Alma Mater Studiorum – Università di Bologna

DOTTORATO DI RICERCA IN

Meccanica e Scienze Avanzate dell'Ingegneria

Ciclo XXVIII

Settore Concorsuale di afferenza: 09-A1

Settore Scientifico disciplinare: ING-IND 03

ESEO SPACECRAFT:

FMEA (FAILURE MODE AND EFFECTS ANALYSIS) AND FDIR (FAULT DETECTION ISOLATION AND RECOVERY)

Presentata da:

MATTEO ALBERTO FERRONI

Coordinatore Dottorato

Prof. Ing. VINCENZO PARENTI CASTELLI

Relatore

Prof. Ing. FABRIZIO GIULIETTI

Correlatori

Ing. NICOLA MELEGA

Ing. ALESSANDRO AVANZI

ANNO 2016

Table of contents

1 Introduction 6

2 ESEO (European Students Earth Orbiter) 9

2.1. Mission description 9

2.1.1. Objectives 9

2.1.2. Requirements 11

2.2. Space segment 12

2.2.1. Spacecraft modes 13

2.2.2. Architecture 21

2.2.3. Subsystems 23

2.2.4. Hardware 28

2.2.5. Software 31

2.2.6. F.M.E.A. (Failure Mode and Effects Analysis) 32

3 Test campaign 44

3.1 Power and electrical interfaces test 44

3.2 Temperature test 47

3.3 Radiations test 47

3.3.1 Total Ionizing Dose: T.I.D. 48

3.3.2 Single Events Effects: S.E.E. 50

3.4 Vibration test 53

3.5 Thermo-vacuum test 56

3.6 E.M.C. test 58

4 F.D.I.R. (Fault Detection Isolation and Recovery) 61

4.1. Level 0: Built-in 66

4.2. Level 1: Hardware 67

4.3. Level 2: Software 71

4.3.1. Platform FDIR 71

4.3.2. ACS/OBDH FDIR 81

4.3.3. Unit FDIR 89

4.4 Failure scenario 99

5 Conclusions 105

6 Bibliography 109

Table of figures

Figure 1.1 ESEO Spacecraft 7
Figure 2.1 ESEO space segment 12
Figure 2.2 Flow diagram of the ESEO mission 14
Figure 2.3 AOCS initialization 16
Figure 2.4 AOCS Damping 17
Figure 2.5 AOCS Nominal 18
Figure 2.6 Re-entry mode 18
Figure 2.7 General mission timeline 20
Figure 2.8 ESEO block diagram 21
Figure 2.9 TMTC set-up 23
Figure 2.10 Architecture of PS 27
Figure 2.11 FMEA Worksheet 32
Figure 3.1 Test set-up 44
Figure 3.2 Climatic chamber 47
Figure 3.3 STM32F407 decapsulated 48
Figure 3.4: ENEA Calliope ^{60}CO source 49
Figure 3.5: EUT inside the irradiation chamber 49
Figure 3.6: STM32F407 Timer 3 50
Figure 3.7 LNS Superconducting Cyclotron 52
Figure 3.8 Electro-Dynamic Shaker 53
Figure 3.9 Low frequency longitudinal vibration environment spectra 54
Figure 3.10 High frequency random environment spectra 55
Figure 3.11: High Level sine results – Z axis MPS Tank 55
Figure 3.12: Random vibration results – Z axis MPS Tank 56
Figure 3.13 Pressure variation limit 57
Figure 3.14 ALTA Thermo-Vacuum Chamber 57
Figure 3.15 ESEO bus, EMC test 60
Figure 3.16 ESEO bus integrated 60
Figure 4.1 Failure detection hierarchy 62
Figure 4.2 EDAC mechanism 66
Figure 4.3 Generic CRC Byte generation 67
Figure 4.4 OBDH OVP/OCP reset 69
Figure 4.5 TMTC OVP/OCP reset 69
Figure 4.6 ACK requests and switch to redundant, for OBDH and PS 72
Figure 4.7 TMTC main FDIR operations diagram, phase M0 73
Figure 4.8 TMTC main FDIR operations diagram, 73
Figure 4.9 TMTC main operations, phase M2-1 74
Figure 4.10 TMTC main FDIR operations, phase M2-2 75
Figure 4.11 TMTC main FDIR operations, safe mode S3 76
Figure 4.12 TMTC main operations, safe mode S4 78
Figure 4.13 TMTC redundant FDIR operations diagram 79
Figure 4.14 TMTC: OBDH reprogramming sequence 81
Figure 4.15 Error flags 83
Figure 4.16 ACS FDIR-1 84

Figure 4.17 ACS FDIR-2 85
Figure 4.18 MM Check 86
Figure 4.19 OBDH FDIR 88
Figure 4.20 PMU FDIR 89
Figure 4.21 CAN Bus failure detection 91
Figure 4.22 Unit FDIR 93
Figure 4.23 Comparison between fault control variable in the HIL simulations (red curves) and numerical simulations (blue curves) in two different configurations 98
Figure 4.24 General Payload FDIR approach 99
Figure 5.1 Render of the ESEO satellite 108

1 INTRODUCTION

The exponential growth in the scale of integration of electronic devices has allowed in the past thirty years to develop increasingly high performance, compact and low cost satellites capable of exploit a different number of experiments and mission scenarios, especially in Low Earth Orbits. In parallel, the development process of the electronic components in the last two decades has undergone an additional boost thanks to the progress in terms of manufacturing like the level of integration of the microprocessor units, VLSI.

Having a look at different markets like industrial, automotive or military, nowadays it is possible to find a series of different ICs particularly suitable to be successfully used onboard a spacecraft: microcontrollers.

The large amount of inputs/outputs, functions and interfaces embedded in this kind of devices perfectly fit the role of main processing unit, thanks also to the performances reached in terms of computing power, the reduced costs and the very low power consumption.

Unfortunately, these devices are typically not designed taking into account all the constraints imposed by the space environment (vacuum, extreme temperatures, tolerances to radiation, etc.) and thus it is usually very difficult to determine their reliability figures when working "outside" the design requirements.

The present doctoral thesis, which takes places in the context of the ESEO (European Students Earth Orbiter) mission, is then focused on design specific methodologies to overcome the limitations mentioned above regarding the reliability of electronic systems and their fault tolerance especially when used in harsh environments. All the subsystems developed for the ESEO microsatellite in fact, share the same design philosophy and are based upon COTS (Components Off The Shell) electronic components, military or industrial grade ones, ensuring considerable savings in terms of costs with minimal impact on the final performance of the system.

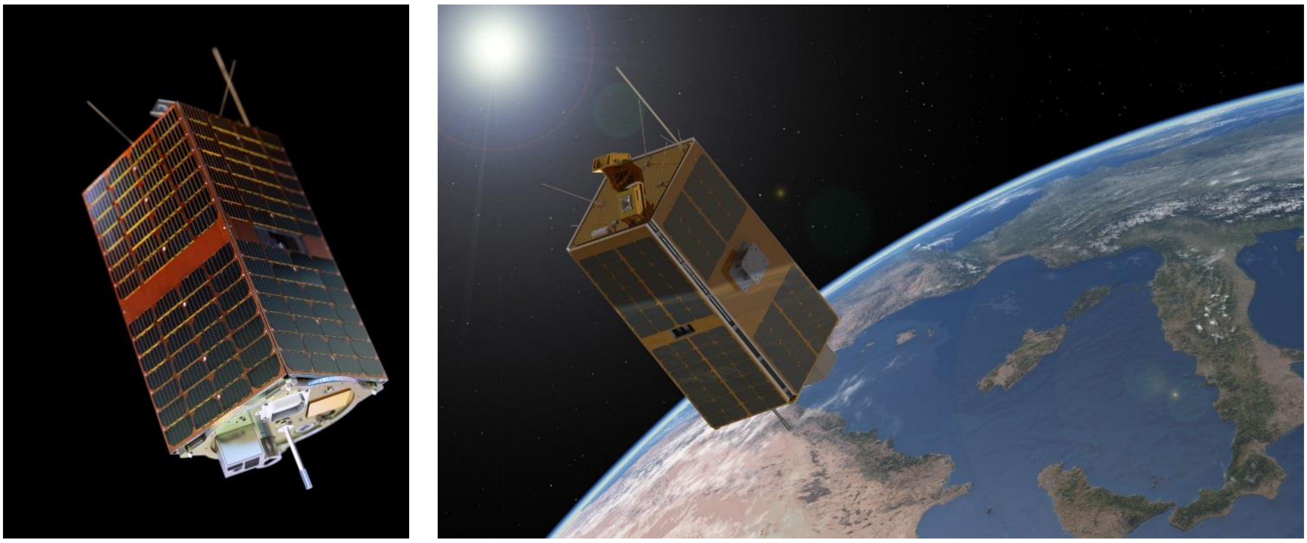


Figure 1.1 ESEO Spacecraft

The ESEO project introduces a step in the progress of the spacecraft concept thanks to the implementation of an uncommon fully mirrored architecture. The system developed around an ARM based microcontroller and a redounded CAN bus communication link, allows a whole set of experiments and payloads carried on board. The FDIR strategy is an essential part for the harmonization of the whole system but, even in a well-defined and structured field as the space one, there are no specific references or standardization like the ECSS, exception made for the industrial consolidated products. Due to its strong correlation with the system specific architecture FDIR strategies are full-custom and the decisions made are based on test carried out, technological consideration (COTS parts) and analyses performed, like FMEA, during the phases that lead to the Assembly, Integration and Validation process. The objective is to enforce the probabilities of the mission success, securing the platform configuration, autonomously or from ground, in case of failure.

The overall FDIR Strategy is an innovative contribution in the sense that aims to cover one of the possible ways, not regulated by standards or procedures, to solve the reliability problem of the platform ensuring reduced mission costs; the goal is a fraction if compared to the conventional space missions. The costs evaluation is affected from parameters such as: human resources, development time, technologies and techniques implemented / produced and also transportation and launch, as well as the following costs to operate the spacecraft and the ground stations, three for the ESEO mission[1]. Acting on the right calibration of HW, SW and Controls and also proportionally to the level of automation introduced on board, it is then possible to reduce the cost of the ground segment.

[1] ESEO Ground Stations, located in: Forlì, Main Station (Developed by the University of Bologna); Monaco, S-Band Station; Vigo, Back-up Station.

2 ESEO (European Students Earth Orbiter)

2.1 Mission description

The European Student Earth Orbiter (ESEO) is a micro-satellite mission to Low Earth Orbit. It is being developed, integrated, and tested by European university students and ALMASpace[2] (now SITAEL Spa) as an ESA Education and Knowledge Management Office project.

ESEO satellite should be ready for launch in the second half of 2016. It will orbit the Earth Sun-synchronously about 550 Km of altitude with a nadir-pointing attitude, taking pictures, measuring radiation levels and testing technologies for future satellite missions.

2.1.1 Objectives

The mission main objectives of the ESEO spacecraft are:

- To take pictures of the Earth and/or other celestial bodies from Earth orbit for educational outreach purposes;
- To provide dosimetry and space plasma measurement in Earth orbit and its effects on satellite components;
- To test technologies for future satellite missions**.**

In order to accomplish the first two objectives the following payloads have been boarded: a micro camera (uCAM), operating in the visible spectrum, the plasma diagnostic probe (LMP) and the tri-dimensional dosimeter instrument (TRITEL). In particular the LMP shall measure the electron density and the electron temperature, while the TRITEL shall measure the LET (Linear Energy Transfer) spectra, the absorbed dose and the dose equivalent.

In order to provide high speed datalink for scientific data transmission a dedicated S-band transmitter (HSTX) is provided as payload complement.

[2] ALMASpace: prime contractor of the ESEO project, was a small Italian company focused on R&D of low-cost small satellites and space technologies. It has been acquired by SITAEL, a bigger Italian company involved in railways and aero-space fields, during 2015.

The realization of third objective consist in the flight testing of a GPS receiver for orbit determination and a de-orbit mechanisms (DOM) to be activated in order to comply with space debris mitigation policies.

Functional and performance tests will be performed during the satellite operative phase and the results examined on ground by the design team, in order to gain a full space qualification in view of their use on other missions.

The satellite will also carry on board a payload proposed by the AMSAT community, it will allow the satellite to be exploited by the radio-amateur community after the end of its operative phase.

With reference to the mission requirements, reported in the Consolidated Report on Mission Analysis document, the following success criteria breakdown has been defined in order to have a numerical evaluation of the objectives of the mission:

First Level Objective	Relative/Absolute value	Second Level Objective	Relative value	Absolute value	Third Level Objective	Relative value	Absolute value
Education	25%	Training	40.0%	10.0%	Lecture Course	40.0%	4.0%
					Training Course	20.0%	2.0%
					Internship	40.0%	4.0%
		Hands-on experience	30.0%	7.5%			
		S/C Engineering	30.0%	7.5%			
Technology Development	25%	Provide dosimetry and space plasma measurement in Earth orbit	30.0%	7.5%	TRITEL P/L	50.0%	3.75%
					LMP P/L	50.0%	3.75%
		Test technologies for future education satellite missions	70.0%	17.5%	HSTX P/L	20.0%	3.5%
					DOM P/L	20.0%	3.5%
					ADE P/L	20.0%	3.5%
					GPS P/L	20.0%	3.5%
					MPS P/L	20.0%	3.5%
Outreach	15%	Take pictures of the Earth and/or other celestial bodies from Earth orbit - uCAM P/L	25.0%	3.75%			
		S/C Telemetry Data freely	30.0%	4.50%			

		distributed via the UHF-band beacon					
		AMSAT-UK P/L	25.0%	3.75%			
		Project Website	15.0%	2.25%			
		Publications	5.0%	0.75%			
Mission Operations	35%	**Space Segment Functionality**	70.0%	24.5%			
		Ground Segment Functionality	30.0%	10.5%	Ground Station Forlì	50.0%	5.25%
					Ground Station Vigo	20.0%	2.10%
					Ground Station Munich	30.0%	3.15%
						Total	100.0%

Table 2.1 ESEO Success Criteria

2.1.2 Requirements

The full set of requirements of the ESEO mission/spacecraft are listed and reported in the Mission Requirements Document (MRD).

The contributions and results of this work regard the fulfilling of the main requirement of the mission concerning the space segment:

- Ensure an orbital life time of six months, extendable up to 18 months.

As shown in Table 2.1 ESEO Success Criteria, the achievement of this goal, space segment functionality, will ensure the 70% of the mission operations success and 24.5% of the whole project.

Degraded mission performance

In case of failure of units, depending on the severity of the impact on the system, mission objectives can be still partially achieved or fully achieved with degraded performance. In particular:

- In case of failure of a redundant platform unit the secondary unit can be used without affecting system performance.

- In case of failure of a non-redundant unit mission objectives can be fully achieved with degraded performance.
- In case of failure of a scientific payload (TRITEL, LMP, CAM) mission objectives can be partially achieved.
- In case of failure of a technological payload (DOM, ADE, AMSAT) mission objectives can be partially achieved.
- In case of failure of HSTX mission objectives can be fully achieved with degraded performance by using the on-board TMTC and the AMSAT payload (with limited data-rate and reduced operations schedule.

2.2 SPACE SEGMENT

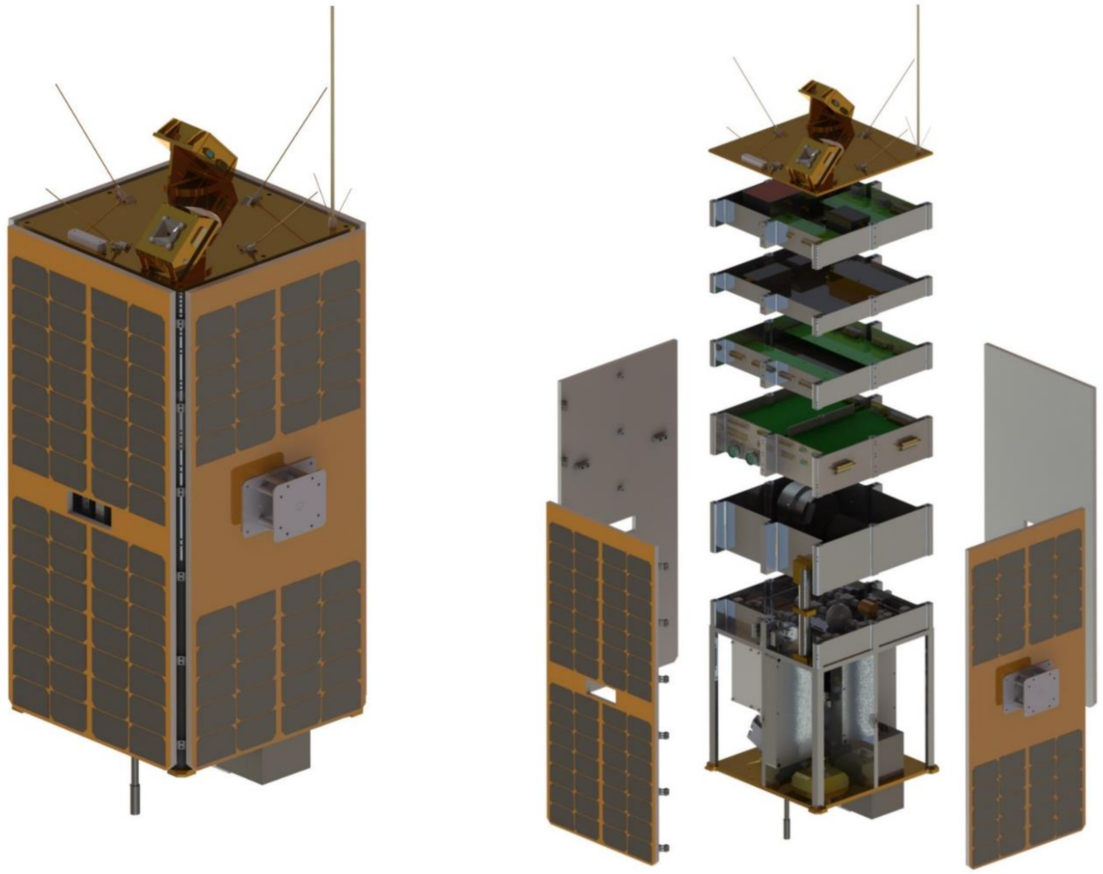


Figure 2.1 ESEO space segment

The ESEO structure is composed by a bus module, containing all the main subsystems and a composite payload module carrying most of the payloads.

The bus module has a tray-based architecture inherited from ALMASat-1, ALMASat-EO2[3]. It must provide mechanical structural integrity to the spacecraft and interface between platform subsystems. Each aluminium tray contain a specific subsystem or a set of it.

The payload module is composed by honeycomb panels and aluminium supports interfacing with the payloads by mean of inserts. Four lateral honeycomb panels complete the assembly and provide the substrate for the main solar arrays, three solar panels body mounted. The final shape is a parallelepiped with a square base of 30 x 30 x 80 cm and a weight of 45Kg.

2.2.1 Spacecraft modes

The ESEO operational modes are derived from the general timeline of the mission, composed by three main phases:

- *Launching and pre-orbital*
- *Orbital*
- *Re-entry*

In Figure 2.2 the Flow diagram of the ESEO mission shows the mission’s phases related to the operational and safe modes of the S/C. The different states are reached asynchronously and the transitions are event driven. In the diagram are shown also the causes/events that lead to a different platform mode, summarizing most of the FDIR actions that will be undertaken at system point of view.

[3] ALMASat-1, ALMASat-EO are previous satellites developed by ALMASpace.

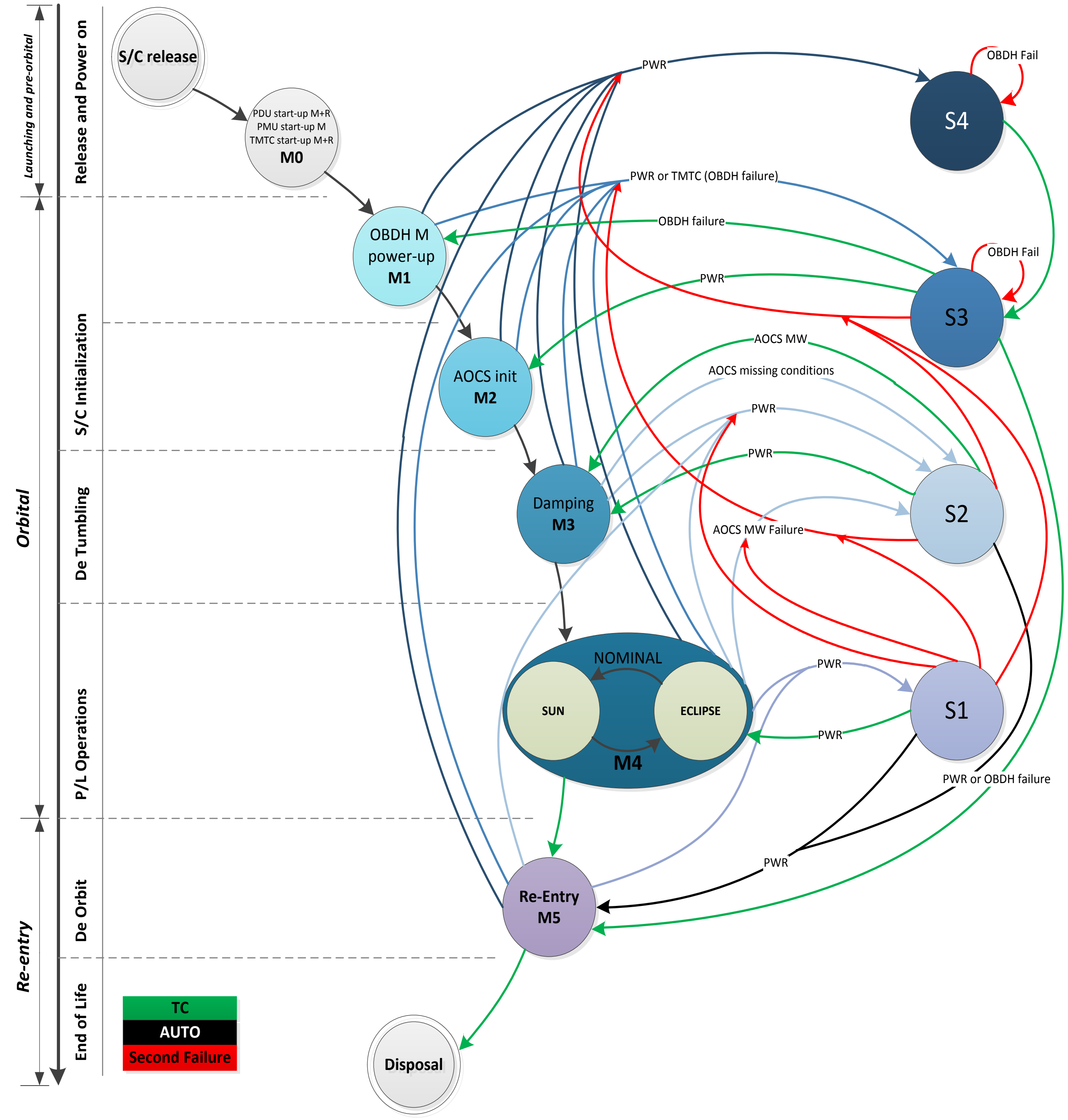


Figure 2.2 Flow diagram of the ESEO mission

2.2.1.1 Normal modes

Launching and pre-orbital

- *Mode 0: Spacecraft start up*

Immediately after the separation, end of the launching and pre-orbital phase, the sequence of events is described as follows: the S/C is powered by the activation of the Isolation Switch, connecting the batteries and the Solar Panels to the power system. This operation is implemented by means of a separation switch, an electro-mechanic interface connected directly to the isolation switch.

Once powered, the main systems are configured as follow:

- TMTC (R-LCL) main and redundant: active
- PDU (directly connected to the power source, S3R) main and redundant: active
- OBDH (R-LCL)main and redundant: stand-by
- PMU (LCL) main: active

Orbital

The OBDH software (ASW, application software) manages the operational modes of the ESEO satellite. The modes are divided in four main sequences.

