

# Standardization training program

## Q-40 discipline:

### Safety

15/10/2019

ESTEC

COPYRIGHT NOTICE: By using the ECSS Training material, developed by ESA, you agree to the following conditions: 1. The training shall take place at your premises and shall be addressed to your staff (internal participants); 2. In case of a training to be given to external participants, the prior ESA written authorisation shall be requested; 3. The ESA Copyright shall always be mentioned on all Training Material used for the purpose of the training and participants shall acknowledge the ESA ownership on such a Copyright; 4. The Training material shall not be used to generate any revenues (i.e. the training and Training Material shall be "free of charge" excl. any expenses for the training organisation); 5. Only non-editable PDF files of the Training Material can be distributed to the participants (nor power point presentations); 6. Any deficiency identified in the Training Material shall be reported to the ECSS secretariat; 7. If the Training Material is modified or translated, the ESA Copyright on such edited Training Material shall be clearly mentioned. A copy of the edited Training Material shall be delivered to ESA for information. 8. You shall always hold harmless, indemnify and keep ESA indemnified against any and all costs, damages and expenses incurred by ESA or for which ESA may become liable, with respect to any claim by third parties related to the use of the Training Material.

# ECSS-Q-ST-40C: Safety

Fabio Restagno

Dependability (RAM) and Safety Section (TEC-QQD)

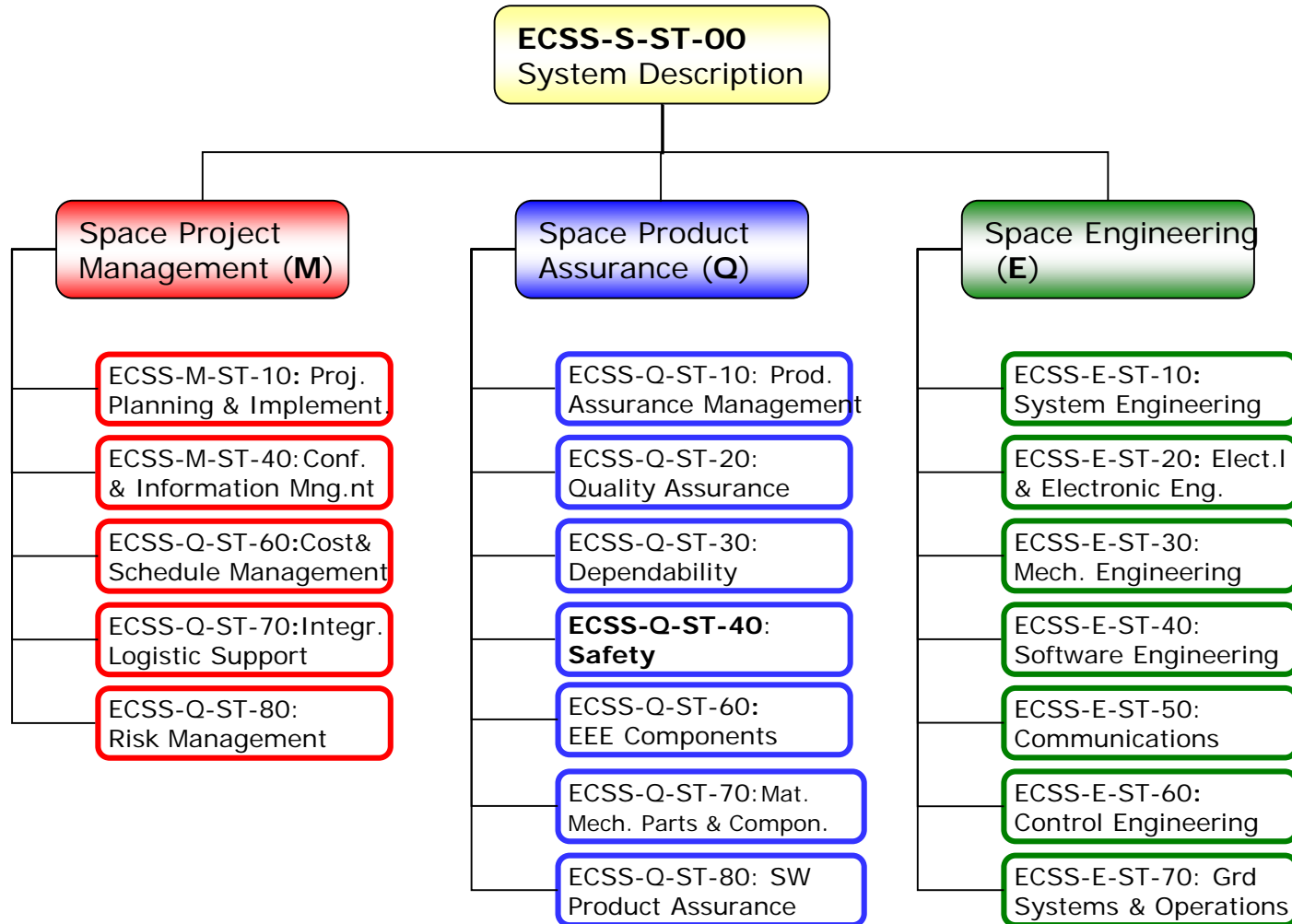
Quality, Dependability and Safety Division

Safety is important in all the industrial and civil activities:

“Safety is a state in which the risk of harm to persons or damage is limited to an acceptable level.” **(ISO 8402:1994)**

In Space Projects and Industry, Safety is an integral part of all project product assurance and engineering activities (it is not a stand-alone activity).

The quality of all safety engineering related work is based on assurance that the system is designed, qualified, manufactured, and operated in accordance with the ECSS product assurance policy and requirements.



# List of more commonly used ECSS of the Q series



- ECSS-Q-ST-40C (Rev.1) Safety
  - ECSS-Q-ST-40-02C Hazard Analysis
  - ECSS-Q-ST-40-12C Fault Tree analysis-Adoption notice ECSS/IEC 61025
- } Safety

ECSS – QA, PA,

Dependability and Materials:

- ECSS-Q-ST-10C Product assurance management
- ECSS-Q-ST-10-04C Critical-item control
- ECSS-Q-ST-10-09C Non conformance control system
- ECSS-Q-ST-20C Quality assurance
- ECSS-Q-ST-20-10C Off-the-shelf items utilization in space systems
- ECSS-Q-ST-30C Dependability
- ECSS-Q-ST-30-02C Failure modes, effects (and criticality) analysis (FMEA/FMECA)
- ECSS-Q-ST-30-09C Availability analysis
- ECSS-Q-ST-30-11C Derating – EEE components
- ECSS-Q-ST-70C Materials, mechanical parts and processes
- ECSS-Q-ST-70-01C Cleanliness and contamination control
- ECSS-Q-ST-70-21C Flammability testing for the screening of space materials
- ECSS-Q-ST-70-36C Materials selection for controlling stress-corrosion cracking
- ECSS-Q-ST-80C Software product assurance

