediate response from the operator, and end-of-life procedures if demonstrated that there is no risk of having to carry out an emergency withdrawal from service.

Are there possible implication on Software for the following functions?

To design, test, validate SW needed for the disposal (passivation & maneuvers) during the design phase

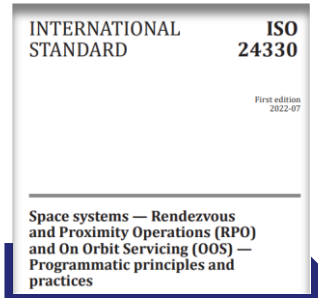
and not wait for the being close to the EoL to do this, as generally done today.

some examples

Date:
Ref:
Template: 83230347-COM-TAS-EN-012

ISO 24330 : RENDEZ-VOUS & CLOSE PROXIMITY OPERATIONS

some examples


INTERNATIONAL STANDARD
ISO 24330
First edition 2022-07
Space systems — Rendezvous and Proximity Operations (RPO) and On Orbit Servicing (OOS) — Programmatic principles and practices

Are there possible implication on Software for the following functions?

Resilient software design and verification

…. Baselining, performance verification, and the ability to update or patch in-flight are key to resilient software design that shall help ensure confidence in mission execution

The systems involved in OOS shall have software design verified for system and operational safety

SW design and verification adapted/improved for the specific safety constrains of On Orbit Servicing missions.

Update servicer spacecraft and associated operating systems (as required)

When a servicer spacecraft is already on-orbit, the servicer updates (as needed) servicer flight software and operational procedure adaptations and tests.

These functions need to be managed with dedicated spacecraft operative modes (e.g. AOCS disabled and FDIR modified for the capture phase).

KEY SOFTWARE ASPECTS TO BE ADDRESSED

Re-assess the space debris mitigation standards and investigate on possible impacts on software design and validation.

Analyze if and how the software can contribute to detrimental environmental effects and disposal activities, enabling appropriate risk mitigation.

The SW concerned with disposal and collision avoidance activities shall be considered as safety-critical.

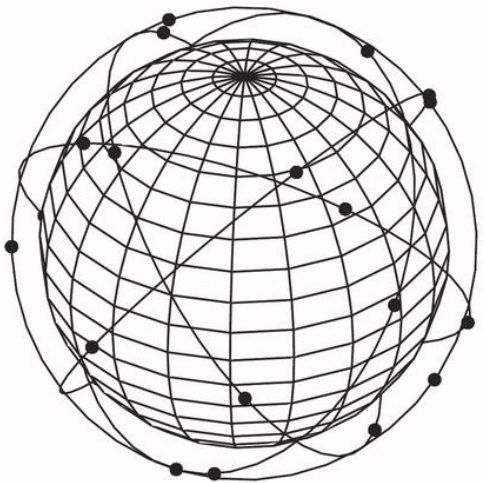
Identify future needs to meet zero debris approach.

COLLISION AVOIDANCE - IMPACTS ON SYSTEM DESIGN (1)

/// Main point to be considered in the big satellite constellation space debris mitigation is the collision avoidance topic that shall be addressed from a system level design (space segment + ground segment) : the embedded software will be one of the main contributor of the system.

/// Today Spacecraft conditions and orbit shall be constantly monitored during satellite operation, to detect any anomaly that could jeopardize its successful behaviour.

/// In the next future this kind of ground-board interaction will be not possible due to the large number of spacecraft to manage.



Date:
Ref:
Template: 83230347-COM-TAS-EN-012

COLLISION AVOIDANCE - IMPACTS ON SYSTEM DESIGN (2)

/// Collision avoidance in satellite systems is a critical function designed to protect spacecraft from potential in-orbit collisions in increasingly congested orbital environments.

/// The process relies on the satellite's ability to access a catalog of space objects and, where available, on-board sensors (e.g., cameras) to augment data.

/// The satellite continuously propagates its own orbit and compares it against the catalog to detect potential conjunctions.