Platform modes:

- *Mode 1: OBDH power up*

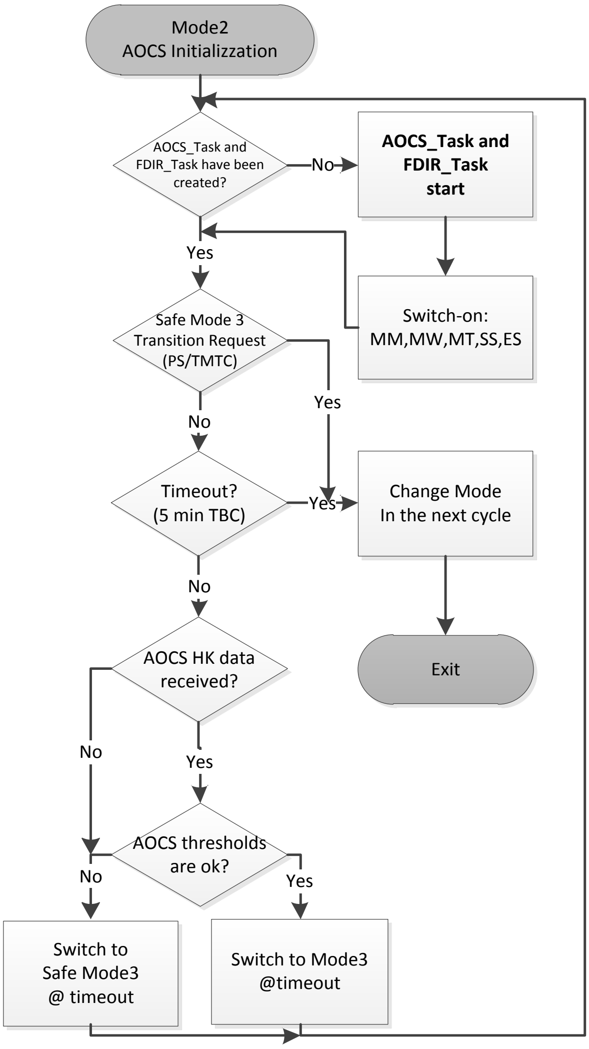
The TMTC, during the initialization, is in charge to turn on the OBDH main unit in order to start the required operations that leads to the nominal mode (Mode 4) of the spacecraft if possible. In this phase the platform FDIR task is active and capable to detect and manage failures of the TMTC, OBDH and PMU. The On Board Data Handling starts the initialization sequence, creating the first SW tasks: Platform time management and the HK and TC management.

- *Mode 2: AOCS initialization*

After the power up, the OBDH perform the initialization of the AOCS task, it turns on the equipment and start collecting HK and generating beacon and then the AOCS FDIR is created and started.

S/C configuration:

- *TMTC (R-LCL) main and redundant: active*
- *PDU main and redundant: active*
- *OBDH (R-LCL) main: active*
- *PMU (LCL) main: active*
- *AOCS Equipment:*
  - *MM (LCL) main: active, MW (LCL) main: active, MT(LCL) main: active, SS (LCL) main and redundant: active, ES (LCL): active*



Mode2
AOCS Initializzation
AOCS_Task and FDIR_Task have been created?
No
AOCS_Task and FDIR_Task start
Yes
Switch-on: MM,MW,MT,SS,ES
Safe Mode 3 Transition Request (PS/TMTC)
Yes
No
Timeout? (5 min TBC)
Yes
Change Mode In the next cycle
No
Exit
AOCS HK data received?
No
Yes
AOCS thresholds are ok?
No
Yes
Switch to Safe Mode3 @ timeout
Switch to Mode3 @timeout

Figure 2.3 AOCS initialization

- *Mode 3: AOCS damping*

The OBDH, through the AOCS task, enter in damping mode to start the attitude and stabilization maneuvers.

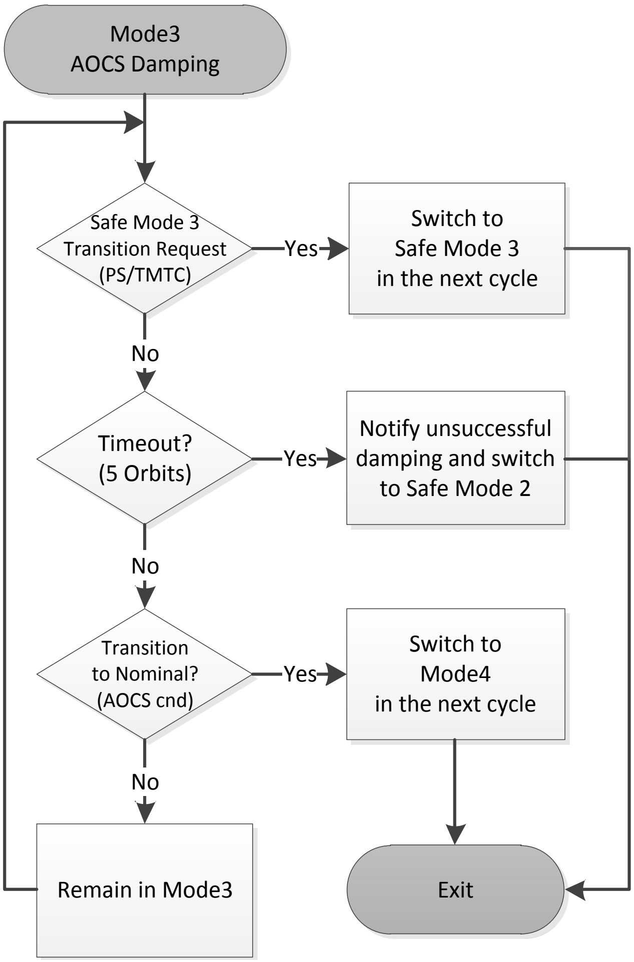


Figure 2.4 AOCS Damping

- *Mode 4: AOCS normal Sun/Eclipse*

This is the normal mode of the satellite, separated in Sun or Eclipse way. The OBDH starts the normal operations, managing the payloads and the equipment according to the scheduling.

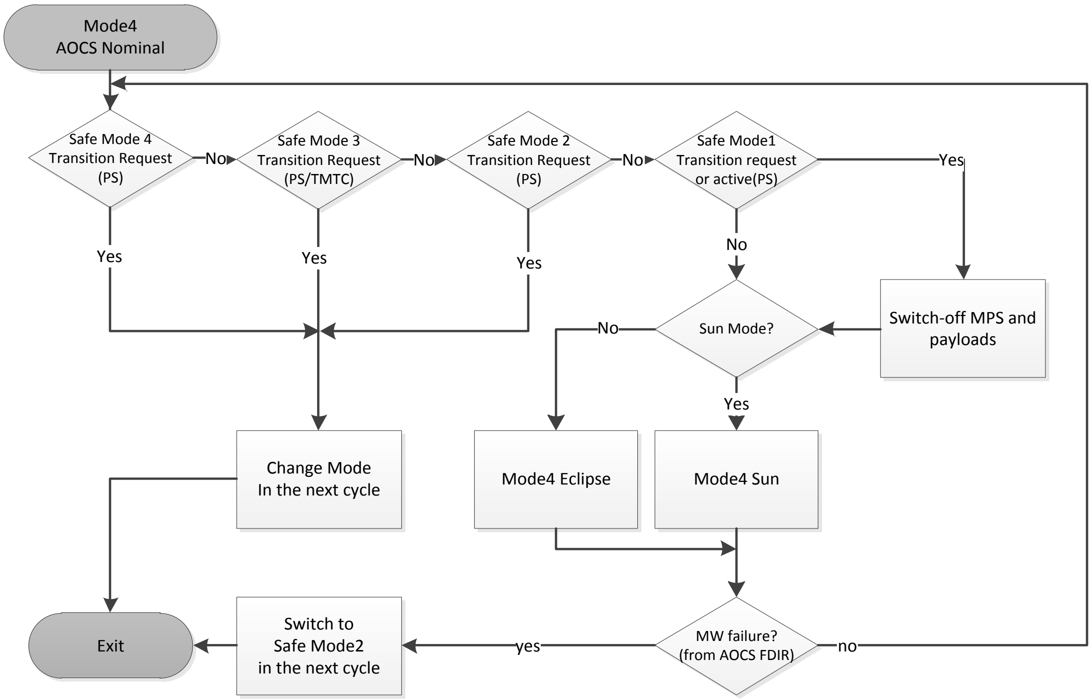

Mode4
AOCS Nominal
Safe Mode 4 Transition Request (PS)
No
Safe Mode 3 Transition Request (PS/TMTC)
No
Safe Mode 2 Transition Request (PS)
No
Safe Mode1 Transition request or active(PS)
Yes
Yes
Yes
Yes
No
Switch-off MPS and payloads
No
Sun Mode?
Yes
Change Mode In the next cycle
Mode4 Eclipse
Mode4 Sun
Exit
Switch to Safe Mode2 in the next cycle
yes
MW failure? (from AOCS FDIR)
no

Figure 2.5 AOCS Nominal

Re-entry

- *Mode 5*

This is the final phase of the mission. The AOCS equipment are switched off and the GPS unit is activated.

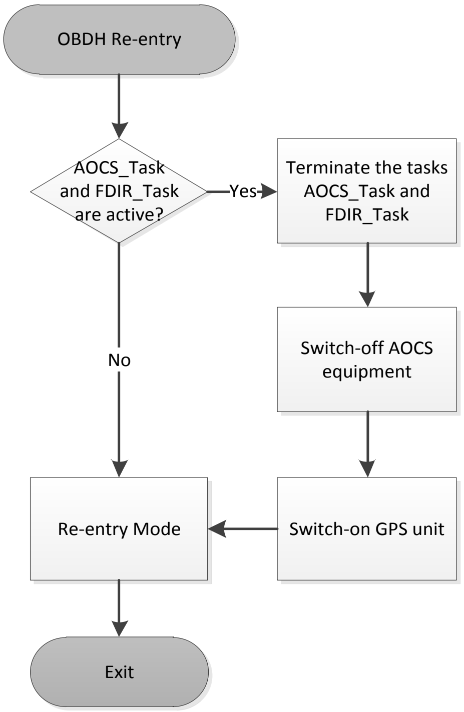

OBDH Re-entry
AOCS_Task and FDIR_Task are active?
Yes
Terminate the tasks AOCS_Task and FDIR_Task
No
Switch-off AOCS equipment
Re-entry Mode
Switch-on GPS unit
Exit

Figure 2.6 Re-entry mode

2.2.1.2 Safe Modes

Four safe modes are included which can be reached asynchronously from the platform modes. The safe modes are activated by hardware thresholds of the power system or by FDIR software due to failures of the ACS equipment. They are:

- **Safe mode S1**: Minor main bus power down.

  This mode is mainly reached during nominal operation, for instance an unexpected decrease of the performance of the main bus referred to the first prefixed threshold. The first action executed is the switch off of the payloads.

- **Safe mode S2**: Severe main bus power down or momentum wheel malfunctions.

  In case of exceeding of a second threshold by the main bus, HW monitored thought PDU subsystem, or the failure of the Momentum Wheel, the OBDH perform the shout down of the payloads, the switches of the wheel, the sun sensors and earth sensors and goes in de-tumbling mode.

- **Safe mode S3**: Major main bus power down, OBDH failure or reprogramming sequence issued.

  In this mode the only subsystems active are the power system and the TMTC whit full functionalities (both RX and TX chain active).

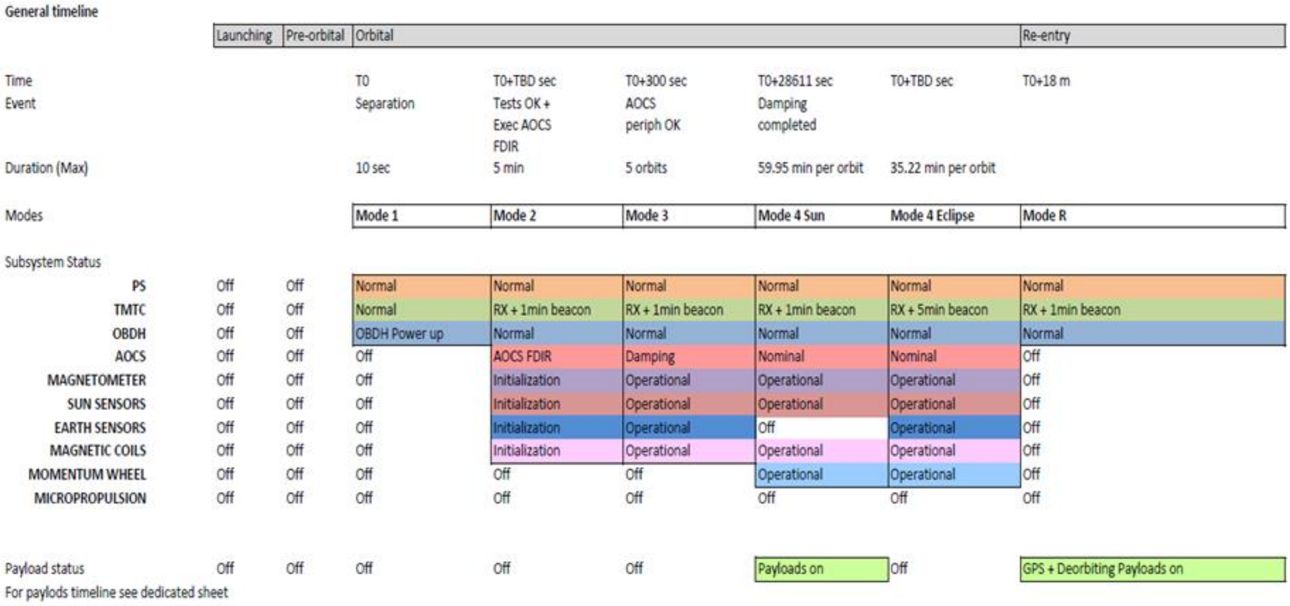
- **Safe mode S4**, or Silent mode: Critical main bus power down. Like S3 mode but the TX chain of TMTC (HPA) is inhibited to save power.

All safe modes can be set and managed by FDIR functions implemented in the S/W of the on-board computer (OBDH), while the S3 and S4 modes can also be invoked by the Platform FDIR processed by TMTC system in case of failure of the OBDH, see chapter 4.

Safe modes recovery requires ground operations.

Safe	Cause		Platform Configuration	State
Mode	PS thresholds	ACS failure		management
S1	Minor bus power down: 23.2V	-	• Nominal Configuration • P/L Off	PS OBDH
S2	Severe bus power down: 22.4V	MW failure	• TMTC On • PS On • OBDH On · MM, MT On	PS OBDH
S3	Major bus power down:21.6V	OBDH Failure or reprogram	• TMTC On • PS On • OBDH (On or Off)	PS TMTC/OBDH
S4	Critical bus power down: 21V	-	• TMTC On (RX Only) • PS On • OBDH (On or Off)	PS TMTC/OBDH

Table 2.2 Safe modes



General timeline								
	Launching	Pre-orbital	Orbital					Re-entry
Time			T0	T0+TBD sec	T0+300 sec	T0+28611 sec	T0+TBD sec	T0+18 m
Event			Separation	Tests OK + Exec AOCS FDIR	AOCS periph OK	Damping completed		
Duration (Max)			10 sec	5 min	5 orbits	59.95 min per orbit	35.22 min per orbit	
Modes			Mode 1	Mode 2	Mode 3	Mode 4 Sun	Mode 4 Eclipse	Mode R
Subsystem Status								
PS	Off	Off	Normal	Normal	Normal	Normal	Normal	Normal
TMTC	Off	Off	Normal	RX + 1min beacon	RX + 1min beacon	RX + 1min beacon	RX + 5min beacon	RX + 1min beacon
OBDH	Off	Off	OBDH Power up	Normal	Normal	Normal	Normal	Normal
AOCS	Off	Off	Off	AOCS FDIR	Damping	Nominal	Nominal	Off
MAGNETOMETER	Off	Off	Off	Initialization	Operational	Operational	Operational	Off
SUN SENSORS	Off	Off	Off	Initialization	Operational	Operational	Operational	Off
EARTH SENSORS	Off	Off	Off	Initialization	Operational	Off	Operational	Off
MAGNETIC COILS	Off	Off	Off	Initialization	Operational	Operational	Operational	Off
MOMENTUM WHEEL	Off	Off	Off	Off	Off	Operational	Operational	Off
MICROPROPULSION	Off	Off	Off	Off	Off	Off	Off	Off
Payload status	Off	Off	Off	Off	Off	Payloads on	Off	GPS + Deorbiting Payloads on
For paylods timeline see dedicated sheet								

Figure 2.7 General mission timeline

2.2.2 ARCHITECTURE

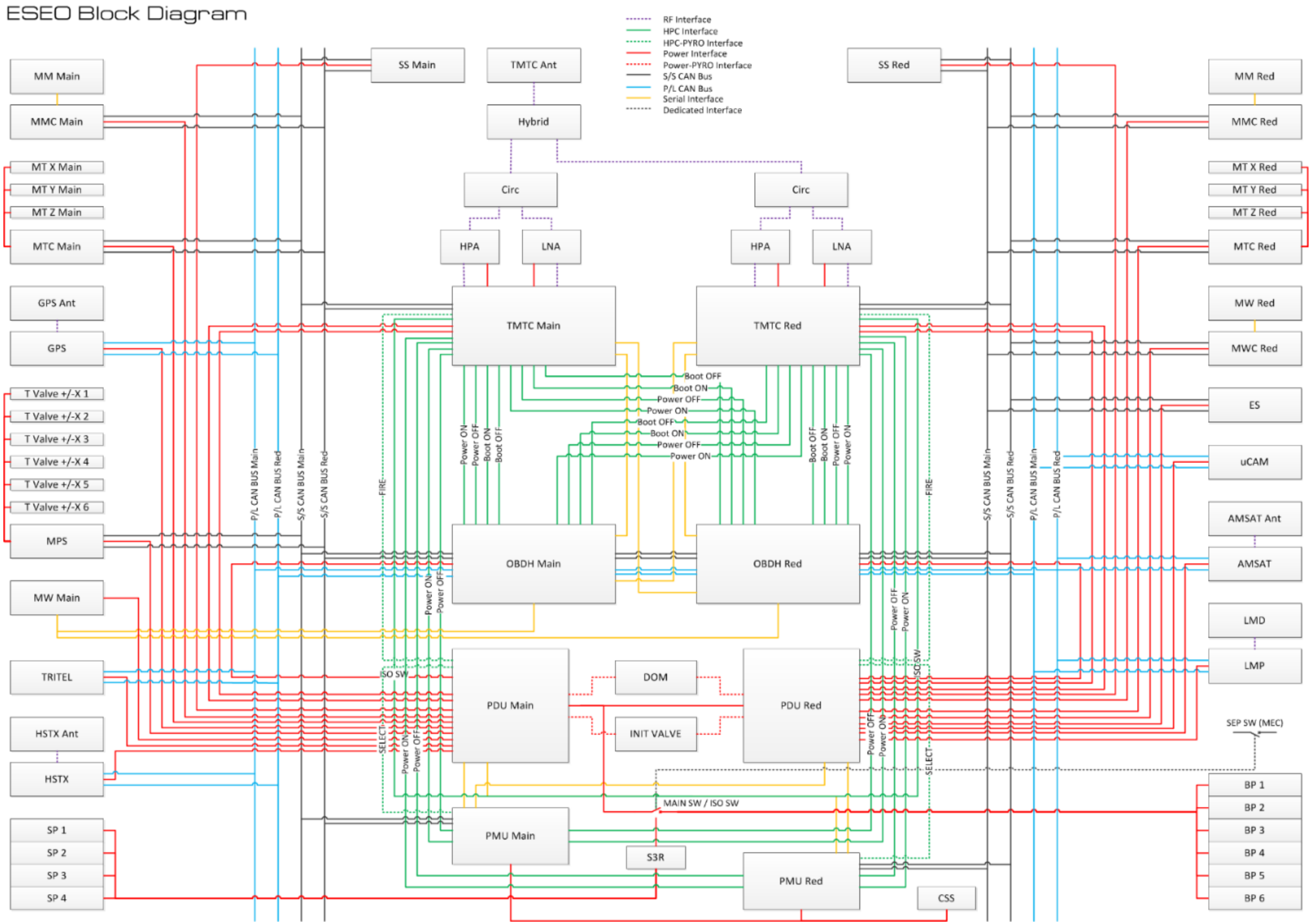


Figure 2.8 ESEO block diagram

Consistent with the block diagram reported above, the spacecraft is mainly based on a fully mirrored architecture. Most functions of the platform are implemented with a «one out of two» cold redundancy to ensure its reliability and availability. In case of a subsystem doubled (or more) but not redounded, the loss of a single unit leads to a performance degradation of the spacecraft, ensuring anyway the mission objectives thanks to a design SPF (Single Point of Failure) free.

The following provides a detailed description of the redundancy concept implemented for the platform:

- Four Antenna are accommodated on the top plate of the spacecraft, one each side to provide Omni-coverage during the orbit.
- At radio-communication level, the HPA and LNA Amplifiers are redounded and managed by the TMTC system.
- The TMTC units are in hot redundancy configuration. The transmitter amplifier (HPA) is in cold redundancy to save power.
- The receiver amplifier (LNA) is used in hot redundancy so as to allow Telecommand reception in any case.
- The Solar Arrays and Battery implement a failure tolerant design. The Solar Array is based upon three body mounted solar panels made of triple junction Gallium Arsenide (GaAs) space grade solar cells. The SA is sized to support the loss of strings during the flight. Six Battery Packs are connected in parallel to provide a reliable design in the occurrence of a battery cell open failure.
- The overall Power configuration provide short charging times and sufficient power to the system, in agreement with the simulations performed on different mission scenarios.
- At Power Managing Board (PMB) level, complex redundancy scheme ensures failure tolerance (Two out of three hot redundancy for the MEA amplifiers and six plus one shunt sections are implemented in the Sequential Shunt Switching Regulator), so to guarantee a spacecraft energetic Fail-Op behavior.
- The PDU Current Limiters (LCL-R-LCL) are not functionally redundant; the open-circuit (O/C) failure case is managed by the switch to the redundant equipment.
- Sun Sensor, Magnetometers, Magneto-Torquers and Momentum Wheel are redundant subsystems. A one out of two cold redounded architecture ensure to drive to a fail-safe design regarding the AOCS functionalities.

- On Board Data Handling (OBDH) is based on cold redundant architecture. The mass memory implemented on each unit is triple redounded managed with a two out of three EDAC mechanism.
- Payload Data are handled directly by the OBDH. The Payloads are interfaced through a dedicated and redounded CAN Bus, and are powered directly by the Power Distribution Unit.

2.2.3 Subsystems

- TMTC

The main function of ESEO Telemetry and Telecommand (TMTC) subsystem is to provide a reliable radio link between the Spacecraft (S/C) platform and the dedicated Ground Station (GS). Moreover, as the only subsystem directly connected with the GS, the TMTC is in charge of manage the Platform Fault Detection Isolation and Recovery (FDIR) operations. Is based on a fully redundant architecture, as shown in Figure 2.9, and guarantees a cold redundancy of the transmitter and a hot redundancy of the receiver. Two independent electronic boards, a main and redundant, have been included in the design, as consequence the electronic board is not single point of failure free. A single electronic board includes the receiver and the transmitter section. The Radio Frequency Distribution Unit (RFDU) connects the two transmitters and the two receivers to the common antenna network, placed on the zenith facet of the ESEO platform.