# A List of ECSS of the E series (with relevance with Safety)



## Design and Engineering:

- ECSS-E-ST-10C System engineering general requirements
- ECSS-E-ST-10-02C Verification
- ECSS-E-ST-10-04C Space environment
- ECSS-E-ST-10-11C Human Factors engineering
- ECSS-E-ST-20C Electrical and electronic
- ECSS-E-ST-20-07C Electromagnetic compatibility
- ECSS-E-ST-31C Thermal control general requirements
- ECSS-E-ST-32C Structural general requirements
- ECSS-E-ST-32-01C Fracture control
- ECSS-E-ST-32-02C Structural design and verification of pressurized hardware
- ECSS-E-ST-32-08C Materials
- ECSS-E-ST-32-10C Structural factors of safety for spaceflight hardware
- ECSS-E-ST-33-01C Mechanisms
- ECSS-E-ST-33-11C Explosive systems and devices
- ECSS-E-ST-34C Environmental control and life support (ECLS)
- ECSS-E-ST-35C Propulsion general requirements
- ECSS-E-ST-35-01C Liquid and electric propulsion for spacecraft
- ECSS-E-ST-35-03C Liquid propulsion for launchers
- ECSS-E-ST-40C Software
- ECSS-E-ST-50C Communication

ECSS-Q-ST-40C Rev.1 ( 15 Feb 2017) Safety,

It defines the safety programme and the safety technical requirements to protect:

- Flight, ground personnel and the general public,
- The launch vehicle, associated payloads, ground support equipment, the space system and associated segments and facilities,
- Public and private property,
- The environment from hazards associated with European space systems.

This Standard is applicable to all European space projects.



The objective of safety assurance is to ensure that all safety risks associated with design, development, production and operations of space products are:

- **Identified**
- **Assessed**
- **Eliminated (when feasible)**
- **Minimised**
- **Controlled**
- **And finally accepted**



Through the implementation of a **Safety Assurance Programme**.

The ECSS-Q\_ST-40C Rev.1 safety policy is implemented by applying a **Safety Programme** that has the scope to ensure that:

- Safety is designed into the system,
- Safety controls are adequately implemented in the verification plan,
- Safety requirements including launch centre safety regulations are met,
- Hazards are identified, and eliminated or, where this is not possible, minimized, ranked and controlled in accordance with project objectives in a manner acceptable to the Customer and to the Safety Organisations involved in the implementation of the mission.

To assure conformance with project safety policy and requirements, the Supplier establish , implement and maintain a **safety programme plan** that covers the **safety tasks** for the phases of the project.

- **Creation of a safety organization and Nomination of a safety manager**

In particular, each supplier has to **appoint a safety manager** who has appropriate safety training or experience.

- **Identification and flow down of the Safety Requirements**

The **safety requirements**, applicable to the project, have to be identified, apportioned and flown down to each subcontractor.

- **Identification and management of the hazards, Safety is designed into the System, Safety controls are adequately implemented and verified**

(The **safety analysis** is a key tool for this process and has to be performed, updated and maintained for each phase of the project.)

## Safety Manager



- Has organizational authority and independence to establish and maintain the Project Safety Programme
- Manages the Safety Assurance Aspects of the Design & Operations
- Coordinate the interfaces:
  - with the relevant bodies involved in the project in accordance with the safety plan,
  - with the **safety launcher authority**.

Depending on the project safety criticality, the safety manager can be combined with other functions (e.g. PA manager) when agreed with the customer.



## Safety Manager Approval authority



To be reviewed and approved by the Safety Manager:

- Documentation related to safety
- Hazardous operations.



## Representation on boards



S.M. is represented at:

- **CCBs** (Configuration Control Board)
- **NRBs** (Nonconformance Review Boards)
- **TRBs** (Test Review Boards)
- **Qualification & Acceptance Reviews** involving safety requirements or safety-critical functions.

## Safety Manager Access



Right of access to safety relevant data



Unimpeded access to any management level on project safety aspects

## Safety Manager Authority

If do not conform to Approved:

- Safety Requirements
- Safety Procedures
- Safety Measures.



Safety Manager can:

Reject any Project Document

Stop any Project Activity



Interrupt hazardous operations

## Safety approval authority

In the frame of the **Safety Review**, the safety approval authority will :

- Review the safety data submittals (including the Hazard Reports),
- Approve the close-out of hazard reports,
- Decide on deviations and waivers,
- Accept the statement of safety compliance.

The Risk identification, reduction and control is part of the project's risk management process (as specified in **ECSS-M-ST-80**) and is a continuous and iterative process throughout the project life cycle, encompassing:

- Allocation of Safety Requirements
- Hazard and Safety Risk identification
- Evaluation (including categorisation) of consequence severity
- Hazard and Safety Risk Reduction and Control.
- Verifications Close out and acceptance of residual risk.



## Typical Applicable Safety Requirements Documents:

The ECSS-Q-ST-40C Space Product Assurance,

The Launcher Safety Documents,

*(e.g. CSG-NT-SBU-166-CNES Payload Safety Handbook it is the Launcher applicable document when the Payload is launched from Kourou)*

The Project Safety Requirements are generated from the Applicable Safety documents and standards.

The following approach is required:

- The supplier has to comply with the Project applicable safety requirements and with all the applicable national or international safety regulations.
- The launch site safety regulations and rules have to be applied.
- The implementation of safety requirements has not to be compromised by other requirements (for example: security requirements).

## **Safety Requirements allocation and traceability:**

Safety requirements have to be identified and traced from the system level into the design and allocated to the lower levels.

## **Safety Documentation**

The supplier has to maintain, as part of the project documentation, all safety-related data to support reviews and safety compliance demonstration and the customer has right of access to it.

The Safety Documentation is prepared and completed through the preparation and development of specific Safety Documents:

**1. The Payload Ground Safety Analysis** (Safety Hazard Analysis), this document is required by, and has to be submitted to, the Launcher Safety Authority.



- It considers hardware design, verification, testing, and ground operations and will cover all the activities that are performed at the Launcher Facilities and the Launcher ascent up to the Payload separation.

**2. The Flight Safety Analysis**, this document is performed on human spaceflight missions.



- It considers hardware design, verification, testing, and flight operations

**3. The re-entry Safety Analysis**, this document is performed for any spacecraft re-entering into the earth atmosphere

The supplier prepare and submit a **Safety Data Package (SDP)** to support reviews



- The safety analyses work and results are documented in the Safety Data Package (SDP) that is the document which include and collects the safety analyses evolution , all the hazard reports and all the supporting safety documentation.
- The SDP is the document that will be submitted to the Launcher Safety Authority.



## Safety Data Package:

The SDP must be a stand-alone package, has to guarantee the traceability of all the safety data, has to meet the objectives of the safety reviews and must be in line with the requirements of the Safety Approval Authority.

The SDP has to contain: the System Safety Analysis (as it evolves along the life of the project including and integrating safety data related to the various subsystems or equipment that makes up the system), the Supporting analyses, the safety risk assessments, the hazardous operations lists and procedures, the safety related RFDs/RFWs, the Safety Verification Tracking Log (VTL)

To perform the Safety Analysis the following **systematic approach has to be performed** throughout all life cycle phases:

- Define the system
- Identify the hazards (hazard scenario identification)
- Assign to each hazard its relevant severity
- Identify the system functions involved in the hazard and define their criticality level in line with the Hazard severity
- Apply the hazard reduction approach (elimination, minimization, control)
- Identify the causes generating the hazards
- Identify safety-critical software
- Identify controls and corrective actions
- Identify the Verification criteria that demonstrate that the controls are appropriate and in place
- Accept the risk
- Provide documentation

# Safety risk reduction and control

## Severity of hazardous event and function criticality



Safety risk reduction & control → **Severity categories** The severity of potential consequences of identified hazardous events is categorized as per the following table. (ECSS-Q-ST-40C Table 6-1).

