ESA ESRIN
Largo Galileo Galilei 1
00044 Frascati
Italy

SPACE RIDER SYSTEM - PAYLOAD SAFETY ANALYSIS TEMPLATE

Prepared by	ESA STS-PF
Document Type	TN - Technical Note
Reference	ESA-STS-SR-TN-2022-0004
Issue/Revision	1 . 0
Date of Issue	21/04/2022
Status	Draft

APPROVAL

Title	Space Rider System - Payload Safety Analysis Template		
Issue Number	1	Revision Number	0
Author	**ESA STS-PF**	Date	21/04/2022
Verified by	**Esther Gaillot** STS-PF Safety Engineer	Date	
Approved By	**D. Le Falc'her** Head of STS-PF Safety Office	Date	

CHANGE LOG

Reason for change	Issue Nr	Revision Number	Date
First issue	1	0	21/04/2022

CHANGE RECORD

Issue Number 1		Revision Number 0	
Reason for change	Date	Pages	Paragraph(s)
First issue	-	-	-

DISTRIBUTION

Name/Organisational Unit
ESA Unclassified – ESA Official Use Only STS-PS STS-PF

Table of Contents

1. INTRODUCTION

This document is a guideline for the PL Sub-Aggregator to perform the safety analysis of the PL, specific GSE (if existing) and ground operations. This safety analysis shall cover safety aspects during the following phases (chronological order):

- Ground phase: Launch preparation campaign.
- Flight phase: Launch vehicle flight.
- Flight phase: SRS mission flight.
- Ground phase: SRS mission post-flight operations at landing site.

ESA PL Safety requirements are reported in [AD1].

The customer shall replace the text in grey with its own assessment.

Indicate the submission phase for which this template is written (definition in [AD2]).

2. APPLICABLE DOCUMENTS

Item	Reference	Title
AD1.	ESA-STS-SR-ST-2022-0001	SRS - payload safety, space debris and collision avoidance requirements
AD2.	ESA-STS-SR-PL-2022-0001	Safety process for space rider re-entry module payloads

3. REFERENCE DOCUMENTS

Please insert in this list the documents used to support the Safety Analysis.

Item	Reference	Title
RD1		
RD2		
RD3		

4. ACRONYM LIST

ACS	Attitude Control System
AOCS	Attitude Orbit Control System
AOM	Avum Orbital Module
AZ	Approach Zone
CAM	Collision Avoidance Manoeuvre
ExO	Experiment Owner
GSE	Ground Support Equipment
KOZ	Keep Out Zone
LSSA	Landing Site Safety Authority
MEOP	Maximum Expected Operating Pressure
MPCB	Multi-Purpose Cargo Bay
P/L	Payload
PLA	PayLoad sub-Aggregator
PLCC	Payload Control Center
SRS	Space Rider System

VCC-OC	Vehicle Control Center – Orbital Control
VCC-LC	In-Orbit Control Center– Landing Control
VTL	Verification Tracking Log

To be completed by Customer

5. DEFINITIONS

Payload mission:

The Payload mission is assumed to start from its unpackage in the launch facilities until its retrieval after landing.

MPCB Operator:

The MPCB Operator is in charge of the definition, development and management of the MPCB PL Aggregate, throughout the overall payload lifecycle, mission preparation, in-orbit follow-up and retrieval, in particular according to the acceptance process described in [AD2].

NOTE: For the SRS Maiden Flight preparation, this role will be covered by ESA IPT.

Payloads sub-aggregator (PLA):

The Payloads sub-aggregator is in charge of the payload acceptance process. The PLA can be responsible of one or more payload (that can be located in different VLs).

Experiment Owner (ExO):

The Experiment Owner is the design authority of the Experiment to be embarked on the Space Rider System.

Multi-Purpose Cargo Bay (MPCB):

For the multiple payload configuration, the SR MPCB may offer different compartments as well as different payload sizes (i.e. small, micro and nano).

MPCB is divided in different virtual lockers whose destination is a function of the experiment to be performed (see following definition).