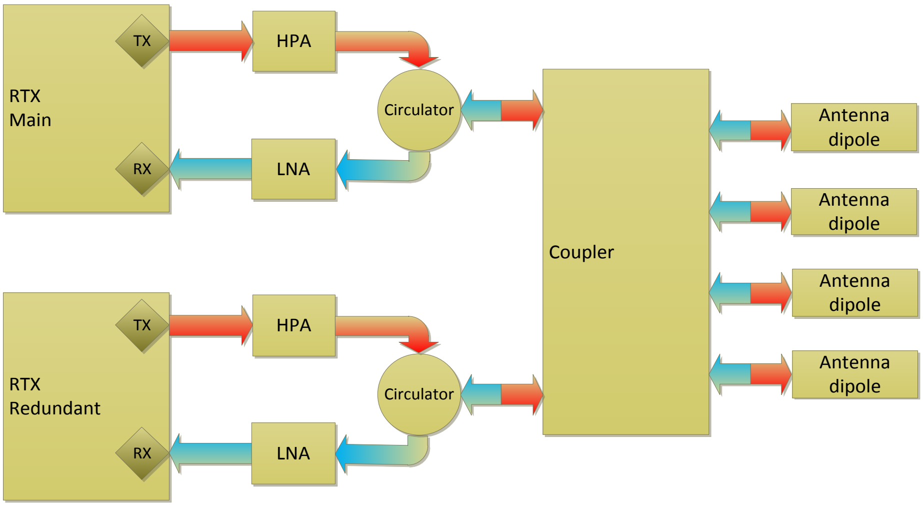


Figure 2.9 TMTC set-up

- OBDH

The ESEO OBDH subsystem consists of two identical units operated in cold redundancy, the Main and Redundant. The OBDH computer hosts also the AOCS functionalities, therefore the system interfaces provide connection with all the peripherals that are necessary to acquire and control the satellite attitude.

The main functions provided by the OBDH subsystem are:

- Validating and executing telecommands received form the ground segment
- Forwarding telecommands to relevant subsystems
- Generating internal telecommands
- Collecting and storing housekeeping data, both from platform and payloads
- Generating periodic reports of housekeeping data, and sending them to the ground segment
- Monitoring a subset of critical housekeeping data, and generating warning and error messages for the ground segment
- Executing the AOCS software
- Maintaining and distributing the platform time

Each OBDH subsystem interface provides data connection with the following subsystems:

- Magnetic coils control boards
- Magnetometer acquisition boards
- Micro-propulsion system
- Momentum wheels main and redundant subsystem
- Sun Sensors
- Earth sensor
- Payloads

The data interfaces are implemented as a redundant CAN bus: two independent busses are used to connect the subsystems, while two additional CAN busses are dedicated to the payload communication. Finally the OBDH is connected with the TMTC subsystem (Main and Redundant) with a serial interface based on the RS422 standard. The only equipment connected with a dedicated data interface, is the COTS main momentum wheel, which uses a serial interface based on RS485 standard.

- Power System

The ESEO Power System (PS) consists of two main subsystems, as shown Figure 2.10 Architecture of PS.

- Power Management Board, PMB
- Power Distribution Unit, PDU

The Power Management Board is a single PCB and includes: the power regulation of the solar panels (S3R), the battery packs I/F, the Isolation Switch and a cold redundant Power Management Unit in charge of the control and measurement of all the fundamental parameters of the system.

The Power System architecture is based on non-regulated topology, in this way the Main Bus voltage is related to the battery voltage. The power conditioning is performed by the Sequential Shunt Switching Regulator (S3R). The solar panels strings are connected to shunt sections which, on the basis of the bus voltage, can decide to open the dump or short the string partially or completely. The Main Bus voltage is acquired by means of the Main Error Amplifier (MEA) which provides a signal proportional to the error integral. For each shunt section a pre-fixed voltage determined by a ladder network determines if the string must be switched on or off as function of the bus voltage. The fault-tolerant design allows the system functioning even in case of failures of the subsystems or parts of the PS itself.

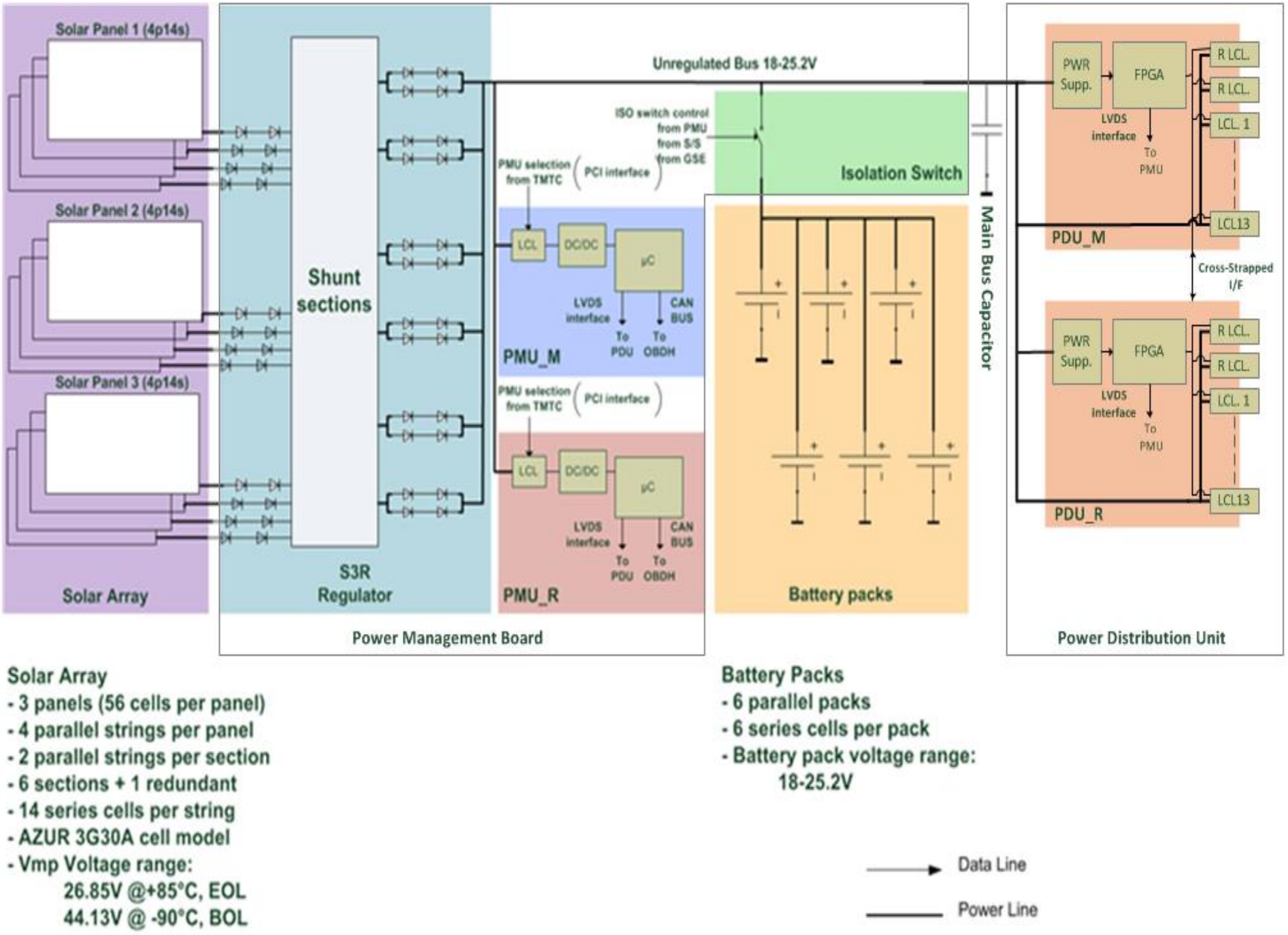
The Isolation Switch, which allows the battery packs connection to the Main Bus, consists in one switch commanded by the mechanical separation switches, by the PMU or by means of dedicated lines in the Ground Segment Equipment (GSE) port. Further, since batteries are directly connected to the Main Bus, the voltage tapering is performed by the S3R regulator limiting the voltage to avoid detrimental effects on them.

The PMU is based on a microcontroller architecture and is directly controlled by the TMTC by means of dedicated control lines (HPC). The data interfaces are implemented as a redundant CAN bus: two independent busses are used to connect the OBDH to provide HK data.

To distribute the electrical power and to protect subsystems and payloads, a Power Distribution Unit (PDU) supplied by BME (Budapest University for Technology and Economics) is used. The PDU is equipped with specific re-triggerable Latching Current Limiters (R-LCL) to protect the essential subsystems (OBDH and TMTC) and a series of LCL for non-essential subsystems/payloads. The PDU is built up on two identical PCB in hot redundancy, placed inside a dedicated satellite tray and communicates with the PMB through a cross-strapped LVDS interface.

The main functions provided by the PS system are:

- Regulate power of the solar panels by mean of Shunt Sections
- Connect or isolate the Batteries power source from the main bus
- Provide Solar Array and Battery Packs interfaces
- Charge Battery Packs
- Provide separate power lines to all subsystems and payloads
- Control the over-current consumption of the loads by mean of LCLs and R-LCLs for the essential subsystems
- Generating periodic reports of housekeeping data, and sending them to the OBDH
- Monitoring a subset of critical housekeeping data, and generating warning and error messages for the ground segment and OBDH.



Solar Array
- 3 panels (56 cells per panel)
- 4 parallel strings per panel
- 2 parallel strings per section
- 6 sections + 1 redundant
- 14 series cells per string
- AZUR 3G30A cell model
- Vmp Voltage range:
  26.85V @+85°C, EOL
  44.13V @ -90°C, BOL

Battery Packs
- 6 parallel packs
- 6 series cells per pack
- Battery pack voltage range:
  18-25.2V

Figure 2.10 Architecture of PS

- Magnetometer I/F

The magnetometer board provide a suitable interface between the magnetometer sensor and the platform communication bus. It is in charge to measure the strength and the direction of the magnetic field on all three axes.

- Sun Sensor

The Sun Sensor itself is based on a redounded architecture of the acquisition channels thanks to the employment of two external ADCs. Located on the top plate of the platform, is the only AOCS subsystem in hot redundancy, responsible to provide satellite-to-sun vector estimation.

- Earth Sensor

The Earth Sensor share the design philosophy of the other boards and is not redounded. The earth recognition capabilities are reached by means of proper on-board algorithms and a thermal imaging camera.

- Magneto Torquers

The Magneto-Torquers board has the task of controlling the coils of the spacecraft. It implements a dedicated driver for the coils and a CAN bus interface. The board is in cold redundancy as well as the magnetic actuators which are disposed on three axes of the platform.

- Momentum Wheels

The Momentum Wheels are used to obtain a stabilization of the satellite pitch axis direction. As for the other functions a cold redundancy architecture is implemented. Nevertheless the main subsystem is provided by Astro-und Feinwerktechnik Adlershof GmbH while the redounded unit, has been developed by ALMASpace so to raise the reliability thanks to technological diversity.

2.2.4 HARDWARE

All the hardware employed in the spacecraft main platform related to the attitude and control system (ACS), the ground communications and the structure, has been designed, developed and partially tested in the ALMASpace facilities in Forlì. The Printed Circuit Boards (PCB) of the satellite are based on Components Off The Shell (COTS) electronic parts, industrial or military grade.

2.2.4.1 Design

The design phase of the subsystems started in the late 2012, inheriting part of the specific unit's architectures from the company's previous projects: ALMASat-1 and ALMASat-EO. The redesign and consolidation step have been performed in accordance with the ESA ECSS standards, but as ruled on the Statement Of Work document (SOW), the standards had to be taken as reference and not strictly applicable.

The design of the Printed Circuit Boards (PCB), has been an iterative process directly related to the test campaign performed at every level of the platform, see chapter 3: Test campaign. The boards have been developed in two different phases: the Elegant Bread Board (EBB), first hardware implementation of the units useful for the first tests and a Flight Model (FM), which represents the final version of the subsystems after the Critical Design Review (CDR).

All the electronics parts have been chosen from lists of selected components, made available by the main space agencies: ESA, NASA and JAXA[4], or directly inherited from previous missions then validated in orbit. The lists are compiled with test results often related with the radiation's characteristics of the device.

The sizing of all the electronic parameters, such as working voltages or characteristics of the components, followed a severe approach about security margins and, in compliance with the ECSS, reduced from 20% to 10% after the tests.

The components implementation followed a de-rating philosophy imposed by ESA and useful to keep all the parts in a safe working-zone during normal operations. For each one of the components, divided by type and family, are identified all the fundamental parameters, such as voltages, currents, and powers, and the thresholds of allowed use fixed in percentage.

2.2.4.2 Part Stress Analysis (PSA)

Strictly related to the component's de-rating, a part stress analysis have been performed. The PSA concerns the thermal behavior of the subsystems due to the power dissipation of the

[4] ESA: European Space Agency, NASA: National Aeronautics and Space Administration, USA and JAXA: Japan Aerospace Exploration Agency

electronic devices. In order to ensure the proper operation the components margins are imposed by the manufacturers and depend on its grade. The common applied temperature ranges definitions are reported in the following:

- Commercial: 0°C to 85°C
- Industrial: −40°C to 100°C
- Automotive: −40°C to 125°C
- Extended: −40°C to 125°C
- Military: −55°C to 125°C

Thanks to an interaction between the Mechanic and the Electronic CAD the boards have been completely modeled and simulated in the temperature range provided by the thermal analysis performed at system level within the mission selected scenario. The parameters taken in to account have been also the PCB manufacture, number and type of layers, dimensions, etc. and the final allocation in the tray. The power dissipation, considered for each component which power consumption was more than 1% of the whole unit, have been checked and compared in order to ensure a safe operation of the devices.

The analysis results leads to some changes in the subsystems design, especially related to the limiting and sensing resistors employed on the power lines and some MOS-FET[5] drivers responsible for the sensor's interfaces or the power management.

2.2.4.3 Production

The EBB boards have been assembled in the ALMASpace clean room in accordance with the space-grade soldering process and supervised by company's internal inspectors. The manufacturing happened in a clean environment with the help of a microscope, fundamental tool to magnify the little components and also survey the soldering joints made of leaded tin. To ensure a proper mechanical backing and don't introduce new stress sources the SMD[6] components have been soldered slightly uplifted from the plane and the through hole parts applied with stress reliefs on the terminals. The most weighted devices have been secured to

[5] MOS-FET: Metal Oxide Semiconductor – Field Effect Transistor

[6] SMD: Surface Mount Device.

the board with thermal adhesives or Kapton[7] tape. The final board's assembly, the Flight Models, will be potted with a space graded resin layer to improve the mechanical and thermal resistance.

2.2.5 Software

ESEO subsystems and main units are equipped with an embedded real time operating [8]system (RTOS): RTEMS.

The data processing and all the functions of the platform are implemented as software tasks such as: FDIR operations, at various level: Platform, AOCS and Unit, HK and TM management, beacon creation, TC decoding, etc.

All the tasks are executed with a period of 1 second and scheduled by means of a Simple Priority Scheduler. The scheduler has the same behavior of the Deterministic Priority Scheduler (schedules tasks using a priority based algorithm, it is implemented using an array of FIFOs with a FIFO per priority, it maintains a bitmap which is used to track which priorities have ready tasks and the algorithm is predictable and fixed in execution time) but uses only one linked list to manage all ready tasks. If a task is ready, a linear search is performed on that linked list in order to determinate where to insert the new readied task. All the nominal tasks implemented have the RTEMS_NO_PREEMPT mode activated in order to avoid the temporarily interruption of the task due to a higher priority task ready to be executed. The task preemption has been disabled to prevent the fragmentation of the task which could result in an increased execution time of the process.

Like every other aspect of the platform also the on board software is covered by dedicated verification, analysis, inspections and tests in order to ensure its proper behaviour.

[7] Kapton: polymide film developed by DuPont in the late 1960 that remains stable across a wide range of temperatures, from −269 to +400 °C.

[8] FIFO: First Imput First Output

2.2.6 F.M.E.A. (Failure Mode and Effects Analysis)

The purpose of the FMEA, in accordance with the standard ECSS-Q-ST-30-02C, is to identify all failure modes of the system and rank them in accordance with the severity of the effects of their occurrence. Furthermore, it is to:

- identify and possibly remove or control the Single Point Failures, to reduce failures causing outages or safety impacts
- identify requirements for controlling failure effects to eliminate failure propagation
- control and reduce failures which, occurred during tests and manufacture and remaining undetected till launch, would seriously impact on mission success
- validate and verify design redundancies.

The FMEA analysis is an iterative process that allow the correlations between the failure's severity and consequences with the compensation methods introduced in the system during the design phase, which is continuously updated by the result of the analysis itself.

Failure Modes and Effects Analysis (FMEA)										
Product: ESEO *Subsystem: TMTC*			***Date: 19/03/2015***			***Document ref.: AS\12_0005\SYS\AR-09*** ***Issue: 1.0***				
Ident. number	**Item / block**	**Function**	**Assumed failure mode**	**Failure cause**	**Missi on phase**	**Failure effects:** **a, local effects** **b, End effects**	**Severity class.**	**Failure detection method**	**Compensating provisions**	**Remarks**
1.1.1.	1	Provide 12V output	Increased output voltage	1, failure of internal control/ driver circuit	flight	a, OVP intervention a, loss of LNA b, loss of board	2	HK and TM, Loss of communication with TMTC redundant and OBDH	1, HW timed power cycle 2, Use of redundant RTX board in hot redundancy with cross-strapping of communication and control lines	Platform FDIR OVP interventi on if Vout >14V
1.1.2.	1	Provide 12V output	Decreased / loss of output voltage	1, failure of internal control/ driver circuit 2, SC/OC of any internal component 3, SC/OC of input EMI filter	flight	a, loss of 3.3V output a, loss of µC a, loss of LNA b, loss of board	2	HK and TM, Loss of communication with TMTC redundant and OBDH	Use of redundant RTX board in hot redundancy with cross-strapping of communication and control lines	Platform FDIR

Figure 2.11 FMEA Worksheet

The tool used to perform the FMEA analysis is called FMEA worksheet, in Figure 2.11 above is reported an example.

The FMEA is focused in the maximization of the mission's success probability, verifying also the design philosophy of the whole system. It is aimed to check and highlight all the solutions implemented at every level of the spacecraft, taking into account the reliability theory and its enhancement.

In the paragraph 2.2.6.2 results will be detailed down to unit level in order to analyze the failure propagation and effects on the internal and external interfaces.

2.2.6.1 System F.M.E.A.

In order to ensure the proper coverage of the failures and simplify the analysis process the spacecraft have been divided in several functions, common for each satellite:

- Communications
- Data handling
- Guidance and navigation
- Power
- Thermal control
- Structure
- Propulsion
- Mechanism
- Scientific

All the subsystems have been related to the main functions of the platform. In the tables below, Table 2.3 and HPC: High Priority Commands; **XS:** Cross-strapped interface; **Lcl:** Latch current limiter; **RLcl:** Retriggerable Lcl; **MUX:** Multiplexed lines; **R**: Redounded

Table 2.4, the redundancy configuration and the unit's interconnections have been highlighted.

Funct. HW	TMTC [HPA, LNA]	OBDH [AOCS SW]	PS [PMB,PDU, BP, SP]	MM	SS	ES	MTQ	MW	BUS Mod.	GPS	MPS	DOM	AMSAT	HSTX	TRITEL	LMP	uCAM
Comm.	Hot Red. Rx Cold Red. Tx												X	X			
Data Handling		Cold Red.															
Guidance Navigation		Cold Red.		Cold Red.	Hot Red.	Cold Red.	Cold Red.	Cold Red.		X							
Power			Hot Red. PDU Hot Red. BP, S3R Cold Red. PMU														
Thermal Control									X								
Structure									Alum. Trays								
Propulsion											X						
Mechanism												X					
Scientific															X	X	X

Table 2.3 System functions and HW redundancy configuration

Function	HW HW	TMTC	OBDH AOCS SW	PS PMB	PDU	BP	SP	MM	SS	ES	MTQ	MW
Comm.	TMTC	CAN R	HPC XS RS422 XS CAN R	HPC XS CAN R	RLcl							
Data Handling	OBDH AOCS SW	HPC XS RS422 XS CAN R	-	CAN R	RLcl			CAN R	CAN R	CAN R	CAN R	CAN R RS485
Power	PS PMB	HPC XS, CAN R	CAN R	Lcl	LVDS XS	ISO SW	S3R					
	PDU	RLcl	RLcl	LVDS XS	MUX	ISO SW	S3R	Lcl	Lcl	Lcl	Lcl	Lcl
	BP			ISO SW	ISO SW							
	SP			S3R	S3R							
AOCS	MM		CAN R		Lcl							
	SS		CAN R		Lcl							
	ES		CAN R		Lcl							
	MTQ		CAN R		Lcl							
	MW		CAN R RS485		Lcl							
Structure	BUS Mod.	Tray 6	Tray 4	Tray 3			4x Body Mounted	Tray 5	Top Plate	P/L module	Tray 2	

HPC: High Priority Commands; **XS:** Cross-strapped interface; **Lcl:** Latch current limiter; **RLcl:** Retriggerable Lcl; **MUX:** Multiplexed lines; **R**: Redounded

Table 2.4 Subsystems interaction matrix

With reference to the system block diagram, reported in chapter 2.2.2, for the FMEA purpose at ESEO spacecraft level, the following high level functional blocks have been identified:

- Platform
- Payload

Log #	Element	Item #	Function	Remarks
	AOCS	**1**	**Guidance Navigation and Control**	
1	MW	1.1	Momentum storage device to obtain a stabilization of the satellite pitch axis direction	
2	MT	1.2	Apply the required attitude control torque	
3	MPS	1.3	Generate thrust to allow in-plane orbital maneuvers	
4	SS	1.4	Provide satellite-to-sun vector estimation	
5	ES	1.5	Provide satellite-to-earth vector estimation	
6	MM	1.6	Measure the variation of the geomagnetic field	
7	SW	1.7	Manage attitude sensor and actuators by means of the implemented control laws	
	OBDH	**2**	**Data Handling**	
8	Onboard computer	2.1	Platform and payloads controller	
9	Power conversion stage	2.2	Provide power conversion from PDU	
10	I/O	2.3	Implement the required analog and digital I/O for HK and ACS	
	TMTC	**3**	**Communications**	
11	RTX - Transmitter	3.1	Provide transmission capability to the platform	
12	RTX - Receiver	3.2	Provide receiving capability to the platform	
13	HPA	3.3	Provide amplification for TX chain	
14	LNA	3.4	Provide amplification for RX chain	
15	RFDU	3.5	Route signal from RTX to the antenna	
	PS	**4**	**Power**	
16	PMB	4.1	Manage power regulation	
17	PMU	4.1.1	Communication and control unit of the PMB	
18	S3R	4.1.2	Manage and regulate power from solar arrays	
19	SA I/F	4.1.3	Provide interface with the solar array	

20	BP I/F	4.1.4	Provide interface with the battery packs	
21	PDU I/F	4.1.5	Provide interface with the power distribution unit	
22	PDU	4.2	Provide power distribution capability	
23	SA	4.3	Generate power during sunlight	
24	BP	4.4	Energy storage and supply	
	STR	**5**	**Mechanical**	
25	Bus Module	5.1	Provide mechanical structural integrity and I/F between platform subsystems	
26	Payload Module	5.1	Provide mechanical structural integrity and I/F between platform and payloads	

Table 2.5 ESEO Platform Functions

Log #	Element	Item #	Function	Remarks
101	uCAM	10.1	Take picture of the earth and/or other celestial bodies from earth orbit	
102	TRITEL	10.2	Measure characteristics of the space environment in terms of LET spectra, absorbed dose and dose equivalent	
103	LMP	10.3	Measure characteristics of the space environment in terms of electron density and temperature	
104	HSTX	10.4	Provide high speed downlink capabilities for payloads scientific data	
105	DOM	10.5	De-orbit the spacecraft by mean of drag sail mechanism	
106	AMSAT	10.6	Provide communication capabilities for educational and radio-amateur community	

Table 2.6 ESEO Payload Functions

To perform the analysis some basic rules and assumptions have been followed and the evaluations applied to all the phases: ground operations, launch and the flight.

The FMEA analysis took into account the reliability target and relevant assumptions reported in the paragraph 2.1.2: Requirements, and fully described in the Mission Requirements Document.

All the analysis has been performed till the point of first failure, unless the malfunctioning considered was related to a vital function of the platform, for example the TMTC system which is the first one in the communication chain, or Power System.