Severity	Level	Dependability (refer to ECSS-Q-ST-30) <i>Extract from ECSS-Q-ST-30</i>	Safety (ECSS-Q-ST-40)
<b>Catastrophic</b>	1	Failures propagation	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.
<b>Critical</b>	2	Loss of mission	Temporarily disabling but not life-threatening injury, or temporary occupational illness; ----- Major damage to interfacing flight system; ----- Major damage to ground facilities; ----- Major damage to public or private property; ----- Major detrimental environmental effects.
<b>Major</b>	3	Major mission degradation	---
<b>Minor or Negligible</b>	4	Minor mission degradation or any other effect	---
NOTE: When several categories can be applied to the system or system component, the highest severity takes priority			



# Safety risk reduction and control

## Severity of hazardous event and function criticality



The **criticality of a function** implemented in the space system is assigned in accordance with the severity of identified hazardous events it can cause, following the categories defined in ECSS-Q-ST-40C rev 1; Table 6-2.

Severity of hazardous event	Function criticality	Criteria to assign criticality categories to functions
Catastrophic (Level 1)	I	A function that if not or incorrectly performed, or whose anomalous behaviour can cause one or more hazardous events resulting in catastrophic consequences
Critical (Level 2)	II	A function that if not or incorrectly performed, or whose anomalous behaviour can cause one or more hazardous events resulting in critical consequences

The highest identified severity of hazardous events shall define the criticality of the function.

The function criticality shall be assigned without taking into account any compensating provisions.

Hazards that have not been **eliminated** and have been subjected to **hazard minimization** have to be **controlled** through preventative or mitigation measures, which are introduced into the system design and operation to avoid the events or to interrupt their propagation to consequences.

Measures are applied with the following order of precedence:

- Design selection (Failure Tolerance, Design for Min. Risk, SW Crit. Categories)
- Automatic safety devices
- Design to contain
- Warning devices
- Crew escape; Safe Haven
- Special procedures.

Safety risk reduction & control → **Mitigation criteria: Failure tolerance.**

Failure tolerance is the basic safety requirement that is used to control most hazards; it is the primary and preferred approach.

The level of fault tolerance to be implemented in the design is determined by the hazard consequence.

2F.T. -> to control hazards that could lead to catastrophic consequences

1F.T -> to control hazards that could lead to critical consequences

Safety risk reduction & control → Typical failure tolerance requirements

- No single system failure or single operator error shall have critical or catastrophic consequences.
- No combination of two independent system failures or operator errors shall have catastrophic consequences.
- Safety inhibits shall be independent, verifiable, stable and stay in a safe position even in case of energy failure.
- Multiple failures, which result from common-cause or common-mode failure mechanism, shall be analysed as single failures to determine failure tolerance.

Safety risk reduction & control → **Design for minimum risk**

“Design for minimum risk” is a safety requirement used to control hazards by specifying safety-related properties and characteristics of the design.

Design for minimum risk is applied for example when in the design are present:

structures, pressure vessels, rotating equipment, energy stored devices, mechanisms, flammability, materials compatibility.

Safety risk reduction & control → Design for minimum risk

## Safety Factors

**Structural Safety factors** are defined and applied in accordance with ECSS-E-ST-32-10C – Structural factors of safety for spaceflight hardware - and with **safety margins** based on Worst credible combinations of environmental conditions.

Structural failures leading to catastrophic or critical consequences have to be designed implementing the **Fracture Control** approach (in accordance with ECSS-E-ST-32-01C – Fracture Control)

# Hazards Control – 5 (Factors of Safety from ECSS-E-ST-32-10C)



**Table 4-3: Factors of safety for metallic, FRP, sandwich, glass and ceramic structural parts**

Structure type	Vehicle	Requirements			
		FOSY	FOSU	FOSY verification by analysis only	FOSU verification by analysis only
Metallic parts	Satellite	1,1	1,25	1,25	2,0
	Launch vehicle	1,1	1,25	See Note <sup>c</sup>	2,0
	Man-rated S/C Launch On Orbit	1,25 1,1	1,4 1,5	See Note <sup>c</sup>	See Note <sup>c</sup>
FRP parts (away from discontinuities)	Satellite	N/A	1,25	N/A	2,0
	Launch vehicle	N/A	1,25	N/A	2,0
	Man-rated S/C Launch On Orbit	N/A N/A	1,5 2,0	N/A N/A	See Note <sup>c</sup>
FRP parts (discontinuities) <sup>a</sup>	Satellite	N/A	1,25	N/A	2,0
	Launch vehicle	N/A	1,25	N/A	2,0
	Man-rated S/C	N/A	2,0 <sup>b</sup>	N/A	See Note <sup>c</sup>
Sandwich parts: - face wrinkling - intracell buckling - honeycomb shear	Satellite	N/A	1,25	N/A	2,0
	Launch vehicle	N/A	1,25	N/A	2,0
	Man-rated S/C	N/A	1,4	N/A	See Note <sup>c</sup>
Glass and ceramic structural parts	Satellite	N/A	2,5	N/A	5,0
	Launch vehicle	N/A	See Note <sup>c</sup>	N/A	See Note <sup>c</sup>
	Man-rated S/C	N/A	3,0	N/A	See Note <sup>c</sup>

<sup>a</sup> e.g.: holes, frames, reinforcements, steep change of thickness.  
<sup>b</sup> This value is for consistency with NASA-STD-5001 and already include a KLD factor.  
<sup>c</sup> No commonly agreed value within the space community can be provided.

**Table 4-4: Factors of safety for joints, inserts and connections**

Structure type	Vehicle	Requirements			
		FOSY	FOSU	FOSY verification by analysis only	FOSU verification by analysis only
Joints and inserts: - Failure - Gapping - Sliding	Satellite	N/A N/A N/A	1,25 N/A N/A	N/A 1,25 1,25	2,0 N/A N/A
	Launch vehicle	N/A 1,1 1,1	1,25 N/A N/A	N/A	N/A
	Man-rated S/C	See Note <sup>c</sup>	1,4 1,4 1,4	See Note <sup>c</sup>	See Note <sup>c</sup>
Elastomer system and elastomer to structure connection <sup>b</sup>	Satellite	See Note <sup>c</sup>	2,0	See Note <sup>c</sup>	See Note <sup>c</sup>
	Launch vehicle	See Note <sup>c</sup>	2,0	See Note <sup>c</sup>	See Note <sup>c</sup>

<sup>a</sup> These factors are not applied on the bolts preload – see threaded fasteners guidelines handbook (ECSS-E-IB-32-2).  
<sup>b</sup> Analysis and test are performed to show that the possible non linear dynamic behaviour of the elastomer does not jeopardize the satellite strength and alignment.  
<sup>c</sup> No commonly agreed value within the space community can be provided.

**Table 4-5: Factors of safety for buckling**

Vehicle	Requirements			
	FOSY	FOSU	FOSY verification by analysis only	FOSU verification by analysis only
Satellite	See Note <sup>a</sup>	1,25	See Note <sup>a</sup>	2,0
Launch vehicle	- Global	N/A	1,25	See Note <sup>a</sup>
	- Local	1,1	1,25	2,0
Man-rated S/C	See Note <sup>a</sup>	1,4	See Note <sup>a</sup>	N/A

<sup>a</sup> No commonly agreed value within the space community can be provided.