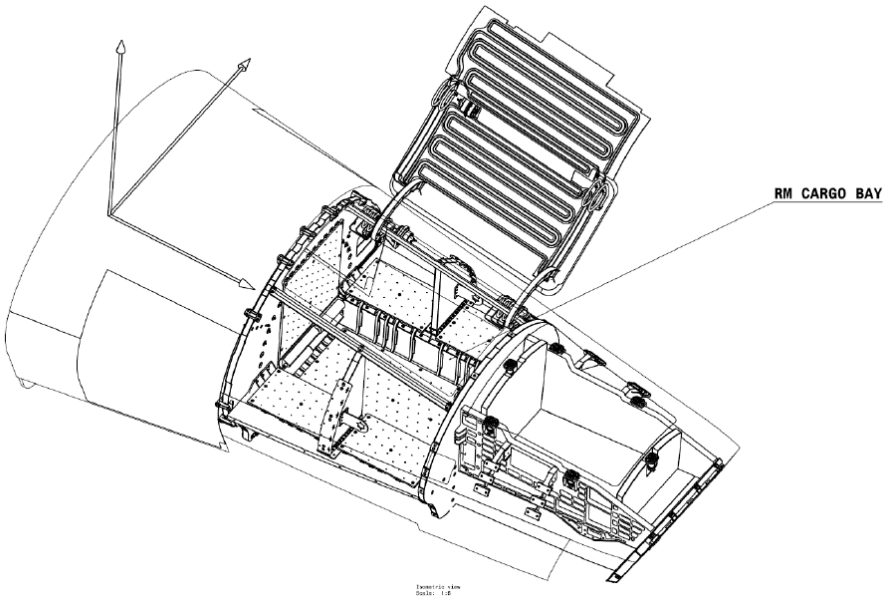

Figure 1 – SR MPCB central door

Virtual Lockers:

A virtual locker is a technical specification of the allocation of services, interfaces and budgets in the MPCB and toward a sub-aggregator.

In the MPCB 8 Virtual Lockers are identified, each of which has specific interfaces and characteristics:

- 2 aft lateral VLs to provide late access before launch/ early access after landing;
- 2 forward lateral + 2 bottom VLs for microgravity payloads
- 2 top VLs for larger payloads or payloads that require direct exposure to the space environment or field of view.

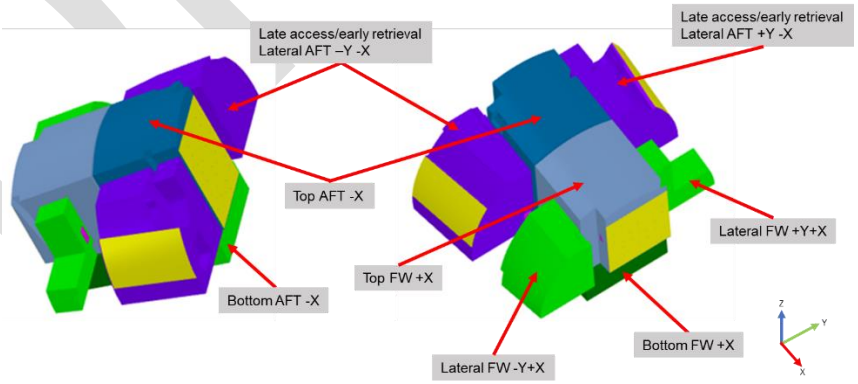

Figure 2 – Virtual lockers 3D model

Payload categories:

For the definition of the flight-only safety requirements it is necessary to define three classes of PL embarked on Space Rider:

- Fixed Payload: any Payload which does not separate from Space Rider MPCB and remain fixed in the virtual locker.
- Deployable Payload (D-PL): any Payload, which can separate from Space Rider MPCB into its own free-flying mission, divided in three sub-classes:
  - Payload deployable with no manoeuvre capability (**D-PL (NM)**)
  - Payload deployable with manoeuvre capability (**D-PL (M)**)
  - Payload deployable with operations within the Space Rider Keep Out Zone (retrieval/re-visitation) (**D-PL (KZ))**
- Movable Payload: any Payload which does not separate from Space Rider MPCB but perform movement inside it (i.e. robotic arm)

P/L Keep Out Zone (KOZ):

Zone inside which the Deployable Payload operations are considered dangerous for Space Rider. The Space Rider KOZ is 200 m (TBC) radius sphere centered at the Space Rider vehicle center of mass.