The Criticality Categories has been assigned to each identified failure mode in compliance to the potential observed failure effect on the system level. The following consequences severity categories according to ECSS-Q-30-02A have been assigned to the identified failure modes:

Severity Cat. ECSS-Q-30-02A (2001)	Severity Cat. ECSS-Q-30-02C (2009)	Index	Failure Effects
Catastrophic	Catastrophic	1S	Loss of life, life-threatening or permanently disabling injury or occupational illness loss of an element of an interfacing manned flight system (*) Loss of launch site facilities Long-term detrimental environmental effects
Catastrophic	Catastrophic	1	Loss of system
Critical	Critical	2S	Temporary disabling but not life threatening injury, or temporary occupational illness (*) Loss of, or major damage to other flight systems, major flight elements or ground facilities public Loss of, or major damage to public or private property Short-term detrimental environmental effects
Critical	Critical	2	Loss of mission
Major	Major	3	Mission degradation
Negligible	Minor or Negligible	4	Any other effects

Table 2.7 Severity categories and classes reference

The suffix "R" has been added to the criticality index in the worksheets when the functionality is redounded.

- Failure Effect Summary List (FESL)

The final report of the analysis include a summary of the FMEA Worksheets, here not annexed. The failure modes thus identified are listed in the failure effect summary list, reporting all the identification numbers, see Figure 2.11 FMEA Worksheet, in order to provide an easy consultation of the ESEO spacecraft and mission failures. In the following table is reported as example the ESEO system FESL:

Item	Failure mode	Severity Category, Index, Effect
Platform	1.7.1, 2.1.1, 2.2.1, 2.3.1, 3.1.1, 3.2.1, 3.3.1, 3.4.1, 3.5.1, 4.1.1, 4.1.5, 4.2.1, 5.1.1, 5.2.1	Critical, 2, Loss of mission
	1.1.1, 1.2.1, 1.2.2, 1.3.1, 1.4.1, 1.5.1, 1.6.1, 4.1.2, 4.1.3, 4.1.4, 4.2.1, 4.2.2, 4.3.1, 4.4.1, 4.4.2	Major, 3, Mission degradation
Payloads	10.1.1, 10.2.1, 10.3.1, 10.4.1, 10.5.1, 10.6.1	Major, 3, Mission degradation

Table 2.8: ESEO system FESL

- **Critical items**

An item has been considered critical if the failure mode is classified as: severity categories 1S, 1, 2S, and 2.

All failure modes leading to consequences with severity category 1S, 1, 2S, and 2 have been analyzed down to a level to identify all single point failures.

With reference to FMEA Worksheets the following item have been identified, at system level, to be critical for the correct fulfillment of all the planned operations:

Item	Action
PMB	Power Management Board architecture and design have been supervised by ESA experts in order to ensure a single point of failure (SPF) free system.

The Power Management Board (PMB), described in paragraph Subsystems, is the first unit in the power supply chain of the spacecraft and also the one responsible for the power generation, in conjunction with the battery packs and the solar array. A critical failure to the main power bus due to a short circuit in the driver electronic will lead to an instant power down of the whole system and thus the loss of the mission. While, thanks to the system architecture, every other equipment or subsystem is protected also by the Power Distribution Unit in charge of monitoring all the single supply lines. Because of this considerations, with the objective to ensure a SPF free design, the development of this unit have been partially performed and supervised by ESA experts and passed the CDR, Critical Design Review sustained with the ESA panel of the ESEO mission during 2015, as well as the tests planned in the test campaign, chapter 3.

2.2.6.2 Subsystem F.M.E.A.

The FMEA for the subsystems have been performed according to hardware approach following the ECSS-Q-ST-30-02C standard like at system level.

Thanks to the modularity applied to the subsystems designed, it has been possible to break up each unit in common functional blocks, plus the custom interfaces.

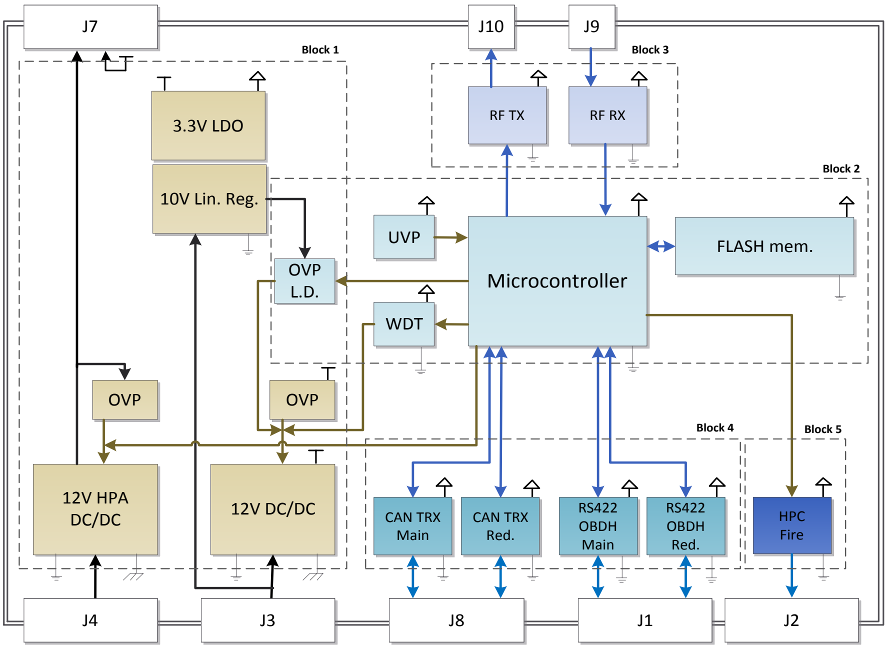
The blocks shared between all the subsystems are:

- Power
- µC and Logic
- Communications
- HPC (High Priority Commands)

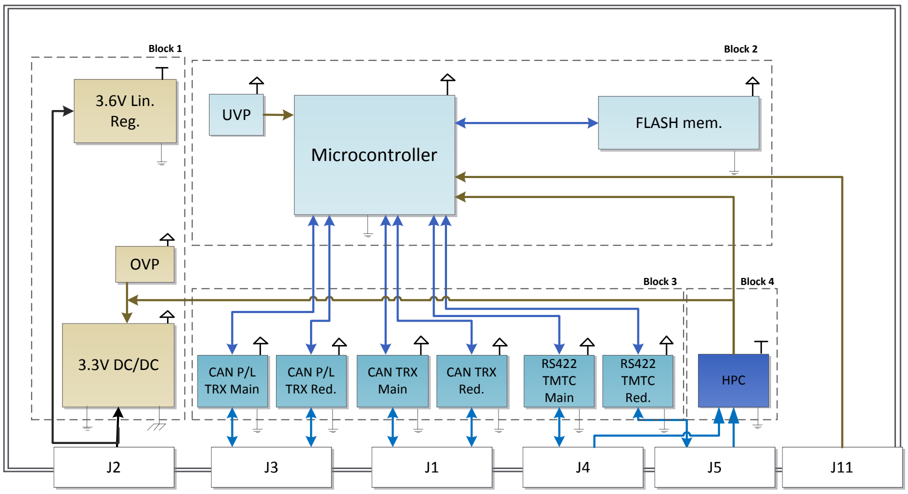
Custom unit's blocks:

- TMTC: Radio, Fire
- PMB: Sequential Shunt Section Regulator (S3R), Isolation switch and battery packs I/F
- ACS units: Actuator or sensor specific I/Fs

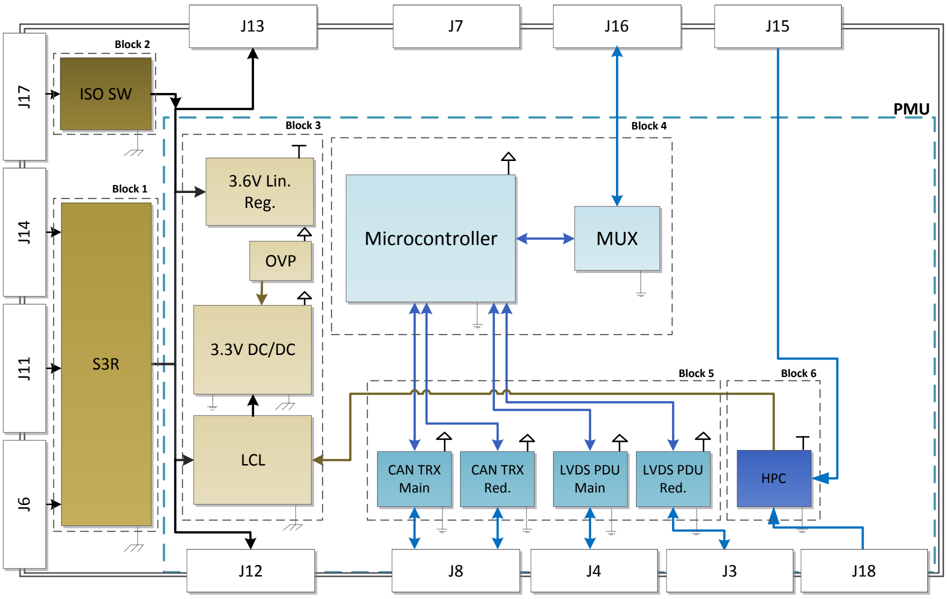
In the following are reported the blocks division for each unit involved in the analysis, the schemes highlight also the connectors name and disposition, in order to permit the check of the platform harness.



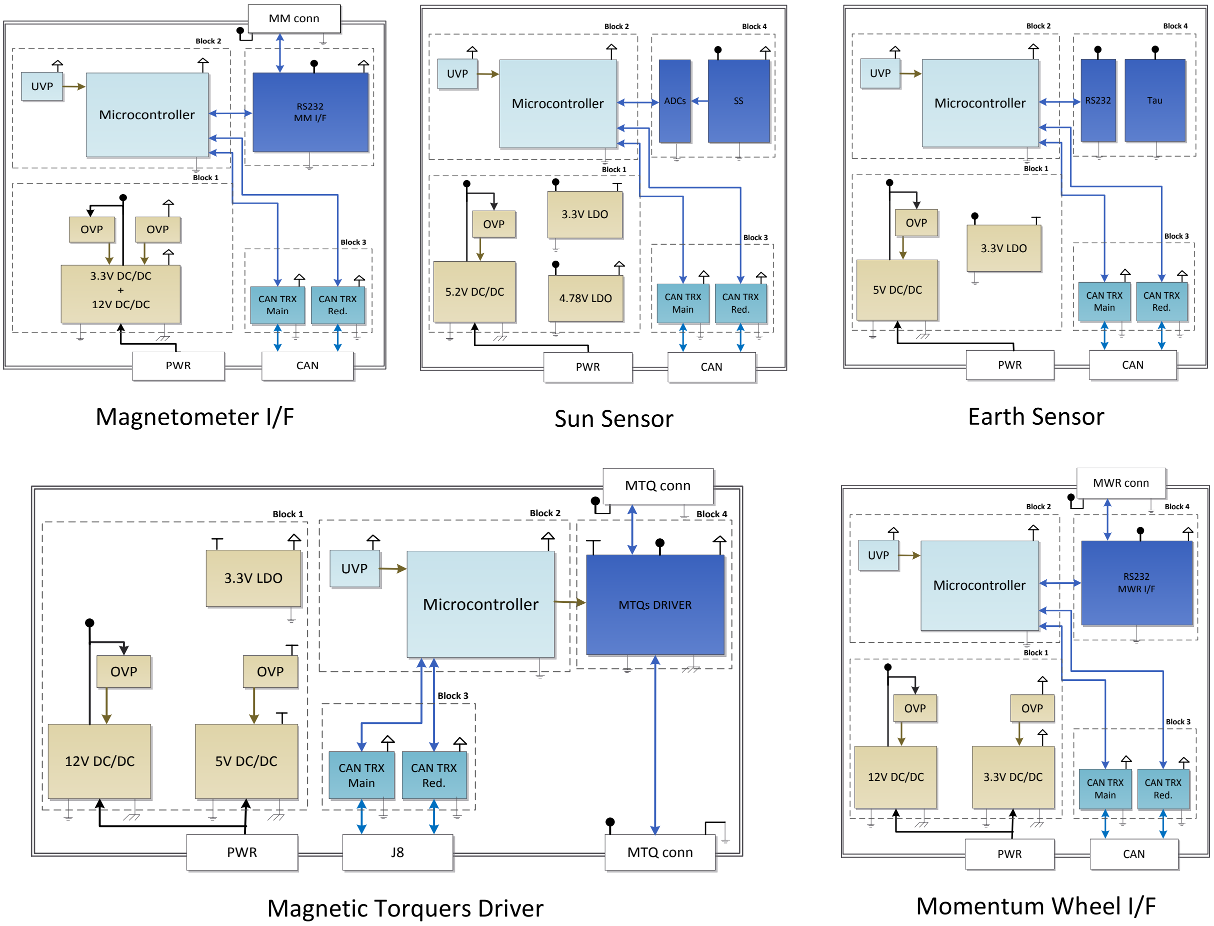
TMTC



OBDH



PMB



Magnetometer I/F

Sun Sensor

Earth Sensor

Magnetic Torquers Driver

Momentum Wheel I/F

Figure 2.1 ESEO Boards: functional blocks division

For each block all the electronic parts involved in the functions have been identified and listed in order to correlate the specific failures and the electrical schematics of the boards, in accordance with the ECSS standard and the literature on the reliability of electronic components about failures.

Summary of the assumed failure modes of the main components:

- Capacitors: Open Circuit (OC), Short Circuit (SC)
- Connectors: omitted
- Diodes: OC, SC (SC to structure is omitted)
- Microcircuits: Any single I/O SC to V+/V-, output stuck to 0/1 or high impedance, OC of any single power supply, SEU: SEL and SEFI, functional failures
- Resistors: OC
- Transformers: OC, SC

- Transistors: Any single terminal OC, SC between any two terminals;
- Opto-electronics Diode OC, Transistor OC, SC between any two diodes and transistor terminals is omitted

The analysis assessed failure effects within the individual hardware block, identified for each subsystem, and the failure effects on the internal and external interface of the subsystems as well.

- Only one failure is considered at each time (first failure) and failures are independent.
- Failures due to wear out are excluded.
- Failures of connectors and mechanical interfaces are considered improbable per design implementation.

At subsystem level the Criticality Category has been assigned to each identified failure mode according to the observed failure effect on the subsystem. The following consequences severity categories have been assigned to the identified failure modes:

Catastrophic – 1, Failure propagation to other S/S

Critical – 2, Loss of Subsystem

Major – 3, Degradation of S/S functions

Minor – 4, Degradation of S/S functions

Even in this case the suffix "R" has been added to the criticality index when the functionality is redounded on board.

Exactly like at system level, the final report include a Failure Effect Summary List detailed for each subsystem involved in the analysis.

The subsystem FMEA showed that the design is free from the following failure mode consequence:

- Failure propagation from one board to any other S/S.

These failure mode effects are given severity level 1 – "Catastrophic".

The following mode effects have been given severity level 2 – “Loss of Subsystem”.

- SPF leads to loss of main functions: Communication, Control, Power
- SPF leads to loss of Subsystem
- SPF leads to loss of power regulation

2.2.6.3 Conclusions

The analysis represents the status of the Spacecraft at CDR stage.

The FMEA covered every kind of failure at system and HW level highlighting for each one the criticality, in reference to the rules and assumptions described above.

No failure propagation between units have been identified (marked as Catastrophic, 1) in the detailed HW analysis. Other severity classification: Critical, 2, loss of the subsystem and Major, 3, degradation of S/S functions have been analysed showing for every failure a compensating method mainly based on platform redounded architecture, with both hot and cold strategy, embedded circuit redundancy and single point of failure free design.

The most critical aspects of the satellite are represented by the PMB, responsible for the power regulation and the PDU in charge of the power distribution. As direct consequence of the FMEA results a detailed analysis of the Isolation Switch and the Sequential Shunt Section Regulator (S3R) have been performed in order to ensure a reliable architecture; furthermore all the units of the spacecraft have been equipped with one or more, depending on the specific architecture and functions, Over Current Protection circuit (OCP) to properly face the single event upsets caused in orbit by heavy ions on the microelectronics. The OCP is described in the FDIR paragraph Level 1: Hardware.

3 TEST CAMPAIGN

Several test have been performed on the ESEO platform boards at system and subsystem level with the aim to validate and support the FMEA analysis, fulfill the system inspection to be compliant with the requirements and also to produce useful inputs for the FDIR strategies. The test campaign has been thought to ensure a complete knowledge of the boards in order to allow a model based strategy, moreover it allows the proper characterization of the device's behavior in a condition as close as possible to the real space environment in which the satellite shall operate.

3.1 POWER AND ELECTRICAL INTERFACES TEST

Electrical and functional test have been performed, at every stage, in order to check and validate the design and manufacture of each subsystem. All the process has been conducted in the ALMASpace Clean room in Forlì. The facility is fully equipped with antistatic floor and furniture and grounded surfaces to properly operate the equipment under test (E.U.T.).

The test has been performed with ambient temperature of 20°C ±1 and the tools used were: digital multimeter, oscilloscope, current clamp, stabilized power supply, balance and digital caliper.

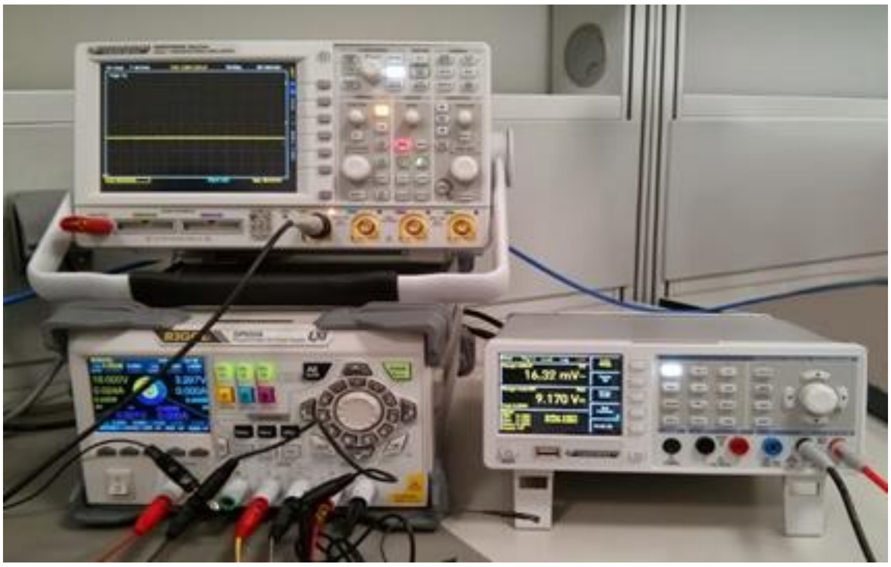


Figure 3.1 Test set-up

For each equipment the parameter checked have been:

Mechanical:

- Visual inspection of PCB manufacture
  The visual inspection allowed the first check of the final assembly, helping reveal production issues.
- Weight
  It has been checked in order to validate the real weight of the PCBs and confirm the mass budget at system level.
- Dimensions and holes matrix
  Sizes and fixing holes have been verified to be compliant with the structure requirements and the tray's footprint.
- Components placing
  The disposition and connections of the electronic components on the boards have been verified in order to remove any schematic mistake.
- Connectors gender verification
  The connectors have been checked in order to allow and define the harness finalization with respect to the structure general definition.

Electrical, tests performed in the main bus voltage range: 18 to 25.2 V:

- Pin continuity and isolation
  All the physical output have been verified to avoid possible damages during the tests or future integration.
- Power consumption
  The power consumption has been estimated in order to confirm the power budget, essential for the mission operations to define the platform capabilities and then the payloads strategy.
- Output voltages and ripple
  The output power supplies of the PCB have been verified in order to be compliant with the system requirements and satisfy the design specifications.
- Over voltage protection (OVP)

The thresholds of the secondary power lines have been checked, discharging a voltage higher than the nominal on the proper test points to validate the circuit design and confirm the functionalities of the device.

- In-rush current

  The current absorbed by the load at first turn on, could be larger than the steady-state current value, typically due to capacitors on the input side. In order to prove the fully conformance of the devices with respect to the Power Unit Distribution the in-rush current have been verified.

Communications and IN/OUT

- Data output: CAN bus, RS485, RS233, RS422

  The communications properties have been checked measuring for each protocol or interface: Tbit, Voltage, Trise, Tfall.
- JTAG, microcontroller programming

  The logic unit have been programmed, through the provided JTAG port, in order to verify the proper behavior of the system and confirm the device implementation.
- High Priority Commands (HPC). The HPC are installed on the three main subsystems of the platform: TMTC (master), OBDH and PMU (slave), and has been tested to ensure the functionalities of the mechanism based on a pulse command interface.
- Custom interfaces, front-ends and drivers

  All the specific driver, interface or front-end has been tested and characterized to allow the proper modeling of the system and a functional verification.

All the tests listed above have been executed by two operators, the system designer and the quality manager, following a dedicated procedure reported in a specific document for each subsystem. The reports, one for each procedure, are to be found in a separated document.

The main results obtained in the previous tests show the full accomplishment of the communication links parameters, the driver’s functionality and the mechanical aspect of the boards. The power levels recorded for each unit, slightly different from the estimated during the design phase, allowed the balance of the power budget at system level, updating the confidence level associated to this parameters from 20% during design to 10% after tests, in accordance with ESA ECSS standards.

3.2 TEMPERATURE TEST

All the ESEO boards have been subjected to a temperature test thanks to the Climatic chamber installed in the ALMASpace Clean room. The machinery, showed in Figure 3.2, is developed to perform humidity and temperature test in a controlled environment. The subsystems passed several temperature cycle in the range of -20 to +70°C with constant relative humidity level, in order to confirm the fully functionality of the EUT and so validate the architecture and design in the temperature range estimated by the thermal analysis of the spacecraft. At both minimum and maximum temperature all the tests reported in paragraph 3.1 Power and electrical interfaces test, have been repeated showing the right behavior of the units in the estimated mission temperature range.

All the units successfully passed the tests.

Figure 3.2 Climatic chamber

3.3 RADIATIONS TEST

The core of every subsystem of the ESEO satellite is composed by a COTS microcontroller: the STMicroelectronics STM32F407. It’s an ARM M4 based cortex architecture, equipped with a variety of useful peripherals and available with industrial temperature range of -20 to +105 °C.

The microcontroller has high computational performance, it can reach the maximum clock of 168 MHz and integrates a Floating Point Units ensuring low power consumption. The device, produced for common industrial applications, during the mission will be exposed to ionizing radiations, high-energy protons, heavy ions and in general galactic cosmic rays, depending on the altitude and then from the atmosphere. The radiations levels have been simulated in the low earth orbit scenario to obtain useful parameters and range to be applied to the tests. In order to completely characterize the main processor in the space environment two different tests have been performed on several sample of the ARM microcontroller: Total Ionizing Dose exposure and Single Event Effects inspection, reported in the next paragraphs. Below a photo of the microcontroller decapsulated for the tests, it is possible to see the large memory area on the top of the Die.

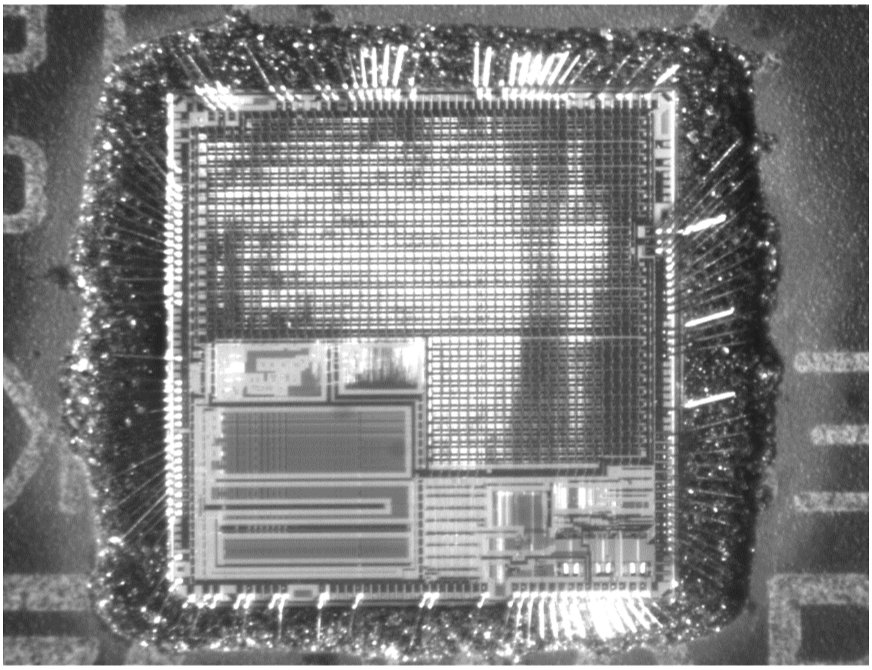


Figure 3.3 STM32F407 decapsulated

3.3.1 TOTAL IONIZING DOSE: T.I.D.

The test was aimed to verify the behavior of the EUT under a maximum radiation dose of 30 Krads , about 10 times the level expected for the whole mission. The test performed to identify the maximum radiation exposure allowable, have been developed in two phases, Irradiation and Annealing, in two different locations:

- Irradiation and electrical test between different dose rates were performed at the Calliope facility at ENEA Casaccia (Rome), Italy.
- Annealing (both T_{amb} and T=100°C) was performed at ALMASpace Clean Room.