/// The satellite computes the probability of collision using on-board algorithms that account for orbital uncertainties. If the computed risk exceeds a predefined threshold, the satellite autonomously generates and evaluates a set of candidate avoidance manoeuvres, considering factors such as fuel consumption, mission impact, and risk reduction.

/// The most suitable manoeuvre is selected and executed, preferably after ground intervention and approval. After the manoeuvre, the satellite verifies the new orbital state to ensure the threat has been mitigated.

/// This on-board, iterative process enhances the autonomy and safety of satellite operations in dynamic space environments.

COLLISION AVOIDANCE - IMPACTS ON SYSTEM DESIGN (3)

Breakdown into Software functionalities:

/// On-board real-time orbit propagation and collision risk assessment, computing probability of collision directly on-board. If it exceeds a mission-defined threshold the event is flagged for mitigation.

/// On-board storage and update of a Space Object Catalogue for satellites autonomous situational awareness.

/// Update of the Space Object Catalogue from ground.

/// Continuous orbit propagation algorithms coupled with on-board catalog cross-checking to assess collision risk.

/// Autonomous manoeuvre planning and execution, based on computed collision risk (see previous function).

/// Autonomous identification and execution of preparatory activities (e.g., attitude adjustments).

COLLISION AVOIDANCE - IMPACTS ON SYSTEM DESIGN (4)

/// All the previous point will be implemented trough the intensive usage of:

- **Dedicated HW for AI**: a possible simple and dedicated HW subsystem
- SW: **new AI algorithms** implementation

/// A new way to validate this kind of software shall be studied including Software Product Assurance practices to the unique challenges these solutions present.

- The current standards do not cover all challenges coming from Machine Learning.
  - The ESA handbook ECSS-E-HB-40-02A (Machine Learning handbook) - 15 November 2024 recommends guidelines applicable to the machine learning development process.
  - Other reference: ESA – TN Machine Learning and Software Product *Assurance: Bridging the Gap – YGT Report*

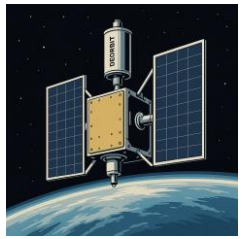
Software criticality category	Application
A	NO
B	YES
C	
D	

Date:
Ref:
Template: 83230347-COM-TAS-EN-012

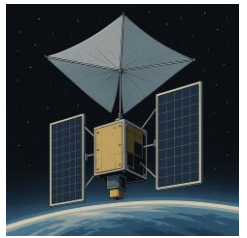
DECOMMISSIONING - POTENTIAL PLATFORMS EVOLUTION

/// Platforms need to evolve to meet the requirements of space debris : by integrating end-of-life technologies, deorbiting systems, passivation functions and design for removal.

/// Decommissioning devices/subsystems can be integrated in current platforms to remove spacecraft from orbit quickly and safely at the end of the mission.



/// Passive deorbit systems methods require no further active control after deployment. Drag devices represent the most common deorbit device for satellites orbiting in low-Earth orbit.



/// Active systems that include commanded and modulated systems, as well as independent service spacecraft will play a key role in the coming years.

Date:
Ref:
Template: 83230347-COM-TAS-EN-012

DESIGN-LEVEL COMPENSATING MEASURES

/// To assess design-level compensating measures for mitigating space debris risks resulting from potential software failures.

/// To explore and to perform analysis about the compensating provisions available in the design of the space and ground segments, in order to identify whether other software or hardware or operational means exist which can mitigate the space debris in case of software failure.

/// ECSS-Q-ST-40C compensatory strategy as enabler of moderation of SW criticality.

/// Segregated, dedicated and simple decommissioning subsystems are the clean and robust evolution for the new Platforms:

- They can be treated with the adequate level of criticality without jeopardizing the Avionics Subsystem.
- Dedicated HW and SW can be co-designed to build up simple and robust solutions to be classified either at Criticality Level A or B.

/// Extensive usage of new AI technology and algorithms:

- New validation approach shall be studied.