P/L Approach Zone (AZ):

The Space Rider Approach Zone (AZ) is the zone around Spacer Rider in which it is necessary to measure the relative position between the Payload and Space Rider to avoid collision.

The Space Rider AZ is a 1 km (TBC) radius sphere centered at the Space Rider center of mass.

P/L Approach Corridor:

The Approach Corridor is the spatial envelope to be followed by the Payload in the Keep Out Zone (KOZ). The notion of corridor, generally understood as a cone originating from the target in which the Payload makes its approach, is extended to address at least:

- Relative trajectory including margin (the relative trajectory might not be a linear translation)
- Range-rate profile (profile of the relative rate versus the relative distance)
- Relative attitude (angles and rates) profile

The qualitative parameters (e.g. reference frame) and quantitative parameters are mission specific.

The Space Rider Approach Corridor is a 10˚ (TBC) cone centered to the docking port axis (Space Rider MPCB) within the KOZ.

P/L Abort Corridor

The Abort Corridor is the spatial envelope, which if exceeded, in case of Payload GNC loss, creates hazardous collision between the Payload and Space Rider. The Abort Corridor, it addresses at least:

- Relative trajectory
- Range-rate profile
- Relative attitude (angles and rates) profile

The qualitative and quantitative parameters are mission specific. The Abort Corridor typically is larger/around the Approach Corridor although some parameters might be different (e.g. a too small relative range rate might not be part of the Abort Corridor whereas it might part of the Approach Corridor).
Violating the Abort Corridor results in an Abort.

To be completed by Customer

7. GENERAL DESCRIPTION

7.1. Mission

Identification of the P/L category.

Mission description.

7.2. PL Description

7.2.1. Characteristics

General characteristics, mass, dimension, one image of the Payload and description of each Experiment included (if applicable).

Late access/early retrieval need.

7.2.2. PL s/s

List of Payload subsystems with a short description (batteries, heaters, tank, payload, etc…). List of fluidic components, identification of their characteristics, hazard levels and quantities, management during mission.

7.3. GSE description

Description of the specific GSE equipment to be used during LV campaign or post-landing activities (GSE provided by launch and SR services not to be included).

7.4. Interfaces

7.4.1. Interfaces with LV

No direct I/F with LV.

Status of PL during LV flight.

7.4.2. Interfaces with Ground equipment

Description of the specific I/F on ground at Launching and Landing Site (if any) and any failure propagation protection. {I/F provided through RM not to be included}.

7.4.3. Interfaces with RM

Description of the I/F with the RM and any failure propagation protection.

Different Status of the PL during its life, starting from integration in RM.

7.4.4. Interfaces with Ground Segment

Description of the interaction with the PLCC during orbital phase.

7.5. Qualification Plan

Description of the qualification plan.

8. SAFETY ANALYSIS

8.1. Hazard classification

(Suggested classification)

Scale	Impact	Definition
G0A	Safety Catastrophic	• Immediate or delayed loss of human life • Permanent disability • Irreversible damage to public health
G0B	Safety Serious	• Serious injury not causing loss of life or permanent invalidity • Reversible threat to public health • Significant property damage: total or partial destruction of public or private property-total or partial destruction of a launch operations facility in CSG • Significant damage to the environment
G1A	Dependability Catastrophic	• Failure propagation (to the MPCB PL or SRS vehicle)
G1B	Dependability Serious	• Loss of PL
G2	Dependability Major	• Major mission degradation
G3	Minor or Negligible	• Minor mission degradation or • any other effect

8.2. Hazardous subsystems

The following table define the risk-related subsystem. (To fill with N/A or YES or TBC)