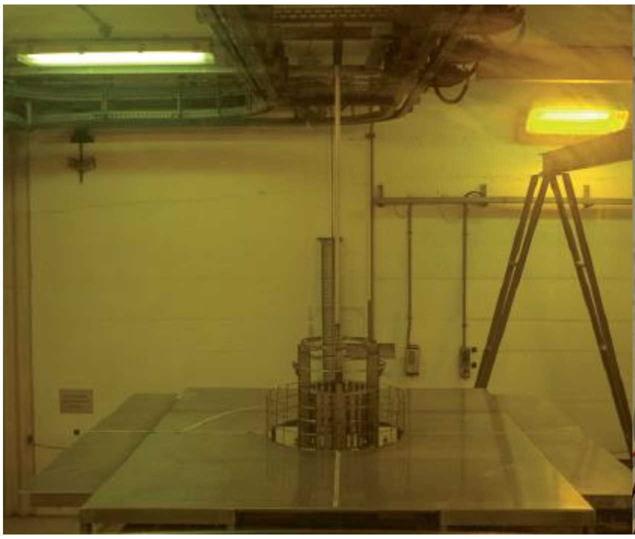


Figure 3.4: ENEA Calliope ^{60}CO source

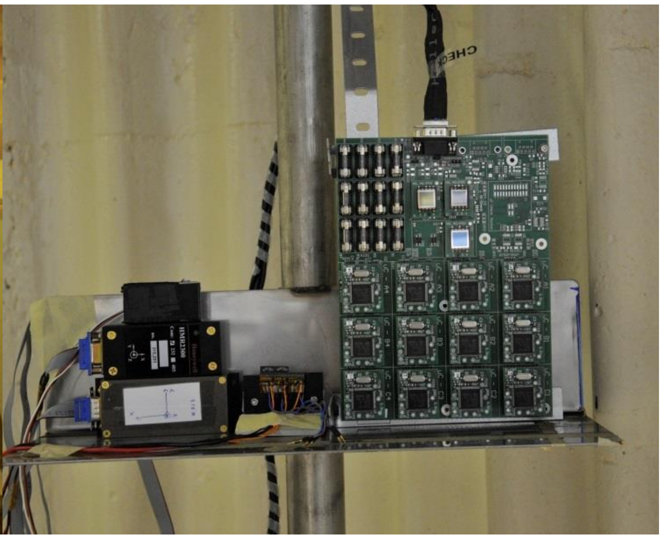


Figure 3.5: EUT inside the irradiation chamber

The “Calliope” irradiation facility at the ENEA Casaccia Research center uses Cobalt 60 for the test exposure, Figure 3.4. The radio isotopic ^{60}CO source has an actual nominal activity of about 0,34x10^{15} Bq. Dose rate is tuned by either placing the EUT, Figure 3.5, at the appropriate distance from the source or using radiation filtering devices. To neutralize the radiation source an automatic lifter was used to move the Cobalt bars in and out the pool, this took several minutes to be operated plus additional time to clean up the ionized air. Once completed the irradiation phase at ENEA laboratories the EUTs were moved back to ALMASpace premises to start the annealing process. Devices were biased for the first 168 hours at room temperature, about 20°C, and then after testing they were inserted inside the thermal chamber for the second part of the annealing at 100°C (biased).

Test have been considered successful having reached a test level of about 10 times the rate expected during nominal ESEO mission. All the devices survived the entire test campaign without showing evidence of malfunctions. In addition:

- All the Serial ports where correctly functioning at the end of the test campaign.
- All the Signal connected to S.P.I. interfaces where present.
- All the CAN ports where correctly functioning.
- It was possible to re-program all the devices.

All the collected data are presented in the proper report document.

The Figure 3.6 shows the total ionizing dose effect on the parameter distribution of a timer's frequency after each step for every sample.

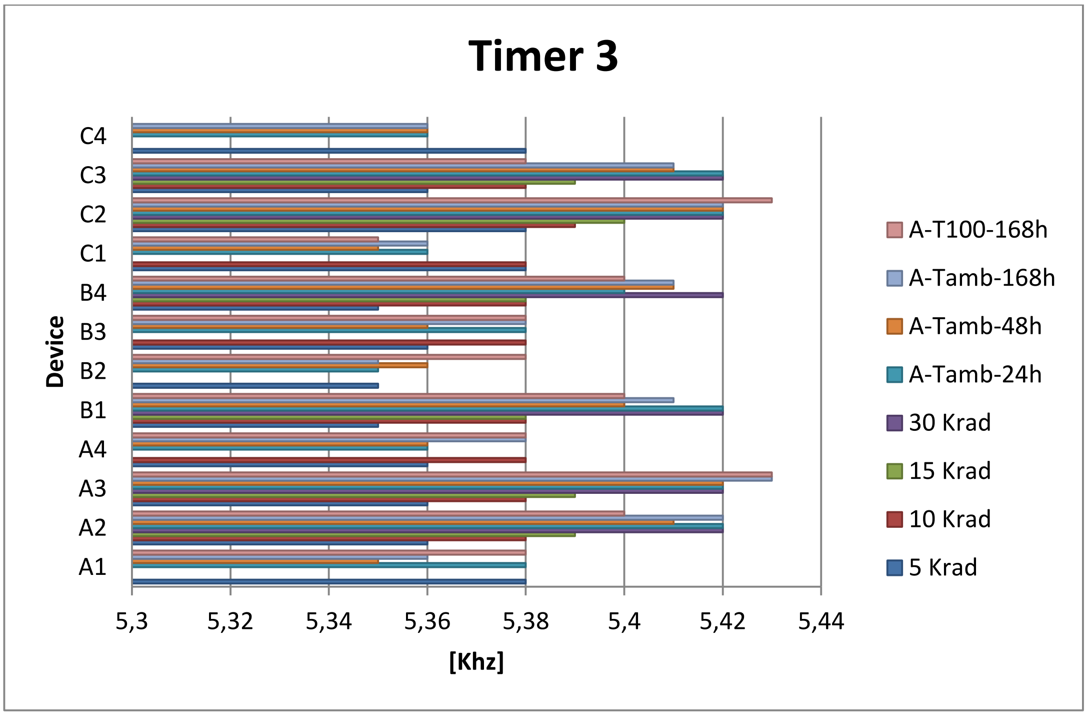
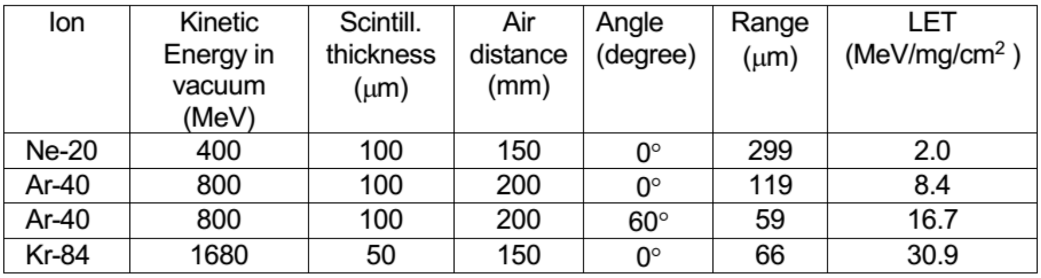


Figure 3.6: STM32F407 Timer 3

3.3.2 SINGLE EVENTS EFFECTS: S.E.E.

The test, performed with the help of MAPRad experts, was focused to monitor Single Event Latch-ups (SELs) and Single Event Functional Interrupts (SEFIs) sensitivity induced by heavy ions on the STM microcontroller. The electronic devices based on doped silicon junctions, if crossed from a heavy ion may trigger a short circuit between the metallization on the top layer of the silicon and its bulk, causing the destruction of the component unless it is not applied a rapid power supply cut off. The test has been executed at Laboratori Nazionali del SUD (LNS) of INFN (Istituto Nazionale di Fisica Nucleare), Catania. The LNS Superconducting Cyclotron (CS), Figure 3.7, used to collimate the ion beam on the Device Under Test (DUT), is a compact strong focusing three-sector machine with an operational range in the radio frequencies between 15 and 48 MHz and ion energies range between 8 and 100 A MeV. The maximum available energy is of 20 MeV/amu for the heaviest ions like $_{238}U_{38+}$, and 100 MeV/amu for fully stripped light ions. The irradiation hall called "Zero Degree" is the location where the radiation hardness studies took place. The beam has been extracted in air right in front of the dosimetry setup of MAPRad. To control and monitor the beam flux and determine the final fluence, a thin plastic scintillator (thickness of 50 or 100 μm) has been connected to a photomultiplier tube in order to detect the heavy ions and the scintillator kept on beam axis in order to monitor online the beam flux. A double-sided micro-strip silicon detector has been used to get the 3D profile of beam and a laser device has been used to measure the distances between DUT surface and beam exit with 200 μm position accuracy). The beam spot size tipically is 3x3 cm$_2$ and for special cases may be enlarged up to a diameter of 7 cm in vacuum. The spot homogeneity were within ±10%.

During this test Krypton, Argon and Neon ions have been used. The microcontrollers have been irradiated in air at normal direction (normal incidence, angle of 0°) and both normal and 60° for Argon. Table 3.1 summarize ion types used, the irradiation configuration and relative LET and Range determined with Geant (Version 4.9.3 Physic List ICRU73).



Ion	Kinetic Energy in vacuum (MeV)	Scintill. thickness (μm)	Air distance (mm)	Angle (degree)	Range (μm)	LET (MeV/mg/cm^2)
Ne-20	400	100	150	0°	299	2.0
Ar-40	800	100	200	0°	119	8.4
Ar-40	800	100	200	60°	59	16.7
Kr-84	1680	50	150	0°	66	30.9

Table 3.1 Ion species and characteristics

The test has been performed by exposing to heavy ions each DUT with an operating voltage of 3.3 V. The SEL has been monitored trough the SELDP, a test bench for the automatic detection and protection from SEL. In case of overcurrent the SELDP interrupts the DUT power supply and increments an internal counter. The time needed to interrupt the power is about 2 μs. After a programmable delay time the instrument restore the power to the DUT. Different trigger threshold for SEL has been set during the test (from 140 mA to 280 mA). SEU and SEFI have been monitored with continuous testing of the device through two loops. In the first loop the communications with all peripherals of interest is monitored, in the second loop write and read operations of the memory are implemented.

Irradiation started with Neon ion, followed by Argon (at 0 and 60 degrees), then with Krypton. Two samples have been used in this irradiation test, performed at constant ambient temperature of 23 °C. In Table 3.3 are showed the SEL Cross Section for the microcontroller while in Table 3.2 the sequence of test runs has been reported.

LET (MeV/mg/cm^2)	SEL CS Sample 1 (cm^2)	SEL CS Sample 2(cm^2)
2.0	1.0x10^{-7}	-
8.4	3.6x10^{-7}	1.4x10^{-7}
16.7	1.7x10^{-5}	6.6x10^{-5}
30.9	8.1x10^{-5}	-

Table 3.2 SEL Cross Section for STM32F407VG Microcontroller

Run	Sample	SEL Thres. (mA)	ION	Tilt(°)	LET (MeV/mg /cm2)	Range (μm)	Flux (ions/cm^2/ s)	Fluence (ions/cm2)	Dose (Krad)	Cum Dose (Krad)	SEL
1	S1	140	Ne-20	0	2.0	299	4.0x10^3	1.0x10^7	0.32	0.32	2
2	S1	280	Ne-20	0	2.0	299	2.0x10^3	1.0x10^7	0.32	0.64	1
3	S1	250	Ar-40	0	8.4	119	1.5x10^3	1.4x10^6	0.19	0.83	1
4	S1	250	Ar-40	0	8.4	119	4.0x10^3	3.4x10^6	0.46	1.29	1
5	S1	250	Ar-40	0	8.4	119	5.0x10^3	3.6x10^6	0.48	1.77	1
6	S1	250	Ar-40	60	16.7	59	1.0x10^3	405713	0.11	1.88	7
7	S1	250	Kr-84	0	30.9	66	0.5x10^3	122851	0.06	1.94	10
8	S2	250	Ar-40	0	8.4	119	6.0x10^3	3.9x10^6	0.52	0.52	0
9	S2	250	Ar-40	0	8.4	119	5.0x10^3	3.3x10^6	0.44	0.96	1
10	S2	250	Ar-40	60	16.7	59	1.0x10^3	152400	0.04	1.00	10

Table 3.3 Sequence of runs during heavy ion test

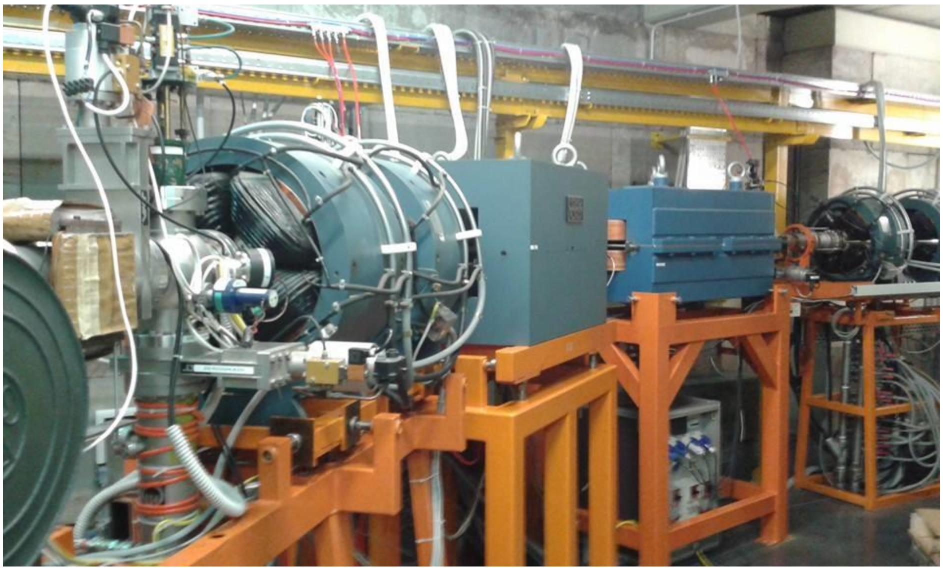


Figure 3.7 LNS Superconducting Cyclotron

Heavy ion test performed on STM32F407VG Microcontroller produced by ST Microelectronics shows, according to the collected data, that the component is not latch-up free even at low LET.

SEL events have been observed since from LET=2.0 MeV/(mg•cm_2) during Neon runs. Its SEL cross section is in the order of 10_{-7} (cm_2) at low LET<8.4 MeV/(mg•cm_2) increasing to 10_{-5}-10_{-4} (cm_2) at LET>16.7 MeV/(mg•cm_2).

3.4 VIBRATION TEST

A whole vibration test campaign have been planned for the ESEO platform: at system level, after the integration of the spacecraft, and at subsystem level, during the unit development. All the single units have been tested and the entire platform will be tested after the assembly and integrations phase starting now, early 2016 in accordance with the AI&V Plan (Assembly, Integration and Validation Document). The test has been performed with the Electro-Dynamic Shaker, Figure 3.8, of the SITAEL's facility located in Mola di Bari. The equipment under test were provided with accurate accelerometer sensors to analyze the feedback and record the data.

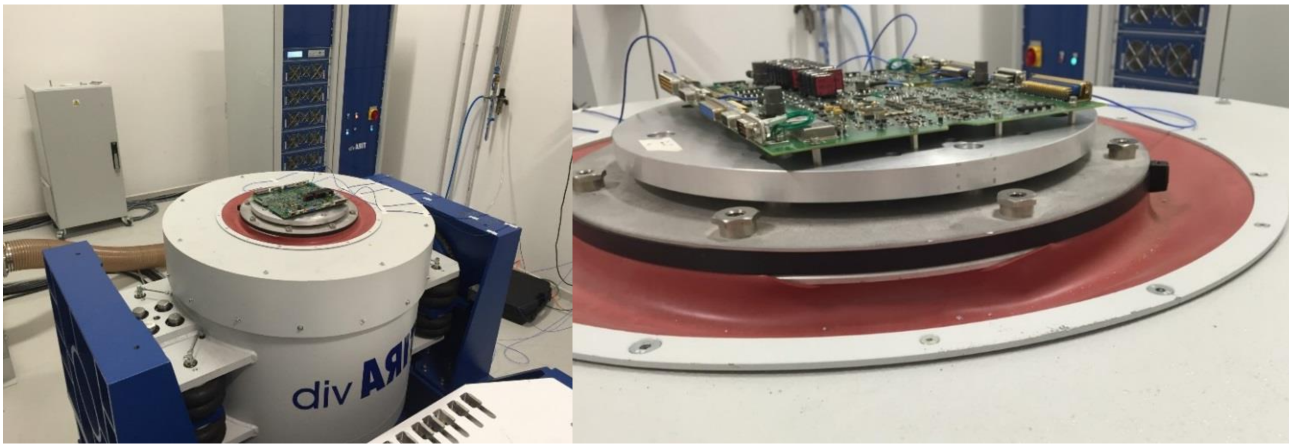


Figure 3.8 Electro-Dynamic Shaker

In reference to the system requirements, the vibration tests are pointed to satisfy a list of them to ensure the expected behavior, in particular in relation to the profiles imposed by the available launchers. The ESEO satellite and the subsystems shall operate nominally at the end of the vibration test campaign and no visible deformations or damages shall be noticed by visual inspection at the end.

In the following the main objectives are reported:

- The satellite platform shall be capable of operating during/after exposure to the range of environmental conditions expected during launch and nominal mission profile.

- The Structure shall be designed to ensure that the first significant satellite frequency is higher than 90 Hz in longitudinal direction and 45 Hz in lateral direction as per Launch Vehicle requirements.
- The structure shall withstand the mechanical loads which the satellite is subjected to during all mission phases including:
    - AIV and testing
    - Handling and ground operations
    - Launch phase
    - In orbit operations

All the boards, fixed as in the final flight configuration to the shaker, have been subjected to sine and random mode vibration on each axis in order to extract the resonation frequency of the EUT and demonstrate the compliance with the requirements. Low frequency longitudinal and lateral vibration environment spectra and high frequency random environment spectra applied:

LONGITUDINAL	
Frequency [Hz]	DLL [g]
4 – 10	**13.3 mm (0 - peak)**
10	**5.0**
100	**5.0**

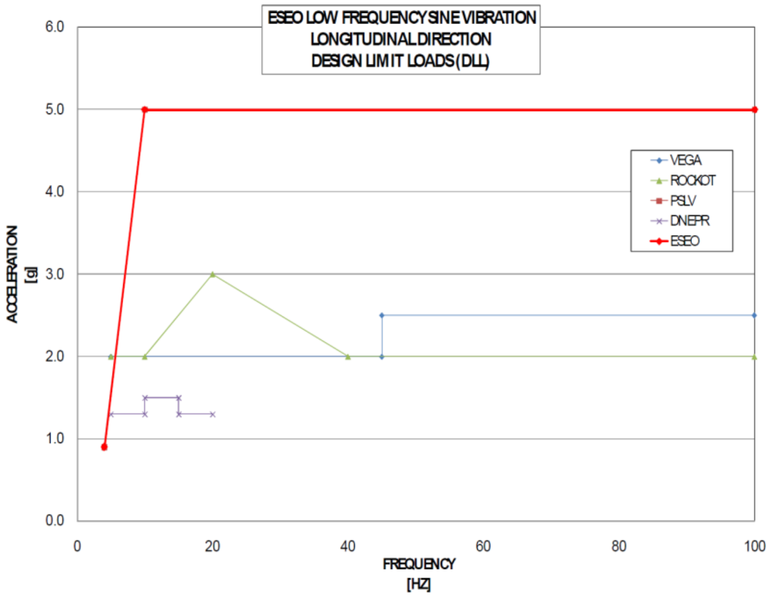


Figure 3.9 Low frequency longitudinal vibration environment spectra

LONGITUDINAL	
Frequency [Hz]	DLL PSD [g^2/Hz]
20	**0.014**
80	**0.014**
160	**0.044**
320	**0.07**
640	**0.07**
1280	**0.034**
2000	**0.01**
Overall g_{rms}	**8.88**

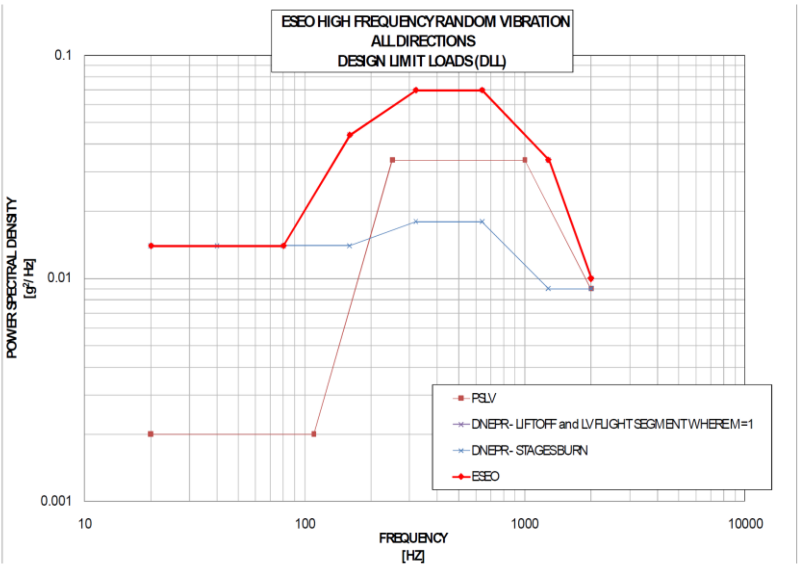


Figure 3.10 High frequency random environment spectra

In the following the results of the Micro-Propulsion System Tank test for the Z axis are reported as example:

- High-Level Sine Test

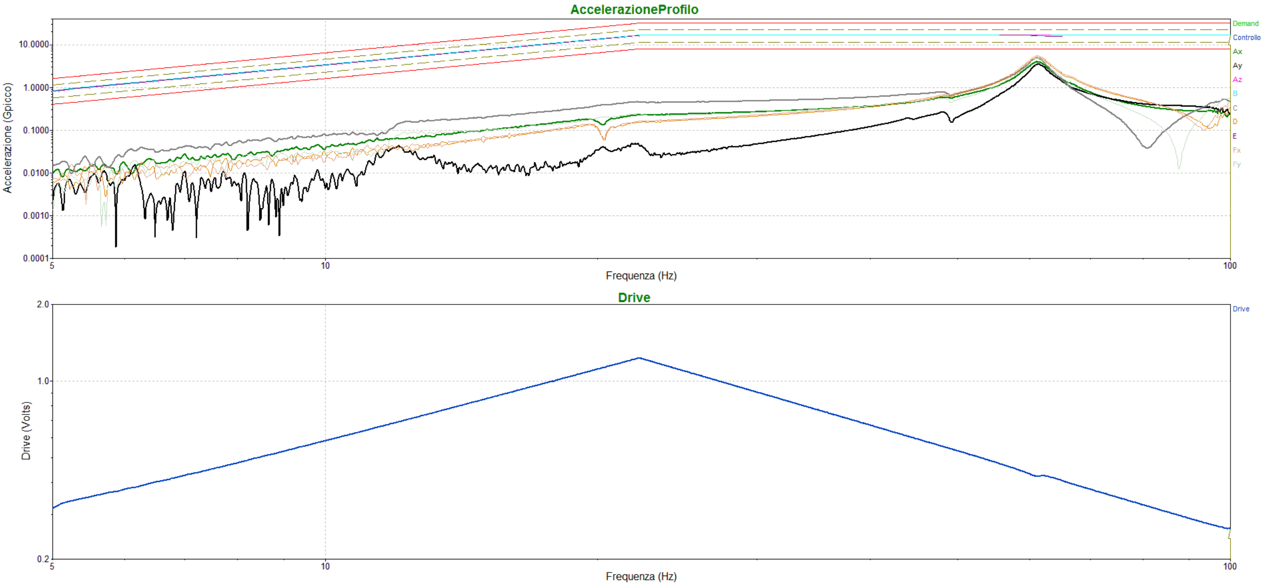


Figure 3.11: High Level sine results – Z axis MPS Tank

- Random vibration test

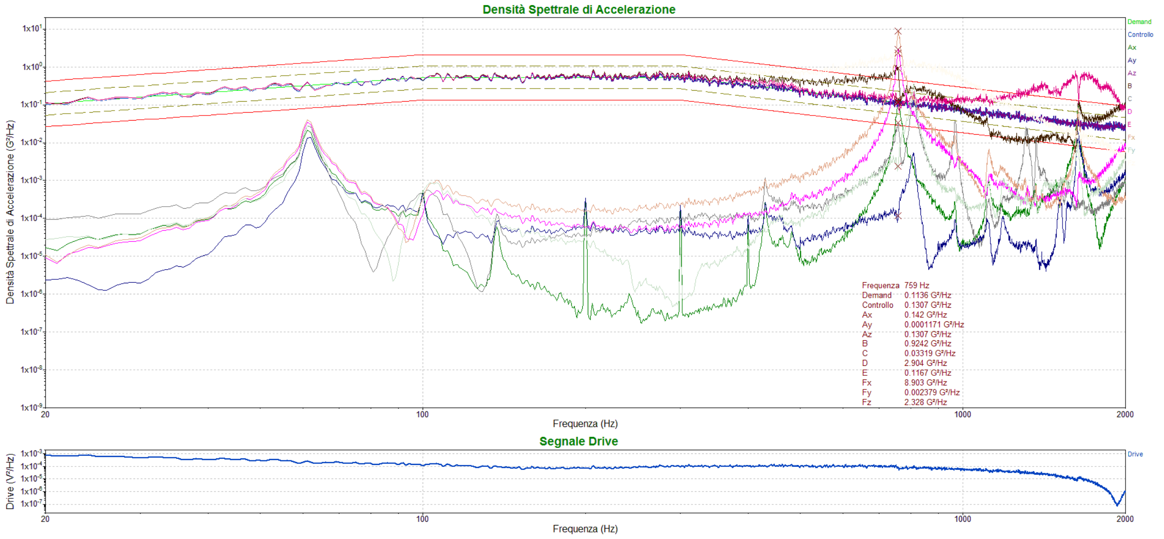


Figure 3.12: Random vibration results – Z axis MPS Tank

Like for every other test executed, the procedures reported in the paragraph: 3.1

Power and electrical interfaces, have been repeated to demonstrate the complete functionality of the units, each one overcoming the check successfully.