**Table 4-6: Factors of safety for pressurized hardware**

Vehicle	Requirements			
	FOSY	FOSU	FOSY verification by analysis only	FOSU verification by analysis only
Satellite	1,1	1,25	See Note <sup>a</sup>	See Note <sup>a</sup>
Launch vehicle	1,1	1,25	See Note <sup>a</sup>	See Note <sup>a</sup>
Man-rated S/C	1,25	1,4	See Note <sup>a</sup>	See Note <sup>a</sup>

<sup>a</sup> No commonly agreed value within the space community can be provided.

Safety risk reduction & control → Design for minimum risk.

## Materials:

Typical hazards deriving from materials are: toxicity, flammability, stress corrosion, outgassing, offgassing, radiation, thermal cycling, arc tracking, thermal degradation, resistance to cleaning fluid and microbiological growth.

## Materials Mechanical parts and Processes are:

- Selected and controlled in accordance with ECSS-Q-ST-70C (Materials, mechanical parts and processes).
- Material selection is applied to assure that hazards due to material are either eliminated or controlled.
- If this is not feasible to eliminate hazardous or prohibited materials from the design, the system shall include provisions to control hazardous events associated with material characteristics.
  - Eg. Containment of hazardous substances.



## Hazard control – Software Criticality:

- **Identify the Functions and define their criticality** (Req – 6.5.1)  
*A function that, if lost or degraded, or through incorrect or inadvertent operation, can result in a catastrophic or critical hazardous consequence, shall be identified as a safety-critical function.*
- **Identify the associated SW** (Req – 6.5.6.1)
  - *Safety aspects associated with the software function shall be an integral part of the overall system safety efforts and not be assessed in isolation.*
  - *A software product shall be considered safety-critical if it implements or affects one or more functions of which at least one has a criticality I or II, as defined in clause 6.4.1*
- **Assign the SW criticality category** (Req 6.5.6.3)
  - *The criticality of a software product (A,B,C) shall be assigned, based on the criticality assigned to the most critical function it implements, and meeting the criteria defined in Table 6-3 and requirements 6.5.6.3b to 6.5.6.3g.*
  - *The criticality of software products shall be assigned considering the overall system design, and in particular whether hardware, software or operational means as compensating provisions exist which can prevent software-caused system failures or mitigate their consequences.*

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: <ul style="list-style-type: none"> <li>- A hardware implementation</li> <li>- A software implementation; this software implementation shall be classified as criticality A</li> <li>- An operational procedure</li> </ul>
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: <ul style="list-style-type: none"> <li>- A hardware implementation</li> <li>- A software implementation; this software implementation shall be classified as criticality B</li> <li>- An operational procedure</li> </ul>
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.	

A system shall be in place that tracks all hazards and related risks, to relate all verifications of the corresponding hazard uniquely to unambiguous causes and controls.

## Hazard reporting and review:

To successfully complete the safety process, positive feedback has to be provided on completion results for all verification items associated with a given hazard.

The supplier has to report, and provide evidence, that

- controls are defined and agreed;
- verification methods are defined and agreed;
- verification is completed

If verification cannot be completed, the supplier shall establish a Safety Verification Tracking Log (SVTL).

## Verification engineering and planning

- Verification engineering select the verification methods consistent with the verification requirements documented in the hazard report and with the launch base safety rules.
- Verification planning commence in an integrated manner upon selection of the control method.

## Verification methods and report

Safety verification methods shall include alternatively or in combination:

- review of design
- analysis
- inspection
- test

For all safety verifications, traceability has to be provided.

## Hazard close-out

### Safety assurance verification

A Safety Verification Tracking Log (SVTL) is established to collect all the open verification items of the different hazard reports from the safety analysis.

In time for acceptance by the customer, and in preparation of transfer to the next stage of system integration, the safety manager has to verify that:

- hazard close-outs performed are still valid;
- the verifications reflect the as-built or as-modified status of the hardware;
- all open verifications at this time are acceptable for transfer to the next stage of system integration;
- all open verifications are entered into the verification tracking log (SVTL);
- the Verification Tracking Log is maintained to reflect the current status.

If the safety verification constrains any ground operations, the safety manager has to give notification to the safety review panel.

## Hazard close-out verification

The safety manager has to assure that each hazard considered for closure has the approval by the safety approval authority verifying that:

- hazards not eliminated are controlled in accordance with the applicable requirements and associated verification activities are successfully completed.
- deviations from, or waivers of requirements, are granted by the safety approval authority.

The safety analysis shall be performed, updated and maintained for each phase of the project:

- Phase 0 -> Mission analysis/Needs identification
- Phase A -> Feasibility
- Phase B -> Preliminary definition
- Phase C/D -> Detailed definition, production & qualification testing
- Phase E -> Utilization
- Phase F -> Disposal



## Mission analysis/Needs identification- Phase 0

The Safety analysis is performed to support the identification of sources of safety risks as well as the performance of preliminary trade-off analyses between alternative system concepts.

## Feasibility – Phase A.

The Safety analysis has the purpose to support trade-off analyses in arriving at a concept that has acceptable safety risk considering the project and mission constraints.

The design technology selected and the operational concept to be implemented are selected based on the analysis of data for the safest system architecture to eliminate or reduce hazards to acceptable levels.

## Preliminary definition – Phase B

The safety analysis has the purpose to support a continued and more detailed safety optimization of the system design and operations and the identification of technical safety requirements and their applicability.

The analysis is used also to provide inputs to safety risk assessment in support of safety risk evaluation and to the identification of risk contributors in the design and in the operational concept.

## Detailed definition, production & qualification testing – Ph. C/D

The Safety analysis has the purpose to support:

- detailed design, production, qualification, testing.
- operational safety optimization, safety requirements implementation evaluation, risk reduction verification, and hazard and risk acceptance.

Analysis of operations is also performed to support the identification of emergency and contingency response planning and training requirements, and the development of procedures.

## Utilization – Phase E

The Safety analysis has the purpose to evaluate design and operational changes for impact to safety, assuring that safety margins are maintained and that operations are conducted within accepted risk.

The analysis has also the purpose to support the evaluation of operational anomalies for impact to safety, and the continued evaluation of risk trends.

## Disposal – Phase F

Safety analysis has the purpose to evaluate all disposal operations and associated hazards and to identify the Disposal solutions which meet the project's safety requirements.

The Hazard Analysis is the main tool, that is delivered at each review to document the results of the safety activities, (project reviews and safety reviews).

The Hazard Analysis is the principal deterministic safety analysis which assist engineers and managers in addressing and implementing the safety aspects in engineering practices and decision making process throughout the process life cycle in design, construction, testing, operation, maintenance and disposal.