Potential hazardous sub-system	Applicability to the PL	Foreseen Compliance	Verified Compliance
Propulsion, AOCS, ACS systems			
+ Command and control circuits			
+ Propulsion system GSE, Operations			
Electrical systems, batteries, Heaters			
+ Umbilical Electrical interfaces			
+ Electrical system GSE and ground operations			
Non-ionizing RF systems, Optical system Laser systems, other RF sources			
+ RF-system ground operations			
Pressurized systems with fluids and gas other than propellants, including biological materials			
+ Pressurized systems Command and control circuits			
+ Pressurized systems GSE and ground Operations			

Mechanical / Electro-Mechanical systems, Transport / Handling			
+ Other systems and equipment			
+ Linked GSE, ground operations			
Hazardous material not previously covered			
Ionizing systems			
Electro-Explosive Devices, Solid Rocket Motor or other pyrotechnical devices			

NB: *It is recalled that ionising system and pyrotechnical systems (at the exception of pyro valves or similar pyro-devices) are forbidden by [AD1].*

NB: *please when missing indicate if a dedicated GSE is foreseen for a potential risk-related system (of course not the one provided by the Launch or Landing services).*

Hazardous material, as identified in chapter 8.1.1 of [AD1], shall be accompanied by MSDS.

8.2.1. Propulsion, AOCS, ACS system

Propulsion system, depending on their nature, may depend on chapter 8.1.1, 8.1.2 or 8.1.4 of [AD1].

An analysis example is provided here after for a liquid propulsion system.

8.2.1.1. Liquid Propulsion system

Describe the liquid propulsion system with functional diagrams and schemes showing position in the satellite.

Describe:

- Nature, mass and volumes of the propellants concerned.
- MEOP on GROUND and on FLIGHT, safety factors of the structure, components and tanks
- List of components of the propulsion system showing:
  - type, manufacturer, and inheritance
  - Formal acceptance pressure (proof-test), qualification pressure and corresponding safety factors
- The methods of assembling components and the propulsion system (welding, bolted assembly, etc.)
- Status of the system in the different phases of the satellite (from LV preparation to landing)
- Control and command circuits, both mechanical (valve, regulator, etc…) than electrical.
- I/F with ground system and if specific Fluidic GSE shall be used.
- Design standard

Identify:

- Feared events and degrees of severity (leakage, mechanical fracture, mixing of propellants, etc…), in the different phases.
- Barriers present. If G0A/G0B events are identified, at least 3/2 barriers shall be present.
- Toxic, corrosion, and other risks.

Analyse:

- Failure modes with associated feared event, detection, and reliability in the four different phases of life.

It is important to note:

- Effort shall be made to avoid failure propagation, outside the PL or MPCB.
- Mixing of propellants shall be avoided.
- Compatibility with the material used.

- Rate of propellant loading/downloading shall not create any hazard.
- Safety factors shall be clearly identified and respected.

8.2.2. Electrical systems

Diagram of the PL's electrical architecture:

Schematic of the electrical connection(s) between, and the operational logic of, the following elements:

1) Kill switches;
2) Remove before flight elements and/or apply before flight elements;
3) The battery & power system and the satellites electrical systems;

Identification of risk related items:

Electrical system may be categorised as risk related if:

- the electrical system activates systems or components containing one or more hazardous products,
- the electrical system may, in case of failure(s), emanate energy (electrical, thermal, etc.) or effluents that may cause direct harm (effect of electrical origin) or indirect harm (effect on a risk-related system connected to the electrical system).
- if it can deliver a current on contact that can cause an electrical shock and burns, with a current greater than or equal to:
    - 3.5 mA for direct and alternating currents up to a frequency of 10 kHz,
    - 350 * F mA (f being the frequency expressed in MHz) for alternating currents of a frequency ranging from 10 kHz to 100 kHz.
    - 35 mA for alternating currents up to a frequency of 100 kHz,

Conformity of the connectors, cables and distribution (strong and weak currents, grounding):

AWG cable, power connector, single point grounding scheme, no sharp edges, etc.

The equipment is designed to ensure that the external metal parts and the shields can be grounded.

Batteries:

Provide a description of the batteries and their characteristics.