3.5 Thermo-vacuum test

A balance and thermal vacuum test campaign will be performed on the ESEO spacecraft assembly. It is aimed to demonstrate the lack of manufacturing and/or integration defects on the ESEO flight models. The EUT under test will be the complete ESEO spacecraft assembly, fully integrated. The integration phase will take place in the ALMASpace facilities while the tests will be performed thanks to ALTA Space[9] Thermo-Vacuum Chamber (TVC), in Pisa.

The ESEO satellite will be installed inside the TVC by means of a dedicated fixture, capable to thermally insulate the EUT from the internal plates of the test facilities. This is required in order to avoid unrealistic conductive path towards the TVC that could invalidate the results.

[9] ALTA Space: small space-oriented Italian company, acquired, like ALMASpace, by SITAEL during 2014-2015.

Two kind of tests will be performed on the ESEO spacecraft:

- Thermal balance, to validate the ESEO thermal numerical model in a mission-like operating environment;
- Thermal cycling, to provide evidence of the integrated system capability to withstand the expected thermal-mechanical stresses and to demonstrate the lack of manufacturing and/or integration defects on the ESEO FM.

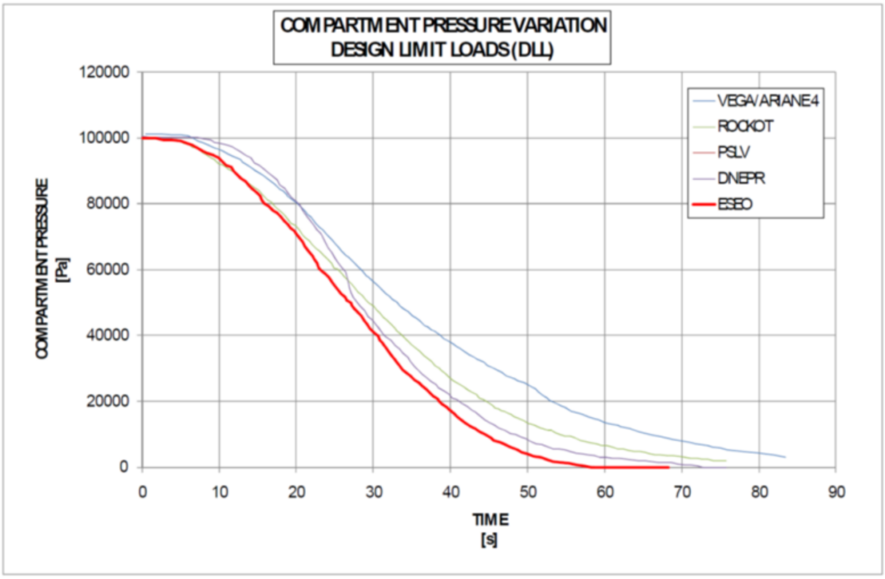


Figure 3.13 Pressure variation limit

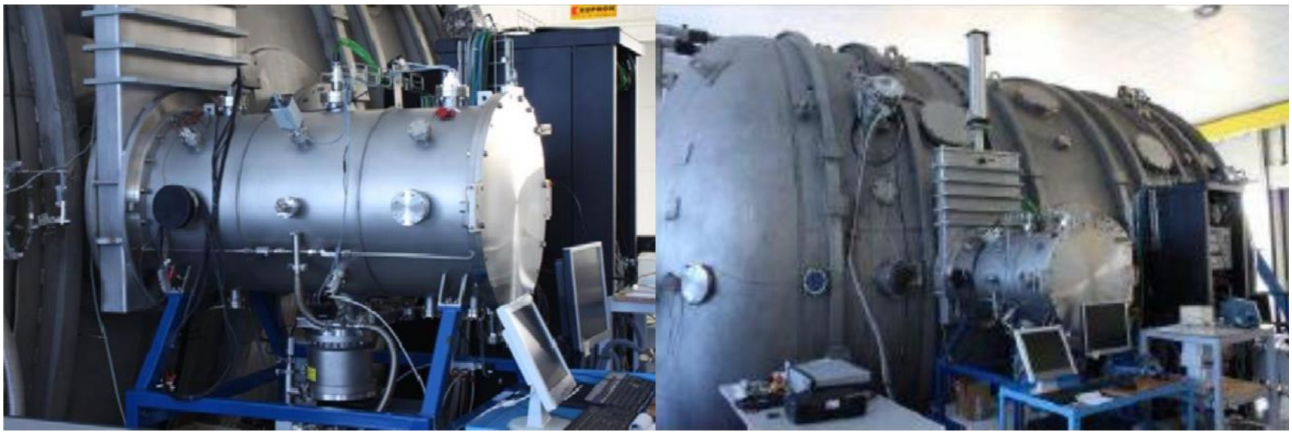


Figure 3.14 ALTA Thermo-Vacuum Chamber

Several points of the assembly will be monitored during the test in order to fully characterize the inspection:

- Externally: a set of thermocouples will be applied externally on the ESEO surfaces to monitor the operating condition of both the solar panel, the radiator panel and the accessible portions of structure.
- Internally: a set of temperatures will be monitored internally in the ESEO structure to check the operating conditions of the spacecraft.
- Built-in: many thermistors are included in the ESEO on-board avionic and will be monitored though the ESEO EGSE (Electrical Ground Support Equipment).

3.6 E.M.C. TEST

The EMC approach is pointed to ensure Inter-System and Intra- System compatibility of the Platform.

The set of requirements which must necessarily be met at Platform and Unit level are verified performing the following tests:

- Grounding, Bonding and Isolation: verified at any level (unit, subsystem, spacecraft)
- Conducted Emissions: verified at any level (unit, spacecraft)
- Conducted Susceptibility: verified at unit level and at spacecraft level.
- Radiated Emissions: verified at any unit level
- Radiated Susceptibility: verified at any unit level

The analysis is focused on:

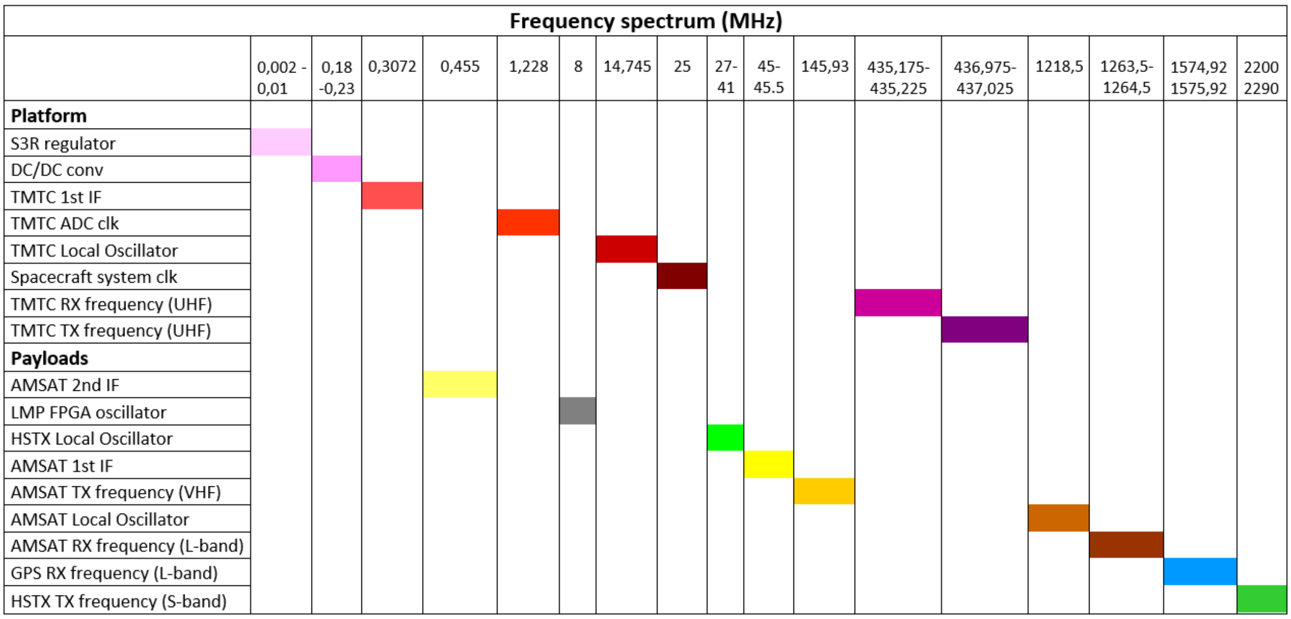
- Radiated compatibility between digital electronics and sensitive UHF receivers;
- Auto-compatibility of telecommunication payloads at transmit frequencies;
- Compatibility between the DC and AC low frequency magnetic field emitted by spacecraft equipment and magnetometer.

The devices representing critical areas are: UHF RF transceivers, AOCS actuators and magnetometers. MT could generate a residual magnetic field that could affect the measurement performed through the MM. This component of the AOCS system is very sensitive to variations of the magnetic field at DC and at low frequency, and the residual emission mask of the MT could overcome the low susceptibility mask of the MM. In order to synchronize the magnetometer acquisition and the magnetic-torquer actuation is necessary to turn off the magnetic-torquer dipole when the magnetometer acquisition occurs. To avoid interference, particular attention has been kept in the placement.

In addition, critical RF payloads such as AMSAT and S-band TX shall be compatible with the RS and CS threshold introduced by the platform critical areas.

In particular, margins are specified to be 20 dB for safety critical circuits and 6 dB for mission critical circuits.

- Susceptibility requirements are equal to the higher level susceptibility requirements.
- Emission take into account the summation of interference's of multiple instruments and other spacecraft systems.



	Frequency spectrum (MHz)																
	0,002 - 0,01	0,18 -0,23	0,3072	0,455	1,228	8	14,745	25	27-41	45-45.5	145,93	435,175-435,225	436,975-437,025	1218,5	1263,5-1264,5	1574,92 1575,92	2200 2290
Platform																	
S3R regulator	■																
DC/DC conv		■															
TMTC 1st IF			■														
TMTC ADC clk					■												
TMTC Local Oscillator							■										
Spacecraft system clk								■									
TMTC RX frequency (UHF)												■					
TMTC TX frequency (UHF)													■				
Payloads																	
AMSAT 2nd IF				■													
LMP FPGA oscillator						■											
HSTX Local Oscillator									■								
AMSAT 1st IF										■							
AMSAT TX frequency (VHF)											■						
AMSAT Local Oscillator														■			
AMSAT RX frequency (L-band)															■		
GPS RX frequency (L-band)																■	
HSTX TX frequency (S-band)																	■

The EMIC/EMI control activity is aimed to realize good performance of the spacecraft in terms of electromagnetic compatibility. The performance requirement is:

- A self-compatibility margin of at least 6 dB between the spacecraft RE and CE and the RS and CS thresholds (20 dB for pyrotechnic equipment);
- A RF compatibility with the launcher and launch pad ground systems in terms of radiated emission and radiated susceptibility;
- A RF self-compatibility between the payload and the other subsystems.

The EMC/EMI Control Program includes application of design rules, EMC analysis and Tests.

The analyses to be carried out to demonstrate the nominal performance of the S/C are:

- assessment of the spacecraft electromagnetic environment and the associated safety margins;
- self and launcher compatibility analysis;

- definition of spacecraft grounding scheme.

The EMC Tests consist in a verification of the qualification status versus the requirements. In case the qualification of a unit is not achieved, the activity shall consists in an analysis of the test results for acceptability or further additional test request or hardware modifications.

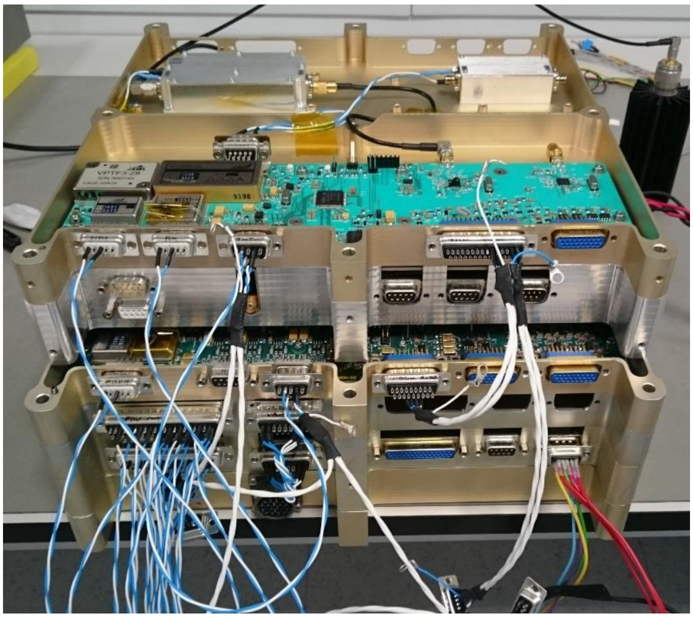


Figure 3.15 ESEO bus, EMC test

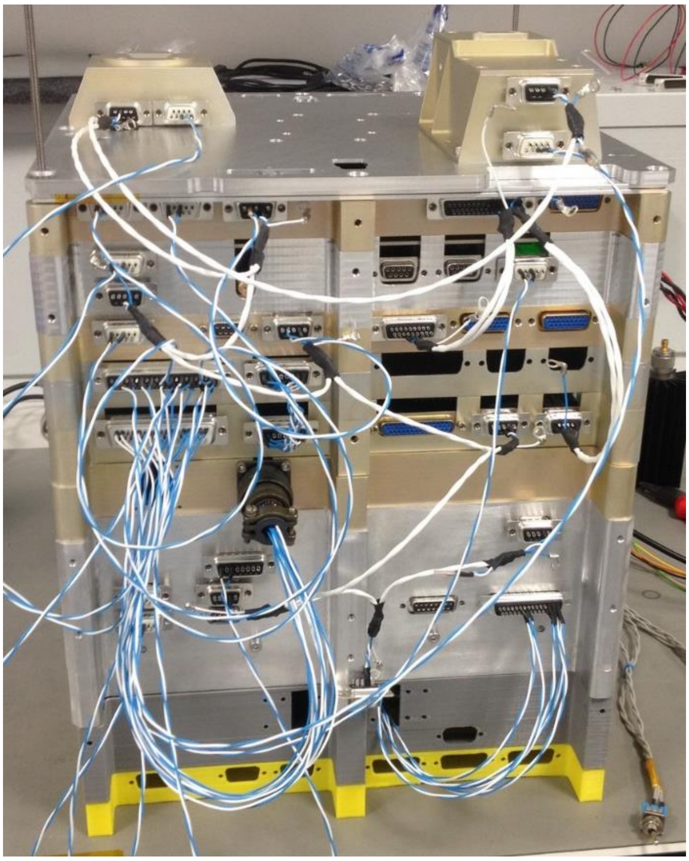


Figure 3.16 ESEO bus integrated

4 F.D.I.R. (Fault Detection Isolation and Recovery)

The ESEO FDIR operations are divided in three main sections: the platform, the ACS and the units FDIR. The first is related to the essential subsystems, the TMTC, the OBDH, the PS and the CAN bus. The second is related to AOCS redundant equipment, the magnetometers, the magnetic coils, etc. and the third pertain the unit's functionalities and communication monitoring.

This FDIR strategies refers to the ESEO Block Diagram reported in paragraph 2.2.2 Architecture.

The ESEO FDIR is based on two main concepts:

- Hierarchical failure detection
- Decentralized detection

The hierarchical failure detection:

It is based on a three-level hierarchy, allowing categorizing each S/C failure depending on the way it is monitored and detected.

The various failures are split over various levels, depending on the way they are detected on board:

In the following, when not specific statement is made, the term SW refers to any S/C Software: TMTC SW (System FDIR task), OBDH SW (ACS FDIR task), or to all the ESEO embedded Software (units FDIR)

- *Built-in monitoring:*

This is the only failure level directly processed on-board.

Level 0: failure associated to an internal single failure in one equipment or subsystem unit which can be automatically recovered by the units itself. See paragraph 4.1 Level 0: Built-in.

- *Hardware monitoring:*

The monitoring performed by the Hardware is by nature SW independent and is based on protections mechanisms such as: over voltage protection (OVP), under voltage protection (UVP), over current protection (OCP), R-LCL/LCL (latch current protection, retriggerable and not) embedded on each subsystem, as well as a watch-dog timer implemented on every microcontroller on-board.

Level 1: failures of the units monitored by a dedicated HW protection or mechanism on-board are described in paragraph 4.2 Level 1: Hardware.

- *Software monitoring:*

The monitoring performed by the Software covers different types of failures and is achieved by mean of an ACK based communication protocol and acquisition of critical parameters, HK and TM data analysis executed on board or from ground.

Level 2: failure associated to a system performance anomaly related to satellite vital function, e.g. ACS, Power managing or distribution, communications.

	Failure Detection Level	**Failed Unit and Function**	**Detection/Isolation Principle**
Built-in	*0*	ALL Memory storage and management.	Built in detection and recovery (fault masking, EDAC)
HW Detection	*1*	ALL Failures of microcontroller's processes. Critical power issues (over-current, over-voltage).	Watch-Dog Timer. Embedded HW protections (OVP, OCP, UVP, LCL/R-LCL).
SW Detection	*2*	ALL Vital S/C functions. Communications failures. Failures of AOCS sensors and actuators.	Communication protocol based on acknowledge mechanism. Acquisition of health status and critical parameters (TM, HK on-board or ground analysis). Function performance monitoring.

Figure 4.1 Failure detection hierarchy

The decentralized detection

As said before all the ESEO systems (main units and subsystems) are provided with a level 0 and level 1 failure detection and or isolation mechanism. Each system integrate also an embedded software capable to recognize failures at different levels according to the hardware hierarchy and the architecture of the satellite.

From the perspective of the operational safety and reliability of the system, the Software integrated on board of the units is basically structured in three layers: system vital functions and communications, ACS operations and units malfunctioning referred to as: Platform FDIR, ACS/OBDH FDIR and Unit FDIR.

In the table below the detection level hierarchy and distribution is summarized:

Failure Detection Level	Type	Detection mechanism	System	Location	Link
Level 0	Built-in	EDAC	All	Integrated on-board	CAN
Level 1	HW monitoring /isolation	WD Timer	All	Integrated on-board/ ext. HW	CAN
		OCP	All	On-board HW	PWR/CAN
		OVP	All	On-board HW	PWR/CAN
		LCL/R-LCL	All	HW (PDU)	PWR/CAN
Level 2	SW monitoring	Platform FDIR	TMTC,OBDH,PMU	TMTC SW Task	CAN, RS422
		AOCS FDIR	MM,MT,ES,SS,MW	OBDH SW Task	CAN, RS485
		Unit FDIR	MM,MT,ES,SS,MW	On-board SW	CAN
		P/L FDIR	P/L	On-board SW	P/L CAN

Table 4.1 hierarchy and distribution

Principle of failure Isolation and Recovery

The failure Isolation allows avoiding failure propagation to the system. On ESEO, this is a partly decentralized function, if the failure is detected at unit level and a quick reaction time is needed, (ex: major power issue, processor stuck, SEL, SEFI) then the unit (or the subsystem it belongs to) performs the failure isolation by itself, leaving the next operation's control to the higher system in the hierarchy, except for the TMTC, the highest level in the FDIR architecture. Otherwise, the failure isolation is performed by the referred SW, most of the time by switching off the failed unit or by performing a transition to Safe mode.

The failure Recovery_allows to continue nominal operations. This function is performed either autonomously on-board or by ground control, depending on the kind of failure and on the Satellite current mode.

Autonomous Recovery

To ensure the reliability of the link with the ground segment under any operational conditions, the TMTC system is always capable to perform the necessary recovery actions. The system, composed by two identical units in hot redundancy, continuously execute a health check of himself through the Platform FDIR task. The two boards are monitored by mean of an Acknowledge mechanism over the CAN bus.

In normal mode (mode 4: nominal operation during Sun or Eclipse), the OBDH system through the ACS-FDIR task is capable to isolate a failed equipment and recovery the function switching to the redounded unit autonomously after the first failure. After a prefixed number of failed attempts to restore the faulty drive this is turned off. The redundant unit is activated and the new configuration of the system is reported and stored in the HK of the OBDH.

The failure management of the CAN bus communications are autonomously recovered and partially decentralized. During nominal operation the CAN bus master node periodically sends an Heartbeat message on the active CAN bus. Each powered unit receives and elaborate the message. In absence of errors and failures no reply is produced. In case of failure of the active CAN bus, or heartbeat not received, the unit reply with an Heartbeat message on the redundant CAN bus in order to allow the master node to switch from the failed CAN bus to the redundant one.

Ground Recovery

In case of major failures detected at Platform FDIR level or failures that lead to safe modes, the S/C recovery is performed under ground control.

4.1 LEVEL 0: BUILT-IN

This failure level is directly processed on-board or within a firmware-integrated mechanism between the units without affecting other system functionalities.

- EDAC (Error Detection And Correction), implemented to supervise Flash and RAM memories. For instance: single bit flips (SEU) in Flash memory are autonomously corrected by the EDAC mechanism.