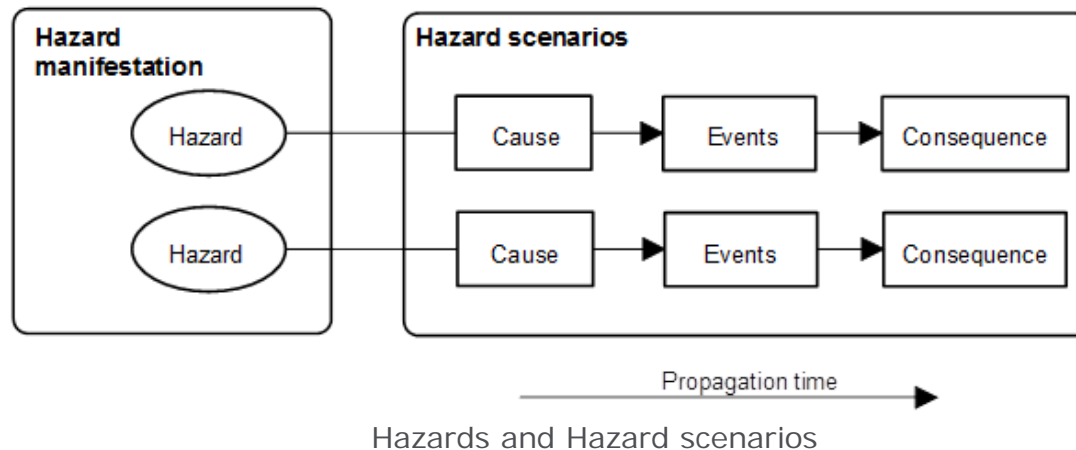
The hazard analysis process comprises the steps and tasks necessary to identify and classify hazards.

Hazard analysis is a System level task. The prime contractor perform it and then request support and inputs to the lower level contractors.

Hazard analysis (ref. to ECSS-Q-ST-40-02C) is based on the following hazard analysis concept:

Hazards, which are present through hazard manifestations in the system, are activated if initiating events (i.e. cause) occur.

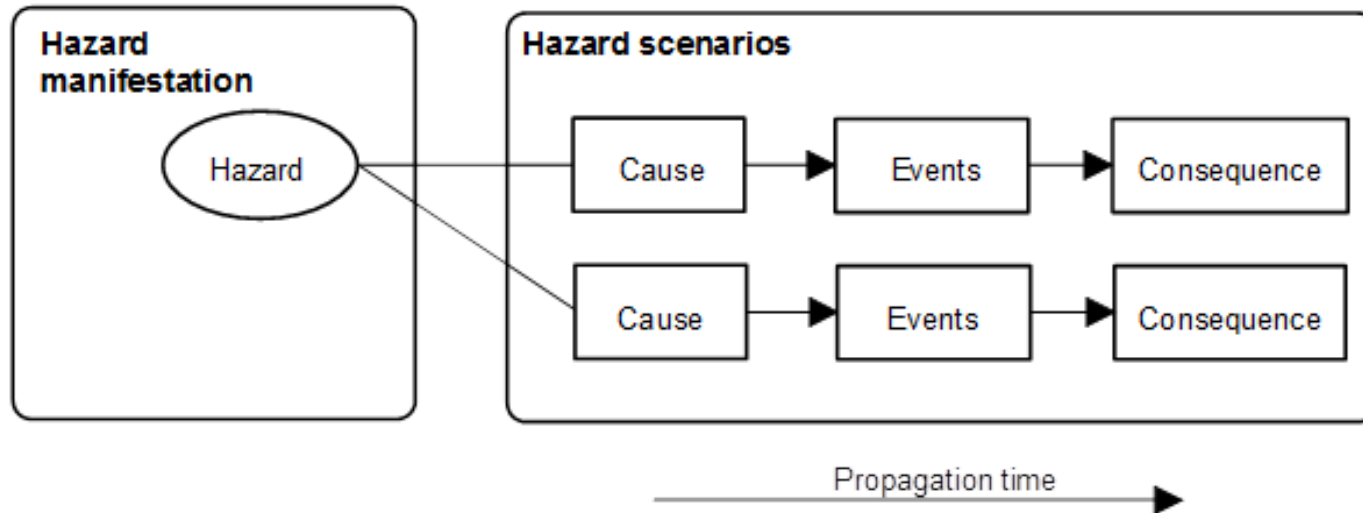
Hazard scenarios reflect the system behaviour to the activated hazards in terms of event propagation from causes to safety consequences.



Safety consequences are characterized by their severity.



Different hazard scenarios can originate from the same hazard:



NOTE:

Hazards can be:



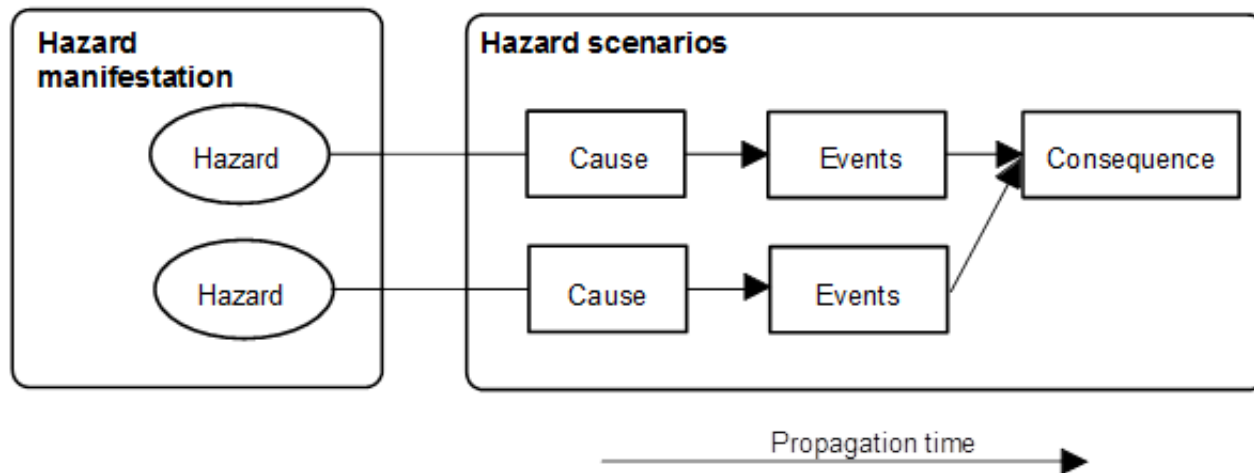
- an intrinsic property of an item or of an entity, (e.g. radioactive sources).