- Batteries shall be easy to disconnect.
- If the battery is not connected, the connection terminals shall be protected to prevent any risk of short-circuiting,
- In the event of a short-circuit, splatters of electrolyte shall be confined.

Indicate any Battery over-voltage, under-voltage and over-current protection.

Provide the maximal duration of the battery.

Shall battery be recharged before launch? If not, how much can remain in stowed condition before recharging?

Heaters:

Describe type, number, location, operating temperature, maximum temperature…

Describe functioning.

In case they may over pass the temperature for skin-contact safety threshold (45°C) during ground operations (in particular on landing site) these will be clearly marked with adequate warning labels.

Risk related items analysis.

Arrangements for the protection of risk-related systems against over-current, over-voltage and short circuiting (Current limiter, etc...)

The electrical risk-related systems shall be protected against transient bursts of overcurrent and overvoltage, or at least the feared event shall be contained in the PL case.

Risk-related electrical systems as well as the electrical systems contributing to the security of resources or maintaining resources in secure mode must be designed so that they cannot be affected by an electrostatic discharge. Warning labels will be also attached to parts or units that include high voltage components or electrodes.

Analyse:

- Failure modes with associated feared event, detection, and reliability in the four different phases of life.
- Provide:
  - Protection arrangements
  - Means of control and monitoring
  - Method for emergency cut-off

EMC compatibility:

Electrical system shall be compatible with EMC levels of the different life phases.

Operations

I/F with ground system, accessibility and if specific Electrical GSE shall be used.

Status of the equipment during the different phases of life.

8.2.3. RF Sources

8.2.3.1. Non-Ionizing radiation

Description of antenna, type and position.

RF interface description (transmission/reception frequency).

Provide Transmitter properties, EIRP, characteristics, emission properties.

Safety analysis

Provide safety distance to be held by operators when antenna is operating.

Operation:

Provide a description of transmission system status during the different phases.

EMC compatibility:

Verify compatibility with SRS system.

If antenna is operated on ground, verify compatibility with ground and LV too.

8.2.3.2. Optical systems

Description:

- Location of source.
- Function.
- Type of source.
- Classification (standard TBW).
- Type of radiation

Operation:

Provide a description of Laser system status during the different phases.

Analyse:

Failure modes with associated feared event, detection, and reliability in the four different phases of life.

Payload's optical instruments will prevent harmful light intensities and wavelengths from being viewed by operating personnel. Quartz windows, apertures or beam stops, and enclosures will be used for hazardous wavelengths and intensities. Light intensities and spectral wavelengths at the eyepiece of direct viewing optical systems will be below a specified threshold.

8.2.3.3. Laser

Description:

- Location of source.
- Function.
- Type of source.
- Classification (standard TBW).
- Type of radiation

Operation:

Provide a description of Laser system status during the different phases.

Special precautions shall be taken in case of operations foreseen on ground (i.e. can be used only in dedicated areas, with hazard warning, etc…TBC). If use is foreseen only on flight, ignore this part.

Analyse:

Failure modes with associated feared event, detection, and reliability in the four different phases of life.

If on ground will not be used, provide an assessment of the potential dangers for the SRS vehicle during orbital phase.

8.2.3.4. Other

TBC

8.2.4. Fluid, pressurized system and biological material

8.2.4.1. Pressurized system

Any pressurized system which is not part of the propulsion system is described here (heating pipes, experiments, etc…).

For the particular case of heating pipes, in case they may over pass the temperature for skin-contact safety threshold (45°C) during ground operations (in particular on landing site) these will be clearly marked with adequate warning labels.

Describe:

- Nature, mass and volumes of the fluids concerned.
- MEOP on GROUND and on FLIGHT.
- Status of the system in the different phases of the satellite (from LV preparation to landing)
- Control and command circuits, both mechanical (valve, regulator, etc…) than electrical.
- I/F with ground system and if specific Fluidic GSE shall be used.

Identify if a risk-related item following this rule.