As already mentioned, software EDAC helps to mitigate the effect of SEU on the processor SRAM memory. The EDAC is implemented as triple redundancy of a subset of SRAM variables. Types and methods are used to facilitate code implementation, to write and read the variables protected by EDAC. At read time, the method checks for validity of the data, and signal a flag if an error is detected. New types are essentially based on structure of three variables of same general type (char, int, float or double). The EDAC component is basically a collection of utilities and type definitions which can be used by the application to protect the declared variables from single event caused by the radiation. If a variable requires to be protected, it is declared using one of the specific basic type definitions: char_edac, int_edac, long_int_edac, float_edac, double_edac. The EDAC variable is implemented as a structure containing three copies of the same quantity. When the application software requires to operate on such variable the two methods are provided: read_edac which compares the three copies in a voting procedure, providing a single result and eventually signaling errors and write_edac which writes the result of operation in the EDAC protected variable.

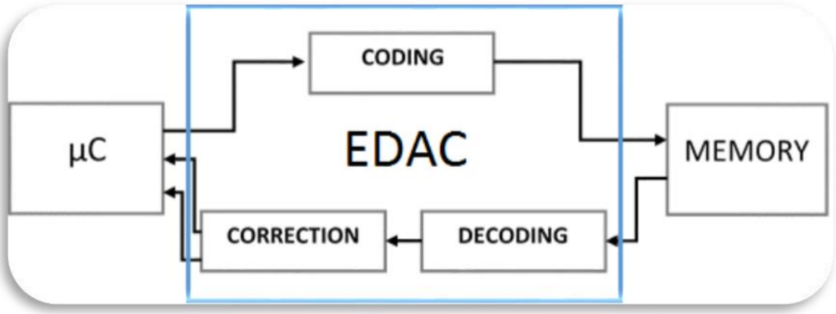


Figure 4.2 EDAC mechanism

- CRC (Cyclic Redundancy Check) implemented in the communication protocols.

Is an error-detecting code used to detect accidental changes to raw data. The data packets is processed by the mechanism and added with the polynomial division result of its contents. On the receiver side, the calculation is repeated and the results checked. In case of values not matching, a packet re-transfer is required due to data corruption. The name CRC is due to the computation algorithm, based on cyclic codes; easy to analyze, and useful to detect errors caused by noise in transmission channels.

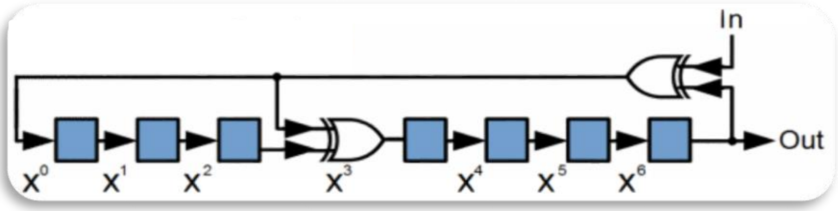


Figure 4.3 Generic CRC Byte generation

4.2 Level 1: Hardware

The failures detected at level 1, HW monitored, are mainly referred to power issues or data-processing failures of the units such as microcontroller stuck or in dead loop.

This covers the following types of failures:

- WDT: Failures of the microcontroller, internal process stuck or dead loops caused by SEFI or any other failure involving the processing unit are monitored by a watchdog timer.

Each unit is equipped with an integrated watch-dog embedded in the microcontroller except for the TMTC system, endowed also with an external HW WD timer in order to improve the reliability of the architecture and assure a safe mechanism for the power managing and the failure detection between the two hot redounded units.

The external WD time of the TMTC is ten times bigger than the internal WD timer, in order to allow at least ten attempts of restart for the µC. After ten consecutive failures, the TMTC main is considered corrupted and the external WDT will be activated; the WD trigger the inhibit pin of the DC/DC converter and switches off the whole board. The architecture of the double WD timer is due to the necessity of a self-switch off procedure on the TMTC unit. In case of adoption of the single internal WDT the activation of the WD will cause the switch off of the µC itself and the inhibition signal will not be activated anymore. With the introduction of an external WDT, supplied by an indipendent regulator with respect to the DC/DC converter, the inhibition signal will remain active after the DC/DC converter switch off. Then the OVP/OCP latch get discharged in order to allow the re-use of the TMTC unit if the error condition has been solved

- OCP: Failures that lead to an over-current absorption of the microcontroller or any other integrated circuit on-board are monitored and isolated by mean of an over-current protection circuit (OCP) on the secondary of the DC/DCs.

Short-circuits at component level and single events latch-up (SEL) are managed directly on-board. The setting of the thresholds levels of the devices are fixed and estimated by tests in nominal operation mode. This protection is embedded on all the systems of the platform and repeated on every different power lines defined in the subsystem architecture, in order to ensure a better identification of a possible failure, rise the reliability of the internal power distribution and also to permit a fine-set of the thresholds. This circuit has been introduced at CDR stage and implemented due to FMEA analysis and the radiation test campaign performed. It has been developed with the supervision of ESA experts, simulated and tested in the expected temperature range.

- OVP: Failures inducing an over-voltage at the secondary stage of the DC/DCs are detected and isolated on-board by an over-voltage protection (OVP) that disable the power supply of the unit acting on the latch embedded on board, as well as the Over Current Protection.

The voltage monitor is based on Zener diode. When the secondary voltage exceeds the Zener voltage threshold the latch is triggered and the DC-DC inhibited. The threshold voltages are sized specifically for each power line and related to the unit design.

Once the overvoltage latch is triggered, it is not released until a power cut of the power supply. This operation is performed by the TMTC with the pulse command interface to the OBDH and PMU or through a power cycle, acting on the PDU’s LCLs, on the other units.

Since TMTC and OBDH are considered essential loads, power supply to these units is always guaranteed by R-LCL on the PDU. Therefore it is not possible to reset the protections through LCL. In the specific case of TMTC and OBDH, the reset of OVP or OCP involves the procedures reported in the following figures at platform SW level.

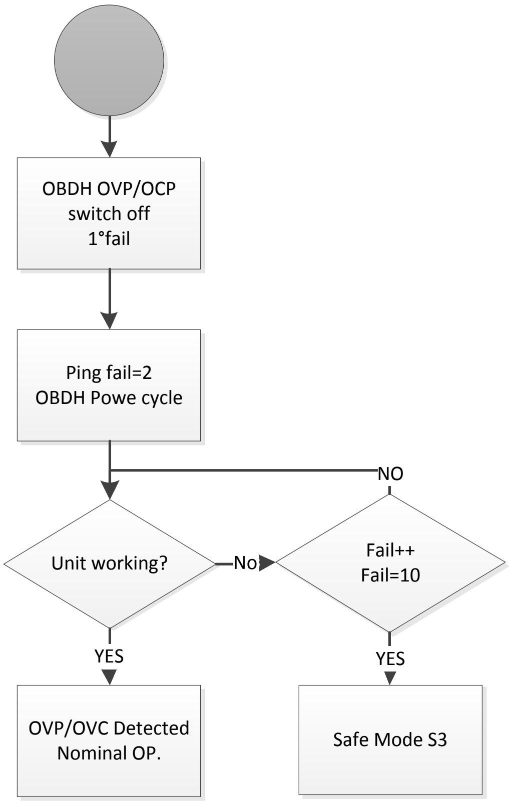


Figure 4.4 OBDH OVP/OCP reset

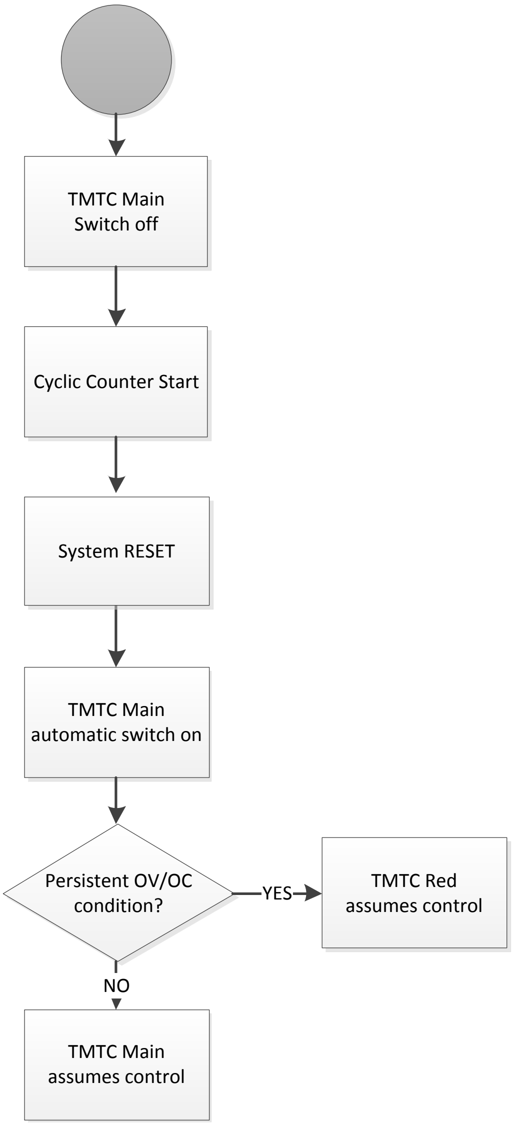


Figure 4.5 TMTC OVP/OCP reset

Post-processing of HK on-ground is necessary in order to verify the conditions for a safe re-activation of the failed unit.

- LCL, R-LCL: Failure involving an over-current absorption at the primary stage of the DC/DC of each unit are detected by use of latch current limiters (LCL).

This protections are integrated on the power distribution unit (PDU) and are divided in two categories. LCLs, ESA qualified, are implemented for all the subsystems except for the critical systems: TMTC and OBDH, provided with a re-triggerable LCL (R-LCL) to ensure the proper power supply. The Latching Current Limiter are separated in three categories depending on the current absorption of the specific load which are connected to. The categories are: 0.25A, 0.5A and 1.2A.

R-LCLs are based on rad-hard integrated current limiters operating in re-triggerable mode. The maximum current of the R-LCLs, the trip-off time and the recovery time is configured by external components. The R-LCLs are configured ON at power up, and can provide analogue telemetry of the current and status information.

In the next table are summarized the current and the shedding classes implemented on the Power Distribution Unit.

Subsystem or Payload name		Current class		Shedding class	
Main	Red.	Main	Red.	Main	Red.
OBDH_M	OBDH_R	0.25	0.25	-	-
RX_M	RX_R	0.5	0.5	-	-
TX_M	TX_R	1.2	1.2	S4	S4
SS_M	SS_R	0.25	0.25	S3	S3
MM_M	MM_R	0.25	0.25	S2	S2
MW_M	MW_R	1.2	1.2	S2	S2
MT_M	MT_R	0.25	0.25	S3	S3
MPS	ES	0.5	0.5	S2	S2
TRITEL	uCAM	0.5	0.5	S1	S1
HSTX	AMSAT	1.2	1.2	S1	S1
GPS	LMP	0.25	0.25	S1	S1
Spare_1.2	Spare_1.2	1.2	1.2	S1	S1
Spare_0.5	Spare_0.5	0.5	0.5	S1	S1
Spare_0.25	Spare_0.25	0.25	0.25	S1	S1
Fire and Select	Fire and Select	1.2	1.2	S2	S2

Table 4.2 PDU, current and shedding class

4.3 LEVEL 2: SOFTWARE

4.3.1 PLATFORM FDIR

The TMTC unit is in charge to perform the Platform FDIR task. This system is the first in in the communication chain with the ground segment and the Platform FDIR is responsible for the satellite vital functions monitoring. Moreover it is appointed for the control of the communications on the CAN bus, the management of the high priority commands (HPC) and pyro functions and it is also intended for the reprogramming of the OBDH firmware.

The Platform FDIR strategy is basically a software state-machine executed by the proper FDIR task at the end of each system cycle, 1 second. This is the last task scheduled by the RTOS in order to perform the required operations by other routines and then check the results.

General description:

- TMTC, OBDH and PMU failure management

The platform FDIR managed by the TMTC subsystem implements a mechanism based on request of acknowledge ACK from the TMTC main to TMTC redundant, to OBDH main and PS main. If the answer is not received, after a pre-defined number of attempts, the TMTC assumes device malfunctioning and switches to the redundant. Note that for the case of TMTC redundant which is in hot redundancy, it is its responsibility to take control of operations if it does not receive ACK request from TMTC main. The ACK mechanism is performed through the system CAN bus developed upon the CAN Open protocol. The CAN SW stack is completely managed by dedicated routine on board of the units. It is implemented by means of HW and SW operations on the CAN internal peripheral of the microcontroller and is supervised by a Watch-Dog timer, as well as every microcontroller's task or routine.

When the OBDH main permanently fails for any reason, not responding to ACK requests, TMTC takes control of the platform, and switches to safe mode S3, where one or both of the OBDH can be reprogrammed, see diagram in Figure 4.14. In this situation, OBDH failed, the TMTC directly generates telemetry beacons. The Power System instead is directly switched by the TMTC in case of failure. The mechanism is described in the following figures and diagrams.

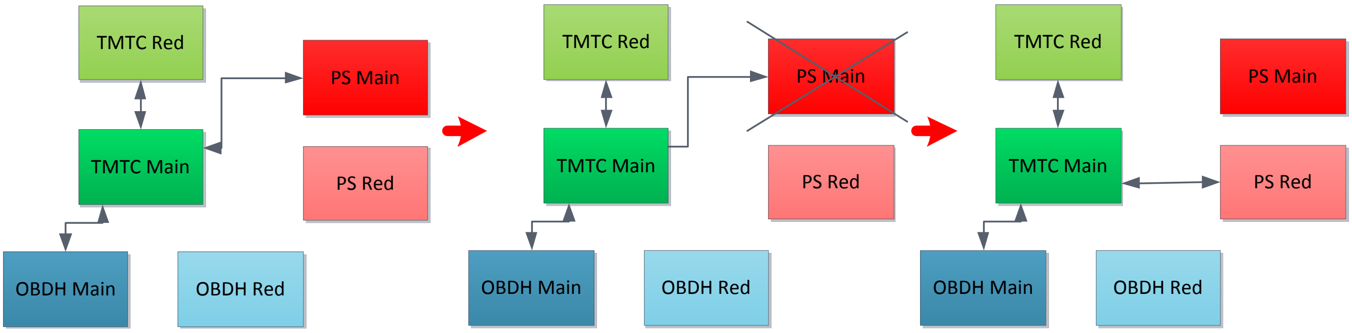


Figure 4.6 ACK requests and switch to redundant, for OBDH and PS

Implementation

The sequence of operations, detailed for the TMTC main and redundant unit, is described in the next section and is based on the mission timeline reported in Chapter: 2.2.1 Spacecraft modes.

In the first diagram, Figure 4.7, is described the phase M0, suddenly after the separation. The FDIR task immediately starts the prefixed controls. This phase is related to the spacecraft initialization and will never be reached again by the platform. A second identical condition, without an active OBDH, will lead the platform in safe mode S3. After the first stage the system enter in M1: OBDH power on, similar to the previous but in this case the TMTC is in charge to turn on the On-Board Computer starting the actions that will lead to nominal operations.

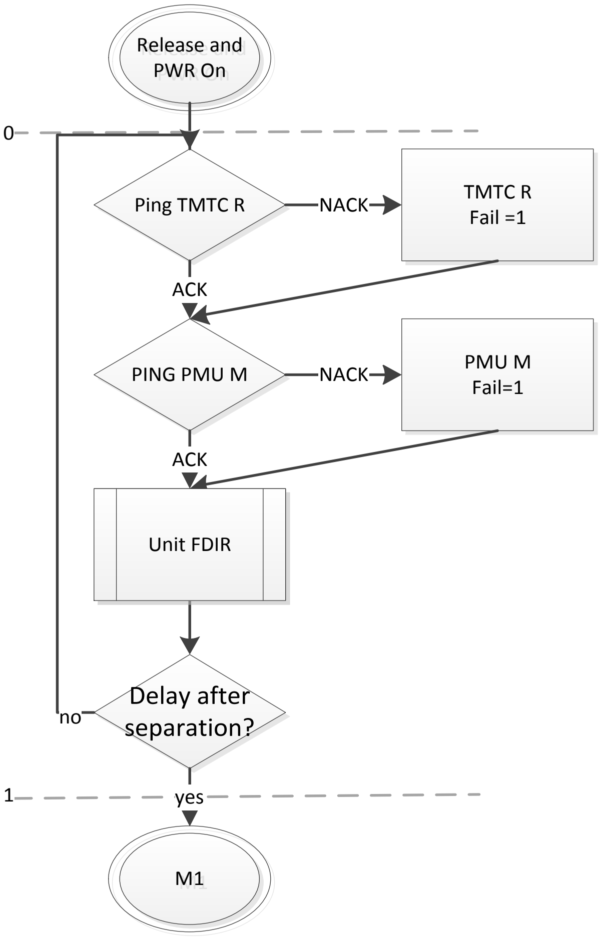


Figure 4.7 TMTC main FDIR operations diagram, phase M0

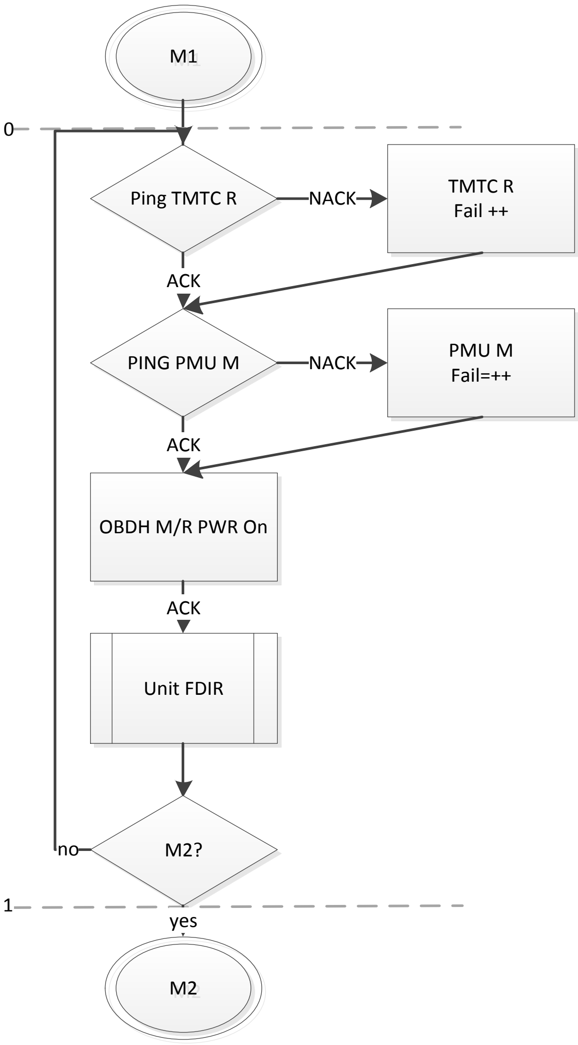


Figure 4.8 TMTC main FDIR operations diagram, phase M1

The following diagram describe in detail the M2 mode for the TMTC main unit. It represents the nominal operations of the system and explain also the failure's treatment. The failure management is highlighted for re-try numbers greater than one in order to show the complete behavior of the strategy.

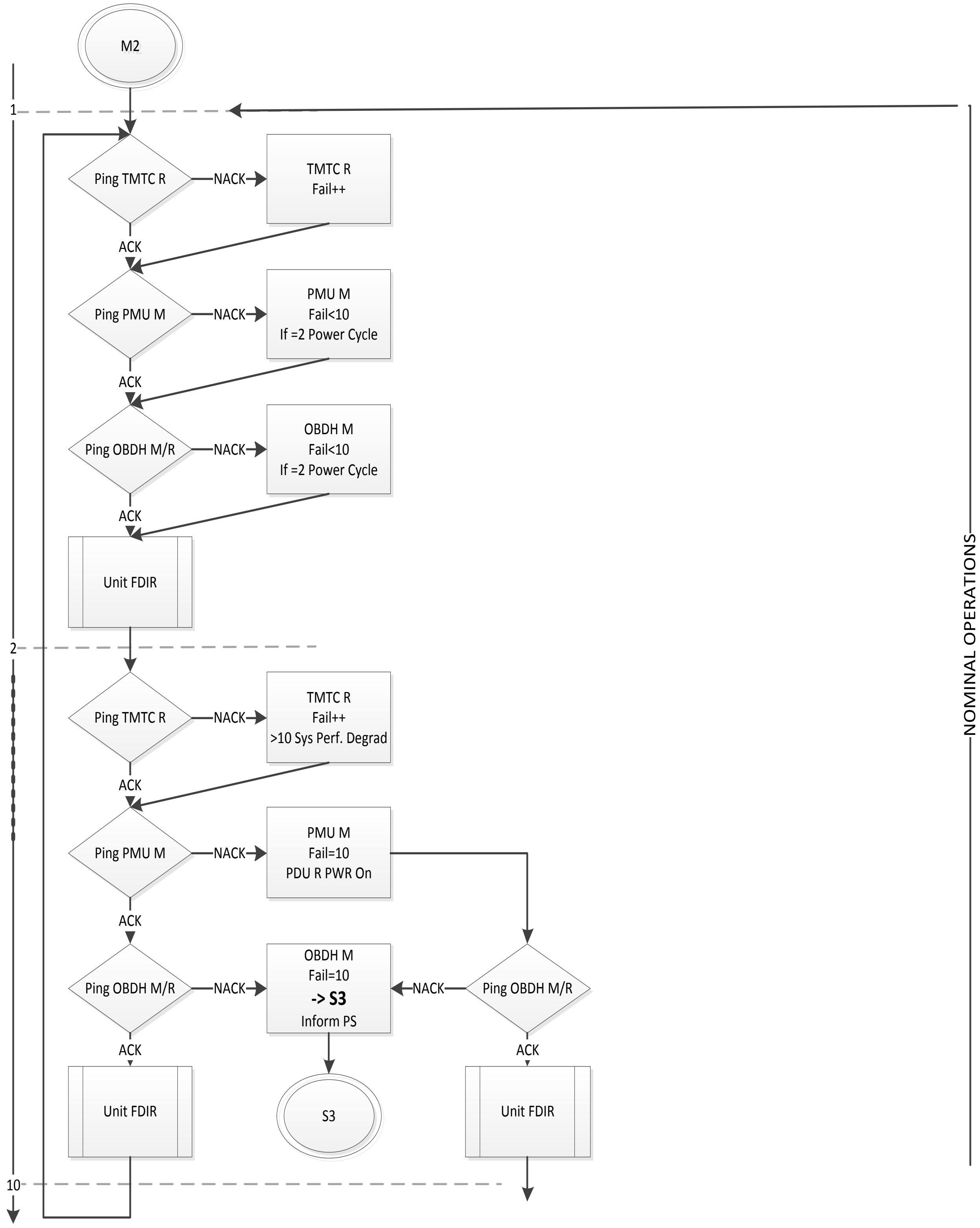


Figure 4.9 TMTC main operations, phase M2-1

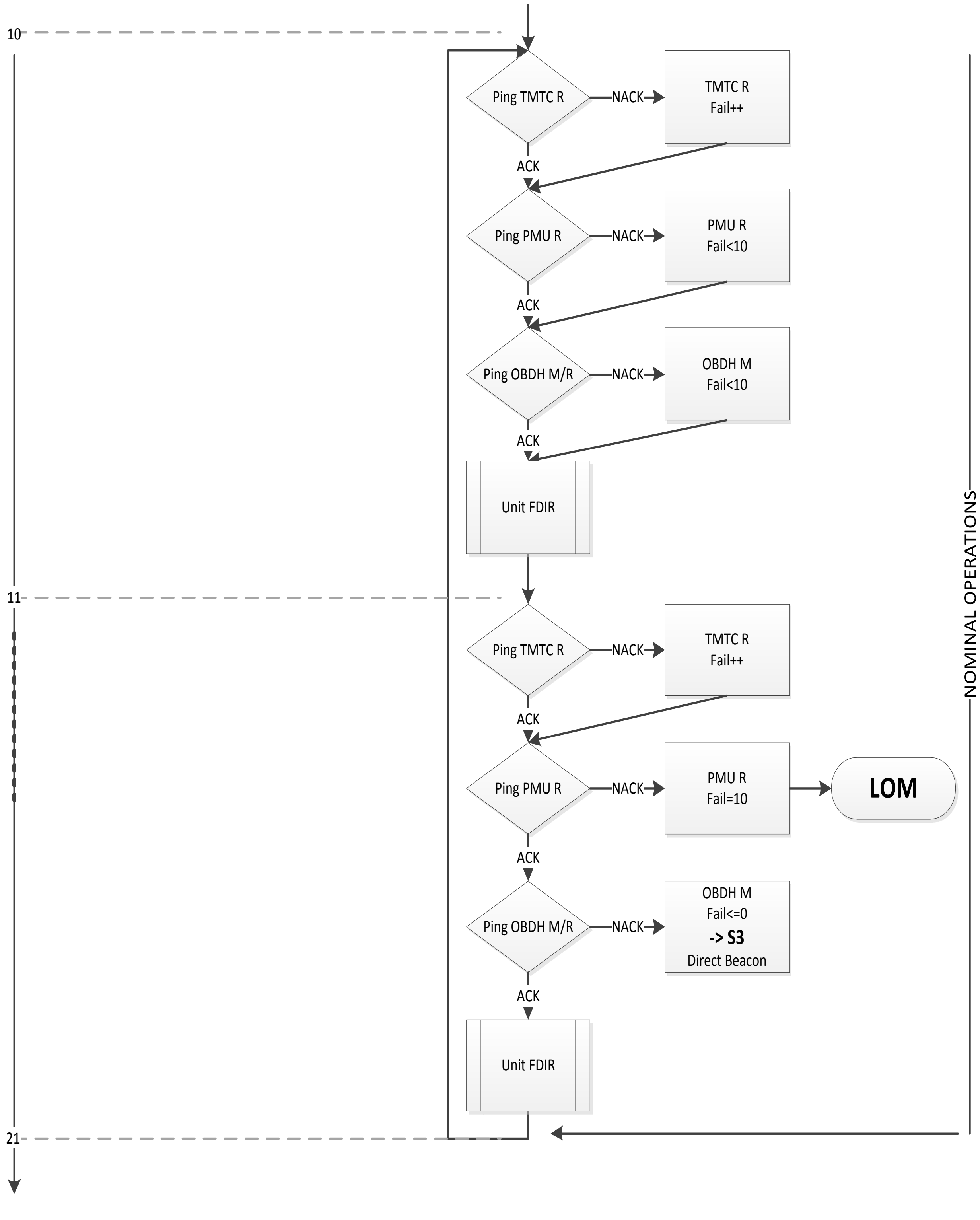


Figure 4.10 TMTC main FDIR operations, phase M2-2

The procedures have been detailed down to the final branch in order to identify all the possible causes and conditions leading to the loss of mission (LOM).