or

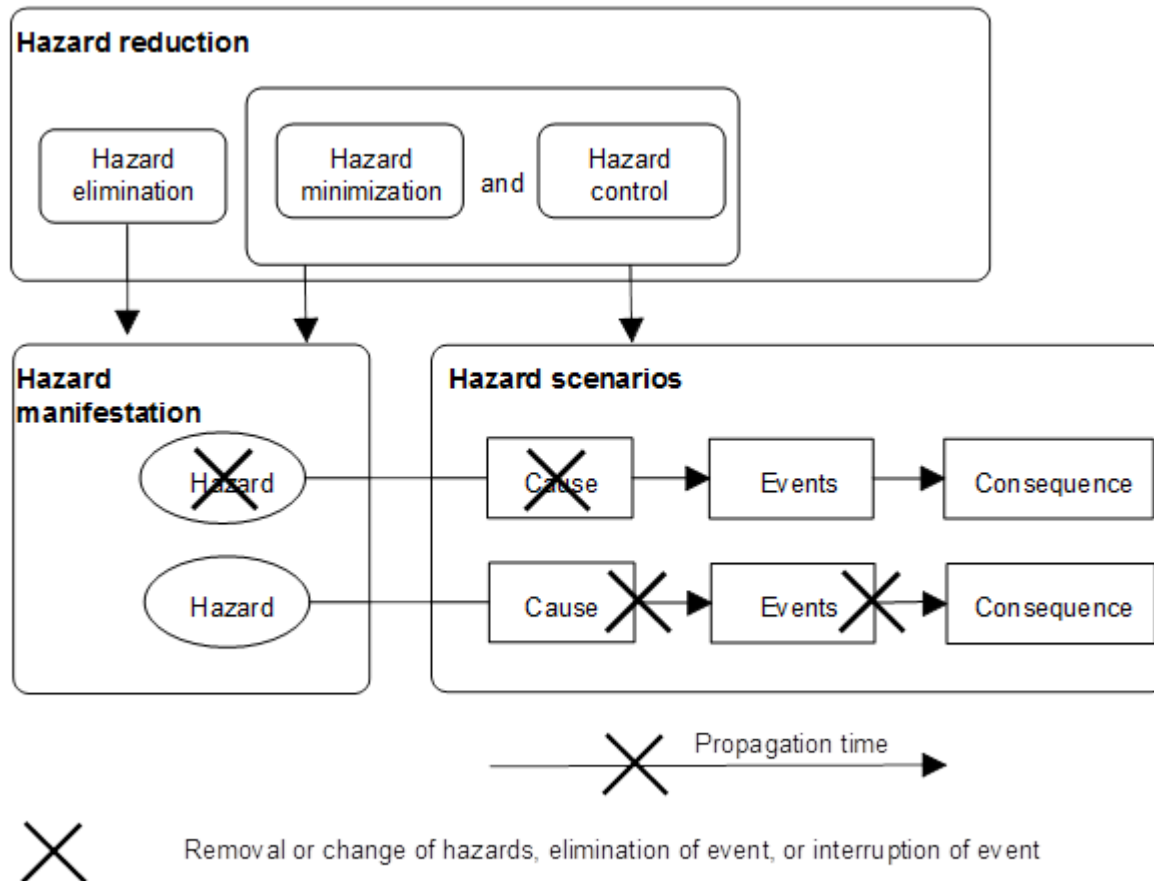


- a functional/physical state of an item or of an entity (e.g. High Pressure in a Vessel; High Temperature of a surface).

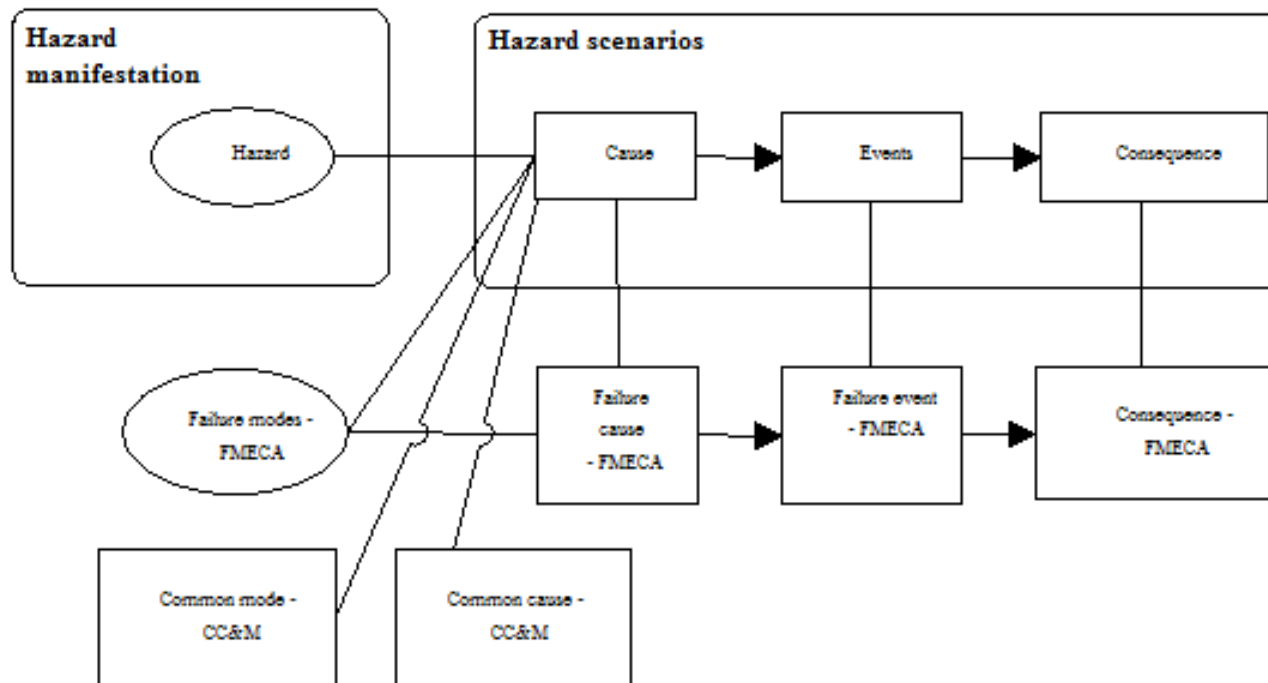
The collection of hazard scenarios leading to the same safety consequence is collated into a consequence tree:



Hazards are reduced by either eliminating them or, if this is not possible, by minimizing and controlling them:



Hazards Analysis is developed in correlation with the other dependability analyses (e.g. FMEA, CC&CM analysis):



## Interface to FMEA and CC&CM analysis

# Hazard Analysis –how to perform it hazard trees & hazard scenarios



The Hazard Analysis is a top-down analysis.

The basic step to perform the hazard analysis is to start from the Hazard Trees, (they can be done in a fault-tree like approach).

The Hazard tree/s provide the starting point to create and analyse the Hazard Scenarios.

The Hazard scenarios will be developed considering each phase of the project: ground phase, launch and ascent, flight, re-entry...

The Hazard Scenarios are then collected and described inside the Hazard Reports.

The hazard reports provide the safety needed data and information.




The purpose of the hazard reports is to document the safety assessment of the spacecraft in a manner that reflects how the its design demonstrates compliance with the safety requirements.

The hazard reports are used as a method to systematically assess compliance with the safety requirements.


The flight Safety Data Package (for manned missions) will contain all flight hazard reports;

The ground Safety Data Package will contain all ground hazard reports.

Refer to the Hazard Tree flow  
(VISIO FORM)

When performing the hazard analysis it is important to identify the hazardous events  that can cause the Top Event  (used as starting point of the hazard tree) and that could occur through the hazard manifestations. 

To identify the hazardous events and the hazard manifestations the safety engineer can start from lists of Hazardous events and generic hazards.

To identify the hazard manifestations that could occur in the project life is useful to make use of lists of generic hazards that can guide in the identification of the potential hazards present in the system design and operations. 

To develop exhaustive lists that are representative for the project, its design and operations, it is useful to use the inputs from the functional analysis and to identify the environmental conditions that will be faced during the different phases of the project.