Nature of the fluid	Container (vessel)	Piping
GAS or liquids whose vapour pressure at the maximum acceptable temperature exceeds normal atmospheric pressure by 0.5 bar.	P > 0.5 bar and V > 1 litre and PxV > 50 bar x 1 or P > 1000 bar	P > 0.5 bar and DN > 32 and PxDN > 1000 bar
LIQUIDS whose vapour pressure at the maximum acceptable temperature is less than or equal to 0.5 bar above normal atmospheric pressure.	P > 10 bar and PxV > 10000 bar x 1 or P > 1000 bar	P > 10 bar and DN > 200 and PxDN > 5000 bar

V : internal volume of the vessel in litres

P : gauge pressure in bars

DN : nominal bore in mm. - Numerical designation of the nominal bore size common to all components of a piping system, other than elements designated by their outer diameter or thread size. The DN value is rounded for reference purposes and has no strict relationship with manufacturing dimensions. "DN" followed by a number indicates nominal bore size.

In a case of a risk-related system safety factors shall be used (generally SF>2, meaning that burst pressure shall be higher 2 times the MEOP)

Safety Analyse:

- Failure modes with associated feared event, detection, and reliability in the four different phases of life.
- Guarantee that in case of leak or other failure mode, the feared event is contained in the PL or at least in the MPCB.

8.2.4.2. Hazardous fluids and biological material

Identify the presence of any fluid with potential human hazard, providing the technical specifications and material data.

Identify the presence of any fluid not compatible with the MPCB environment.

Identify the presence of Micro-organic materials, microbes, living cells, bacteria, samples of human, animal, or vegetal origins, organic fixatives, and similar biology specimens. Those will have to be declared along with their classification in terms of hazard and toxicity level.

All products belonging to this class will be accompanied by a specific MSDS (Material Safety Data Sheet) and by adequate safety instruction.

Those fluids shall be retained by the fluid system and will be subject to extensive leak verifications by testing in the worst operational conditions.

Analyse:

- Failure modes with associated feared event, detection, and reliability in the four different phases of life.
- Guarantee that in case of leak or other failure mode, the feared event is contained in the PL.

8.3. Hazardous Materials

Identify any material which is not part of the previous section that may provoke a hazard to personnel, structure or vehicle (i.e. material with toxic or corrosive off-gassing).

The minimum use of flammable materials will be the preferred means of hazard reduction. A flammability assessment will be documented, according to standard ECSS-Q-ST-70.

Hazardous materials shall not be released inside the Space Riders MPCB and MSDS will be provided.

Payload organizations will submit material data for toxicological assessments, according to the applicable standards.

8.3.1. Genetically Modified Organisms (GMOs)

Describe if GMO will be used in the experimentation.

Use of GMOs for specific experiments will be accompanied by approval of the competent authorities, clearly stating compliance to human safety regulations and ethical standards.

8.4. Mechanical, transportation and other

Demonstration of mechanical sizing of the payload and corresponding hoisting points (burst safety factor > 2).

Clarify transportation and handling to CSG teams, in particular for hazardous products.

Dedicated mechanical GSE is not expected. If not, this section will be completed.

8.5. Flight-Only safety analysis

8.5.1. Failure propagation Avoidance

As a general approach it shall be avoided any failure propagation from PL to other PL or SRS system. This is declined in the previous sub/system chapter, but if any failure mode exists at PL system level, not previously mentioned, please complete here the analysis.

For example:

- Payload sealed compartments will be designed to withstand the maximum pressure differential created by the Space Rider de-pressurization or re-pressurization activities.
- Vented compartments will size vent flow areas such that structural integrity is maintained at the maximum rate of change of pressure.

What concerns deployed P/L and movable P/L to be treated a part.

8.5.2. All P/L category requirements

Report compliance to the requirements applicable to all P/L categories.

Description of the methodology, tools, standard may be useful to support the requirement verification.

Presentation of the results, with possible evidence, is required.

8.5.3. Deployed P/L category requirements

Report compliance to the requirements applicable only to Deployed P/L categories.

8.5.4. Movable P/L category requirements

Report compliance to the requirements applicable only to Movable P/L categories.