DESIGN SOFTWARE TO SUPPORT NEW FEATURES

Key design drivers for the SW supporting a decommissioning subsystem:

/// Criticality level : safety critical SW is either A or B (implying ISVV and, optionally, a third-party development).

/// Minimal footprint:

- Dedicated Application-level functions (AOCS modes/submodes).
- Reduced PUS standard services with dedicated configuration to support basic on-board functions (TC management, pre-defined observability, events management, time management, pre-defined monitoring & event-action management).
- Reduced basic services and HW drivers.

/// Full ECSS life cycle applicability (as per Level A or B).

/// Early HW/SW Co-engineering activity to address specific SW needs.

CONCLUSION PART 1 – CONSIDERATION ON THE STANDARDS

European space debris mitigation standards	• Standards are not mentioning Software explicitly. In our opinion, they should. Moreover ECSS Q30-40 and Q80 standards do not specifically mention new debris standards.
Working groups	• Working groups on environmental effects questions need to be focused also to Software.
Safety standards and Software standards	• Definition of safety catastrophic and safety critical for what concerns the environmental effects has not changed after the new space debris mitigation standards. (same definition from 2017).

Date:
Ref:
Template: 83230347-COM-TAS-EN-012

CONCLUSION PART 2 – SYSTEM DESIGN AND SOFTWARE DESIGN

SW parts concerned with disposal operations and collision avoidance	• The current applicability for the **development category for all SW parts concerned with disposal operations** (passivation, EoL manoeuver execution) **and collision avoidance** is via ECSS Q-40 and Q-80. The hazard the SW has to control are critical or catastrophic in nature. (polluting the LEO orbit, Earth reentry hazard o population)
Technological evolution	• The promotion of technological evolution toward less expensive missions shall consider also software architectural design evolutions and platform evolutions together with the willingness to integrate debris approach in SW requirements objectives.
Design and its associated safety	• The design and its associated safety shall be considered at system level (space segment + ground segment). • Mitigation and safety measures analysis shall effectively begin from the project start with the system-level safety and dependability analyses that identify critical functions, including software, to analyze if and how the software can contribute to detrimental environmental effects and disposal activities, enabling appropriate risk mitigation. • The main recommendation is to establish a system level FMEA to identify critical functions including SW concerned with disposal activities and so to allow and address the proper risk mitigations.

ESA SPACE DEBRIS MITIGATION WEB PAGE

https://technology.esa.int/page/space-debris-mitigation

1) Policy:
ESA Space Debris Mitigation Policy (2023)

2) Standards (Requirements):
ESSB-ST-U-007, Issue 1 - ESA Space Debris Mitigation Requirements – 30/10/2023
ESSB-ST-U-004 - ESA Re-entry Safety Requirements - 04/12/2017

ECSS-U-AS-10C, Rev .2 - Space Sustainability - Adoption Notice of ISO 24113: Space Systems - Space debris mitigation requirements - 09/02/2024

ISO 24113:2023 - Space systems - Space debris mitigation requirements
ISO 24330 : Space systems — Rendezvous and Proximity Operations (RPO) and On Orbit Servicing (OOS) — Programmatic principles and practices

3) Handbooks:
ESSB-HB-U-002 - ESA Space Debris Mitigation Compliance Verification Guidelines - 14/02/2023

4) Supporting document:
Compliance matrix to ESSB-ST-U-007, template in excel format, 01/10/2024
ESA's Space Debris Mitigation Requirments - training - 7th October 2024

ZERO DEBRIS APPROACH AND SOFTWARE DESIGN CONSIDERATIONS

SOFTWARE PRODUCT ASSURANCE CONFERENCE 2025
22-25 September | ESA ESTEC | The Netherlands

THANK YOU !

Gianluca Caruso
gianluca.caruso@thalesaleniaspace.com

Alessandro Marini
alessandro.marini@thalesaleniaspace.com

Sante Candia
sante.candia@thalesaleniaspace.com

Web: www.thalesaleniaspace.com