Herewith is provided an example of a List for Hazardous Events that can be used as starting point for further improvement depending the design and operations:

- COLLISION
- CONTAMINATION
- ELECTRICAL SHOCK
- ELECTRICAL SHORTS
- EXPLOSION
- FIRE
- INJURY-ILLNESS
- LOSS OF HABITABLE ENVIRONMENT (e.g. from pollution, toxic release, Temperatures...)
- DEPRESSURIZATION (for manned modules)
- ENTRAPMENT

A useful suggestion can be to identify also the undesirable effects that could derive from energy sources that could be present in the system.

As an example, the following slides provide a list (taken from the ECSS-Q-ST-40-02C – Annex A) of generic hazards that could be used as starting point for the identification of the hazards present in the system that will generate the hazard manifestations.

They are organized in groups to facilitate the identification approach and additional hazards can be added in the relevant group.

It is worth to highlight that additional groups can be necessary and is a responsibility of the safety engineer to develop the hazard list for the project (complete and exhaustive).

## **Thermodynamic and fluidic**

- Pressure (difference, high, low, vacuum)
- Temperature (difference, high, low)
- Heat transfer
- Fluid jet
- Thermal properties of materials

## **Electrical and electromagnetic**

- Voltage (high, medium, low)
- Static electricity
- Electric current (high, medium, low)
- Magnetic field (induced, external)
- Ionization
- Spark

## **Radiation**

- Light (infrared, visible, ultraviolet, laser)
- Radioactivity (alpha, beta, gamma rays)
- Open fire

## Chemical

- Toxicity
- Corrosiveness
- Flammability
- Explosiveness
- Asphyxiant
- Irritant

## Mechanical

- Physical impact or mechanical energy
- Mechanical properties of materials (e.g. sharp, rough, slippery)
- Vibration

## Noise

- Frequency and intensity

## Biological

- Human waste
- Microorganism
- Carcinogenic

## Psychological

## Physical

- Confined space

## Environment - Space

- Zero gravity
- Vacuum
- Atmospheric composition
- Contaminants, pollutants
- Meteorite and space debris
- Temperature (difference, low, high)
- Radiation
- South Atlantic anomaly

## Environment - Earth

- Environmental extremes
- Natural disasters
- Lightning

Once the hazard manifestations have been identified, the system design is analysed in term of its functionalities to identify those characteristics that could lead their occurrence, for example:

Fluid Systems requiring thermal control.

Electric systems

Materials

Pressurized Systems

Structures

Mechanisms

Radiation emitters

Propulsion systems

Glasses and shatterable items

Cryogenics

...

Once the system design characteristics/functionalities have been identified the step forward is to identify the System Items that are related to them:

Electric Batteries

Condensers

Pressure Vessels

Electric power sources

Antennas

Mechanisms

Primary, secondary structures

Propulsion systems and devices

Accumulators

Thermal control subsystems (and relevant devices)

Environmental control subsystems (and relevant devices)

Lamps, windows and glasses

...

- Once the System has been identified and “exploded” in its main safety constituents, the causes that could trigger the chain of events that will lead to the Hazardous Events have to be identified.
  
- This exercise is one of the key points in the development of the hazard analysis and particular attention needs to be dedicated to all the engineering aspects of the design, (HW failures, SW errors, Human errors but also materials compatibility, environmental factors, control systems, inhibits...)
  
- All the system, its functions and its devices have to be analysed in term of :
  - “Loss of functionality”
  - “Unwanted functionalities”
  - “Degraded functionality”
  - “Possibility to perform different than expected”
  - “Possibility to interfere with other functions or other functionalities”
  - “Possible common cause or common modes affecting main and redundant item”
  - “Capability to sustain all the environmental factors during the different mission phases”



For each identified **cause** one or more **controls** have to be identified, in line with the:

- The fault tolerance requirements,
- The design for minimum risk requirements,
- The SW criticality levels,
- The operational procedures,
- The inhibit requirements,
- The Caution and warning design requirements and procedures.

They will be implemented according to the required effectiveness with the aim to guarantee the safety of the personnel and of the public and the safety of the system.

For each **control** identified, one or more **verification** methods have to be identified and addressed.

The main categories for the verifications are:

- **Verification by review of design and by analysis**

This group comprises the design reports, the analyses (e.g FMEA, Technical Notes, derating analysis...) in general all those analyses that allow to verify that the “as-designed” is compliant to the requirements.

- **Verification by test**

This group comprises all the tests, the tests reports, the tests results that allow to verify that the “as-built” is compliant to the requirements and performs as expected.

- **Verification by inspection**

This group comprises all the verifications that have to be performed by inspecting the “as-built” to verify that the implementations required by design have been effectively introduced in the HW and the drawings and the manuals are done as required (e.g. sharp edges, labels, connectors, dye penetrants on structures, manuals and procedures).

All the above information has to be collected in the hazard reports.

Each hazard report contain the following data:

- Title;
- Types of hazards and description of their manifestation in the system design and operational configuration and environment;
- Identified hazard scenario with description of causes (associated with the hazard manifestation), hazardous events (physical and functional propagation) and consequences;
- Consequence severity category;
- Propagation time from cause to consequence;
- Applicable safety requirements;
- Hazard reduction measures (implementation of safety requirements, hazard elimination or minimization and control);
- Verification measures;
- Status (safety verification actions open or closed, non-conformances and waivers);
- Approval;

# Hazard Report Exemple



## SPACE STATION HAZARD REPORT

**1. Hazard Number:** Manned Module-000X-01

**2. Hazard Scenario Description:**

Contamination in the NSTS/ISS external environment due to outgassing from materials

**3. Status:** CLOSED

**4. Severity:** Critical      **Likelihood:** Remote

**5. Mission Phases:**

- O Launch
- X Rendezvous
- X Deployment
- X On-Orbit Operation
- X Return

**Mission Type**

- X Passive
- X Active

**5. Detection and Warning Method(s):** N/A

**6. Safety Requirements:** SSP 41164 para 3.3.1.1.3 Materials and Processes

**7 Hazard Cause:** (1) Improper material selection/use

**8. Hazard Controls:** (c.1a). Polymeric materials which are exposed nominally to space vacuum are selected to meet the requirements of JSC-SP-R-0022 or ESA-PSS-01-702, to define low outgassing characteristics (TML <= 1.0 percent and CVCM <= 0.1 percent).

**9. Safety Verification Methods:** (v.1a) Review of Material Identification Usage List (MIUL)

**10. Status of Open Work:** (v.1a) CLOSED.

All data relevant to Manned Module materials properties are contained in the Manned Module MIUL (Material Identification Usage List), doc. Manned Module-LI-XXX-001X. The MIUL has been reviewed to verify that materials nominally exposed to space vacuum do not generate TML and CVCM rates higher than those specified. Where requirement cannot be satisfied, MUA has been issued for NASA approval. Summary of the Manned Module submitted MUA's is contained in doc. Manned Module-LI-XXX-0101 "Manned Module MUA Summary List".

European Space Agency

As part of the Safety Data Package (SDP), a SVTL log collects all the still open safety verification items from the different safety analysis/hazard reports of the SDP at the end of the production and qualification phase of the project.

It provides information of the verification effort and gives reference to the close out documents (e.g. test reports, analyses, and procedures).

Depending on the number and severity of the open verification items it can be the basis for the decision to put the next processing steps (like acceptance or integration into the next higher level) into hold.

The SVTL is part of the SDP at the end of the qualification phase.

The SVTL is based on:

Inputs from the different safety verification tasks:

- hardware and software changes,
- tests,
- review of design activities,
- analyses,
- inspections and development of procedures which are performed as agreed per “hazard reports” of the Flight-SDP (FSDP) and the Ground-SDP (GSDP) - or a combination thereof.
- Other information like constraints and schedule.

SVTL is composed with the following parts:

### **General information:**

- Name of the project for which it has been established.
- Project documentation identification number.
- Applicability for flight or ground safety verifications.
- Indication of the specific page number followed by the total number of pages.
- Name of the equipment, payload or experiment for which the SVTL has been established.
- Mission or flight to which the equipment, payload or experiment has been manifested.
- Dates of issue and update.

### **Log Number:**

- For each verification item to be tracked is used a unique identifier

### **Hazard Report number:**

- The identification number of the hazard report containing the verification item is always indicated

### **Safety Verification number:**

- The verification method or the verification means is transferred from the hazard report to the SVTL including the procedures by number and title.

# Safety Verification Tracking Log

## Annex C #4



### **Ground Operations constrained:**

- The input of "yes" or "no" has to indicate whether this safety verification constrains any ground operations.
- If "yes" for flight tracking log: an attachment has to be provided that identifies which ground operation is constrained.
- If "yes" for ground tracking log: the ground operation constrained by this verification has to be indicated specifically in the user manual and included as a step in a procedure.

### **Independent verification required, "yes" or "no":**

- The input of "yes" or "no" has to indicate whether the verification has to be performed independently.

### **Scheduled Completion date:**

- The planned date for the completion of the verification has to be indicated.

### **Method of closure/comments:**

- The SVTL log has to indicate the title and serial number of the tests, review of designs, inspections and analyses by which this verification is formally closed.
- Any appropriate information or remarks may be added.



# Safety Verification Tracking Log

## Annex C #5



Safety Verification Tracking Log form (as per annex C of ECSS-Q-ST-40)

<b>Safety verification tracking log</b>				Flight <input type="checkbox"/>	Ground <input type="checkbox"/>	page ___ of ___		
Project ID:								
Equipment, payload, mission							Issue date	updated
Log no.	Hazard report number	Safety verification number	Safety verification method (Identify procedures by number and title)	Ground operations constrained	Independent verification required	Scheduled completion date	Completion date	Method of closure/comments (Provide reference ID)

'CE' Marking is a requirement that is applicable to virtually all products which are designed and intended for use on the Ground. This includes all Ground products and Ground Support Equipment (GSE) and in particular all EGSE and most MGSE.

The **'CE' is a mark** by the producer/supplier to show he has satisfied all applicable Directives for the safety of his product and is intended to allow the 'Free movement of Goods' within the European Community. This requires compliance with European directives - generally through assessments to EN standards.

It is an offence to:

- Put a 'CE' mark on a product, without the supporting 'Technical File';
- Not to CE mark a product, if there is an applicable directive(s);
- Take a non-compliant product 'into service' anywhere within the European Community.
- CE Marking is applicable to all Ground products including GSE regardless of whether it is being passed to a third party, a customer or designed and built for internal Company use.

## Responsibility of the design authority

It is the responsibility of the 'Design Authority' to identify all directives which apply to the product design and to ensure assessment and compliance of the product(s) to the most recent edition of all applicable directives, legislation and relevant EN standards.

The 'Design Authority' is required to:

- Identify all applicable directives;
- Demonstrate technical compliance;
- Hold a 'Technical File' for 10 years;
- Issue a 'Declaration of Conformity', a User Manual with safety warnings and put the 'CE' mark on the product.

All published EU legislation and directives should be evaluated and applied if applicable to the product.

Term	Meaning
Accident	undesired event arising from operation of any project-specific item that results in: <ul style="list-style-type: none"> <li>• human death or injury,</li> <li>• loss of, or damage to, project hardware, software or facilities that can then affect the accomplishment of the mission,</li> <li>• loss of, or damage to, public or private property, detrimental effects on the environment</li> </ul>
Anomaly	any deviation from the expected situation
Caution condition	condition which has the potential to degrade into a warning condition, and which can call for specific action, including the implementation of special procedures or restrictions on the operation of the system
Common cause failure	failure of multiple items occurring from a single cause that is common to all of them
Common mode failure	failure of multiple identical items that fail in the same mode
Contingency procedure	pre-planned procedure to be executed in response to a departure from specified behavior
Derating	process of designing a product such that its components operate at a significantly reduced level of stress to increase reliability
Design to minimum risk	design of a product to an acceptable residual risk by conformance to specific requirements for safety, other than failure tolerance.

# Most commonly used terms



Term	Meaning
Emergency	condition when potentially catastrophic or critical hazardous events have occurred, and immediate and preplanned safing action is possible and is mandatory in order to protect personnel
Fail-safe	design property of an item which prevents its failures from resulting in critical faults
Failure	termination of the ability of an item to perform a required function
Failure mode	observable effect of the mechanism through which the failure occurs
Failure tolerance	the attribute of an item that makes it able to perform a required function in the presence of certain given sub-item failures
Fault (1)	state of an item characterized by inability to perform as required
Fault (2)	unplanned occurrence or defect in an item which can result in one or more failures of the item itself or of other associated equipment
Fault tolerance	the attribute of an item that makes it able to perform a required function in the presence of certain given sub-item faults
Flammability	measure of the ease with which a material is set on fire
Flight operations	all activities related to the planning, execution and evaluation of the control of the space segment (or subsets thereof) when in orbit

# Most commonly used terms



Term	Meaning
Hazard	existing or potential condition of an item that can result in an accident
Hazardous event	occurrence leading to undesired consequences and arising from the triggering by one (or more) initiator events of one (or more) hazards
Human error	inappropriate or undesirable human decision or behavior that reduces, or has the potential for reducing effectiveness, safety, or system performance
Incident	unplanned event that could have been an accident but was not
Inhibit	design feature that provides a physical interruption between an energy source and a function actuator
Mission	specific task, duty or function defined to be accomplished by a system
Outage	state of an item of being unable to perform its required function
Performance	aspects of an item observed or measured from its operation or function
Preventive action	action to eliminate the cause of a potential nonconformity, or other undesirable potential situation
Procedure	specified way to carry out an activity or process
Process	set of interrelated or interacting activities which transform inputs into outputs
Redundancy	existence of more than one means for performing a given function

# Most commonly used terms



Term	Meaning
Reliability	ability of an item to perform a required function under given conditions for a given time interval
Required function	function or a combination of functions of an item which is considered necessary to provide a given service
Residual risk	risk remaining after implementation of risk reduction measures
Risk	undesirable situation or circumstance that has both a likelihood of occurring and a potential negative consequence on a project
Safety critical function	function that, if lost or degraded, or as a result of incorrect or inadvertent operation, can result in catastrophic or critical consequences
Safing	action of containment or control of emergency and warning situations, or placing a system (or part thereof), in a predetermined safe condition
Severity	classification of a failure or undesired event according to the magnitude of its possible consequences
Single point failure	failure of an item which results in the unrecoverable failure of the product
Stress-corrosion	combined action of sustained tensile stress and corrosion that can lead to premature failure of materials
Undesirable event	those events whose occurrence can jeopardize, compromise, or degrade the mission success or the safety objectives