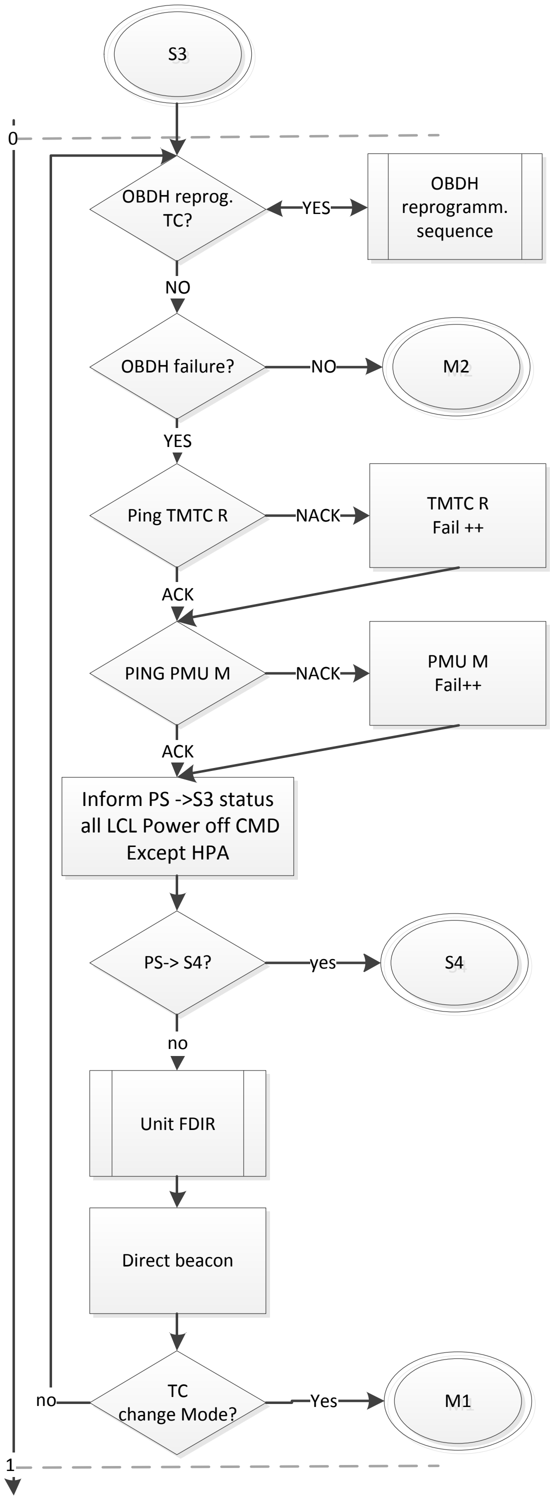


Figure 4.11 TMTC main FDIR operations, safe mode S3

As mentioned before, the TMTC system is in charge to manage the platform in case of failed OBDH, in the previous diagram, Figure 4.11, the procedures performed by the system are explained for the safe mode S3. Because the same safe mode could be reached also due to main bus power down, it is possible to call this mode even by the OBDH, thanks to the PS telemetry. In this situation the communication system will act transparently, performing the nominal operations detailed in mode M2.

Different considerations have been made on the safe mode S4, reported in Figure 4.12. In this system state, reached exclusively due to a critical power down condition on the main bus, the platform is silent. All the LCLs of the PDU are turned off, including the Hi Power Amplifier (HPA) power supply link and the beacon generation is inhibited. Like for the others safe modes, a ground Telecommand is required in order to exit the state and change configuration. The only possible mode after S4 is S3 in order to keep the platform in a known set-up right after the telecommunication recovery. In case of OBDH active, once again, the TMTC system is transparent and keep performing its nominal operation. The up-link is inhibited directly by the On-Board Computer.

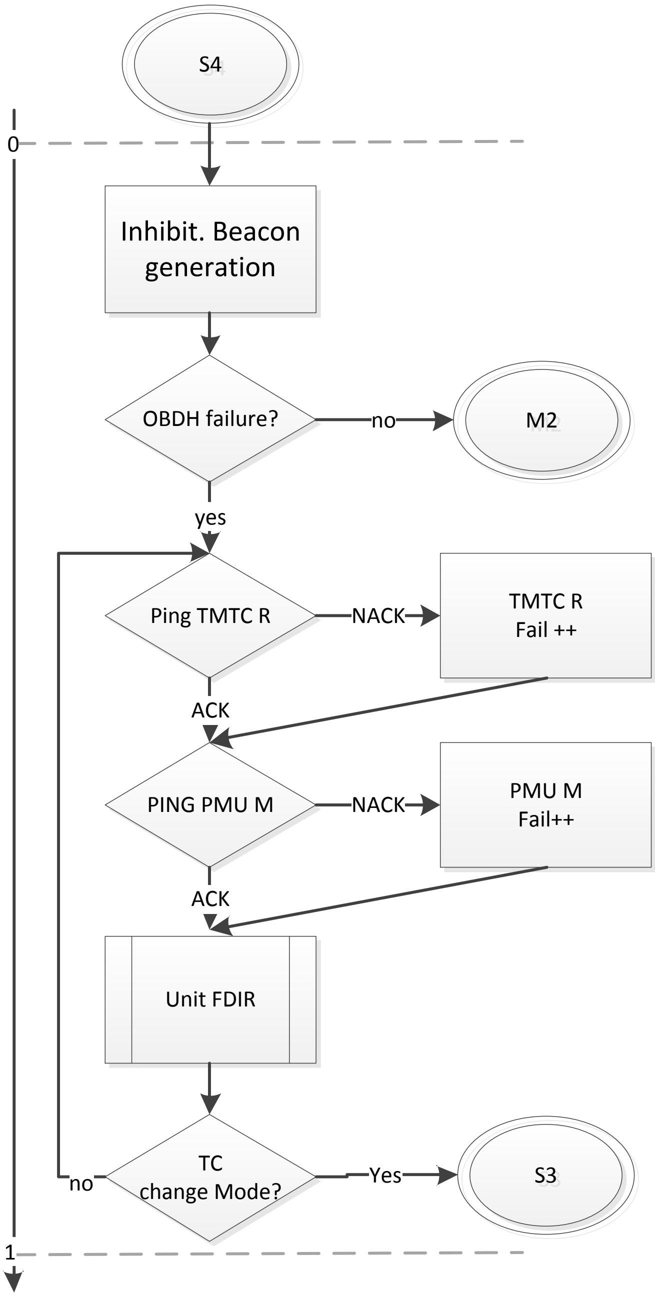


Figure 4.12 TMTC main operations, safe mode S4

As already introduced since TMTC main and redundant are in hot configuration, it is responsibility of TMTC redundant to detect failures of the main unit. Therefore its sequence of operation is different, and described by the following diagram.

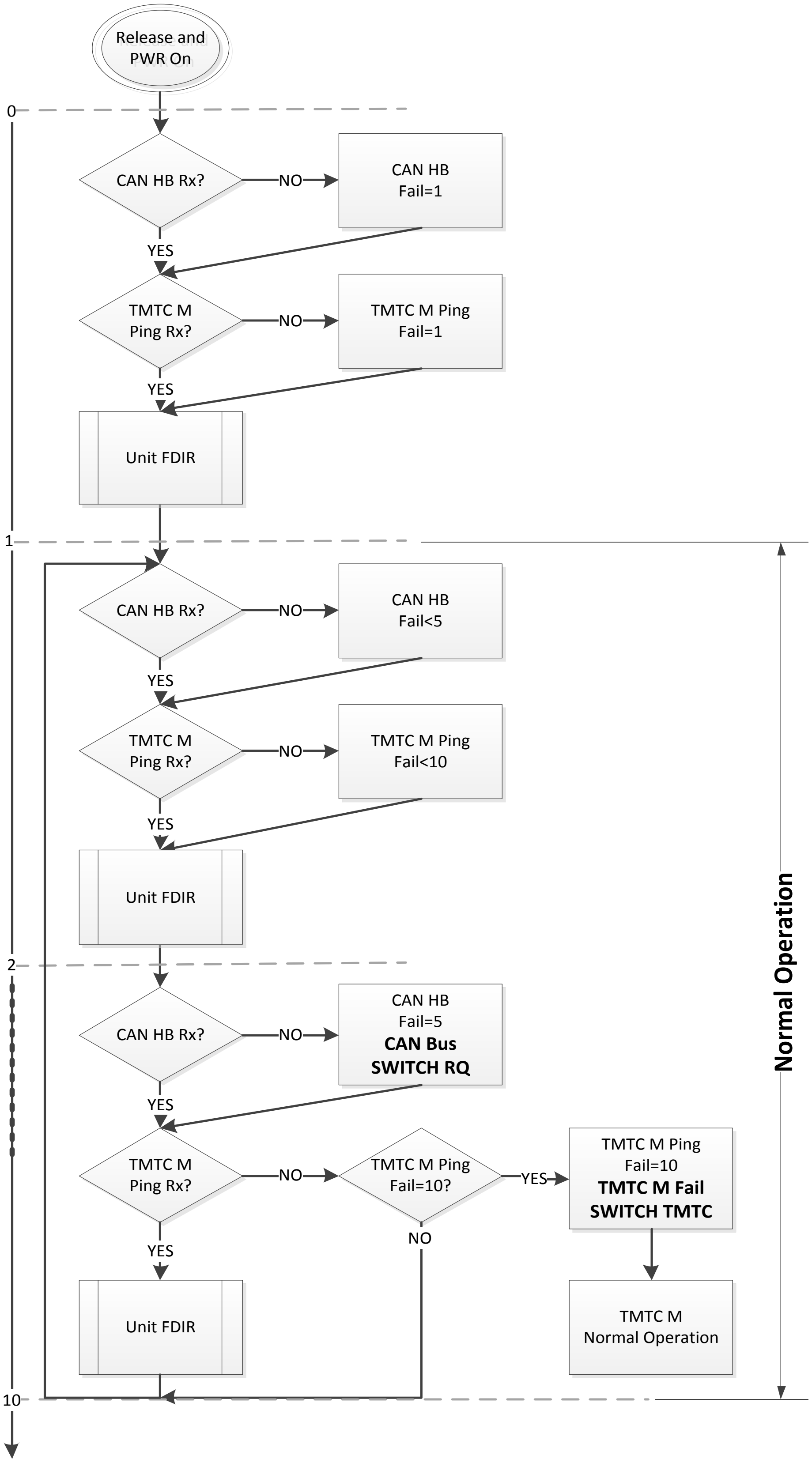


Figure 4.13 TMTC redundant FDIR operations diagram

The main TMTC is also responsible of the identification of active CAN bus. In case of failure of the main TMTC this role is taken by the redundant. The mechanism to identify active CAN bus makes use of a CAN-Open protocol service called *Heartbeat*. It is essentially based on a periodic broadcast of a message on the bus marked as active. The equipment/subsystem expects to receive the message. If they don't, they start to communicate on the redundant bus signaling to the heartbeat producer that the main bus is corrupted. Then, the TMTC starts producing heartbeats on the redundant CAN bus, signaling to every equipment/subsystem that it is the bus to use for communications.

- OBDH reprogramming

The OBDH reprogramming functionality is available in safe mode S3 only, which can be reached because of:

- Critical power down of the main bus
- A dedicated TC sent from ground
- OBDH failure

In the first two cases we assume that the OBDH is active, either the main or the redundant. In the last case, the OBDH units is not working properly. When in safe mode S3, the reprogramming sequence is triggered by a dedicated HPC (High Priority Command), and the operations are executed according to the diagram in Figure 4.14.

The diagram assumes that the software is already stored in TMTC external flash memory. At the beginning of the mission, the memory stores the software version already programmed in the OBDH, so reprogramming attempt may be performed without having to transfer new code.

It is also possible to send to the TMTC a new software from the ground segment, in order to upgrade the OBDH firmware or fix any further issues detected by processing the data received from ground. This is also a powerful tool to re-configure the platform in orbit, in the case of new developments of FDIR control methods and/or equipment management.

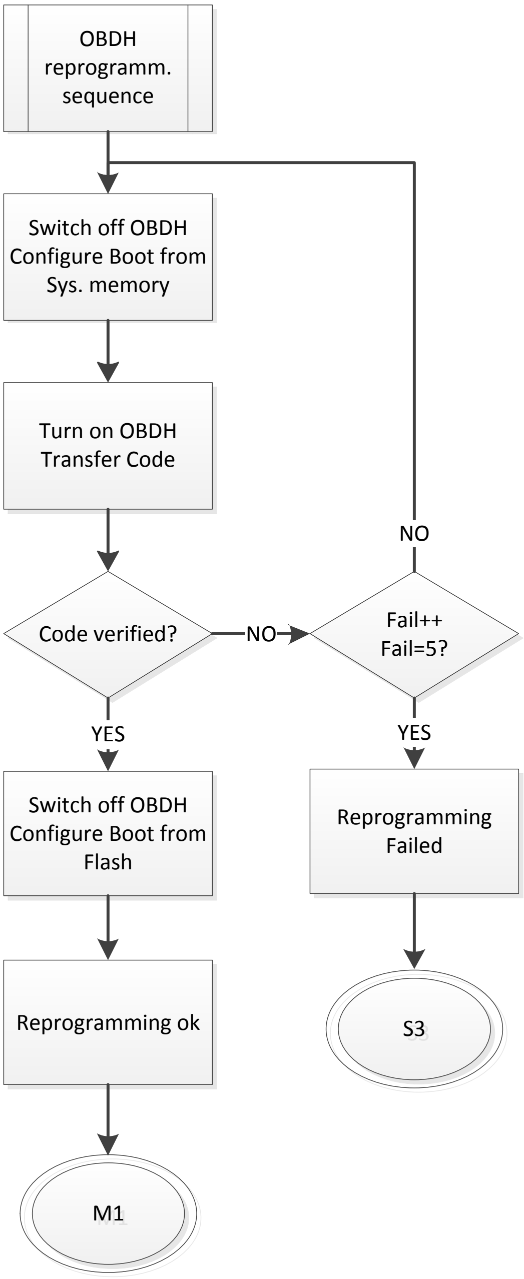

OBDH reprogramm. sequence
Switch off OBDH Configure Boot from Sys. memory
Turn on OBDH Transfer Code
Code verified?
NO
Fail++ Fail=5?
NO
YES
YES
Switch off OBDH Configure Boot from Flash
Reprogramming Failed
Reprogramming ok
S3
M1

Figure 4.14 TMTC: OBDH reprogramming sequence

4.3.2 ACS/OBDH FDIR

The AOCS FDIR task is embedded in the OBDH software. It is aimed to supervise the ACS operations, control and manage the main and redounded equipment in case of failure. The

OBDH FDIR is also in charge to supervise the Power System and TMTC housekeeping in order to generate alarms and switch the platform in the S/C safe modes reported in chapter 2.2.1.

The FDIR functionality implemented in the AOCS system manage all the sensors and actuators in order to select the suitable configuration to achieve the mission purposes. Each actuator includes a fault detection routine in the internal SW, described in chapter 4.3.3. Moreover a warning packet is sent to the main AOCS unit in order to perform the recovery action foreseen by the FDIR routine.

The system automatically select the best configuration of the actuators:

- If a failure occurs on the magnetic torquers switch the control to the backup unit
- If a failure occurs on the MW set the S/C in S3 mode.
- If a failure occurs on the magnetometer immediately switch to the redounded unit
- If a failure occurs on a digital Sun Sensor unit the FDIR functionality isolate the failed sensor signaling a performance degradation.

If necessary it is possible to use also the coarse sun sensor in order to obtain roughly the sun direction during a failure on a sun sensor.

When a failure occurs, the main recovery action performed by the AOCS FDIR routine is the hard reset of the faulted peripherals.

The OBDH application software (ASW) collects the HK data from the on-board active equipment. The list of the HK data collected, here omitted, are reported in the proper document: ESEO TMHK protocol. All the equipment includes a dedicated variable to specify an error or a warning condition. The OBDH ASW verify the received data and generate errors and warning flags for a finite number of equipment or collects the flag generated directly from the equipment. In the following the error and warning flags are specified for each equipment.

Equipment	Errors and warning flag generated by (OBDH/Equipment)	Ref. HK data
OBDH	OBDH ASW	OBD_TEMP_ERROR
AOCS	OBDH ASW	ACS_ERR
PMM	OBDH ASW	PMM_ERROR_1 PMM_ERROR_2
PMR	OBDH ASW	PMR_ERROR_1 PMR_ERROR_2
TTM	OBDH ASW	TTM_ERROR
TTR	OBDH ASW	TTR_ERROR
SSM	Equipment	SSM_ERROR
SSR	Equipment	SSR_ERROR
ESE	Equipment	ESE_ERROR
MWR	Equipment	MWR_FAULT
MWM*	Equipment	MWM_STATUS
MPS	OBDH ASW (TBC)	MPS_ERROR
MMM	OBDH ASW	MMM_ERROR
MMR	OBDH ASW	MMR_ERROR
MTM	OBDH ASW	MTM_ERROR
MTR	OBDH ASW	MTR_ERROR

***the warning flag of the MWM is provided by means of the RS422 communication link.**

Figure 4.15 Error flags

The detailed steps performed by the ACS FDIR are reported in the next figures: ACS FDIR-1 and 2. In order to manage properly each equipment, the strategies applied are slightly different, according to the system requirements and the device priority in the control chain. For instance the magnetometer, needed with high availability by the attitude and control routine, is immediately switched in order to receive the next data set as soon as possible and ensure low error on the propagator. A hard fault on the momentum wheel is managed switching the whole platform in safe mode S2, similar to M3: De-Tumbling, in which the attitude control is performed only through the magnetic actuators and sensors. Other failures on the equipment mainly lead to degraded mission performance thanks to the ACS's algorithm capability to ensure the system control even with faulty secondary units, such as Earth Sensor and Sun Sensors.

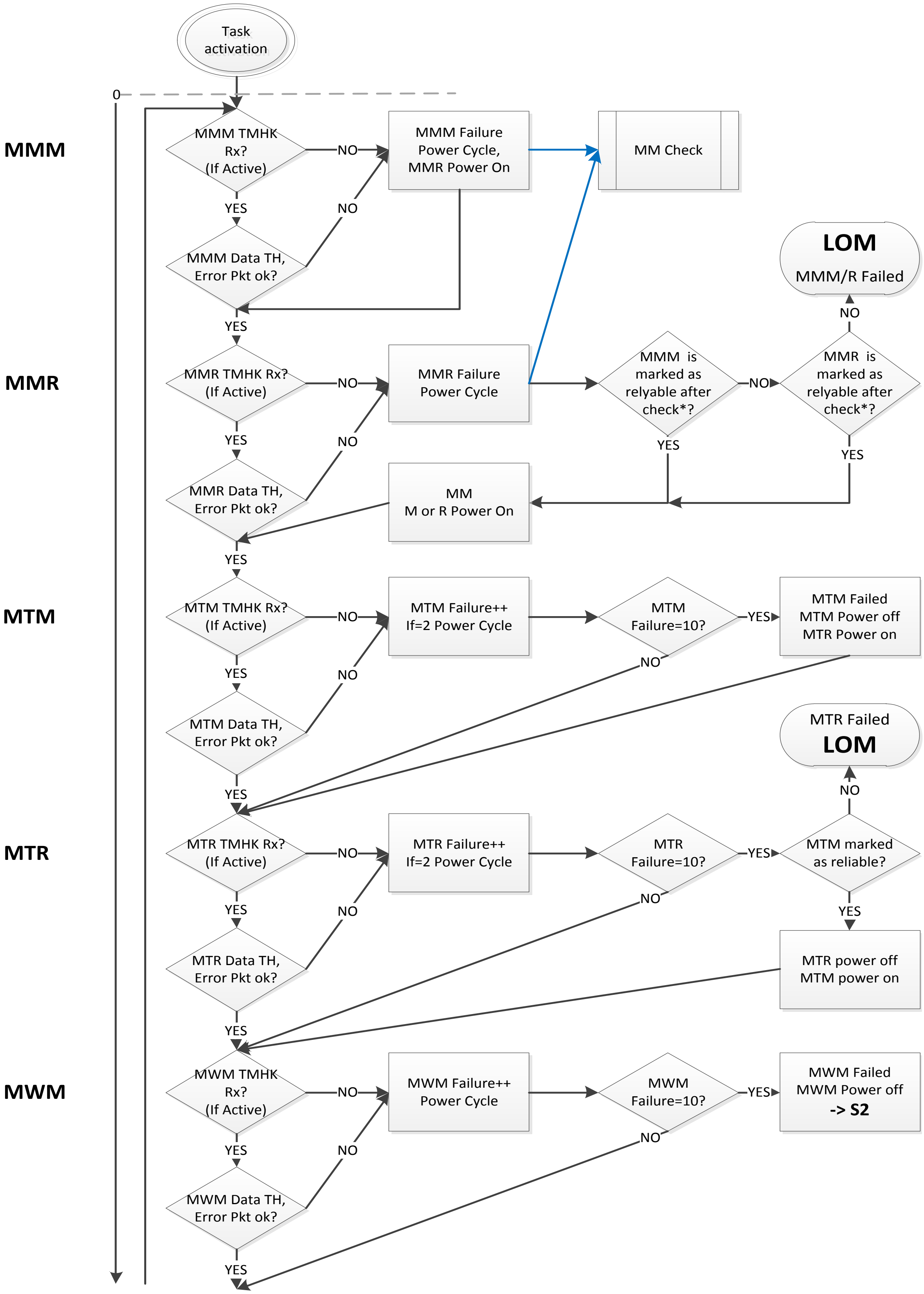


Figure 4.16 ACS FDIR-1

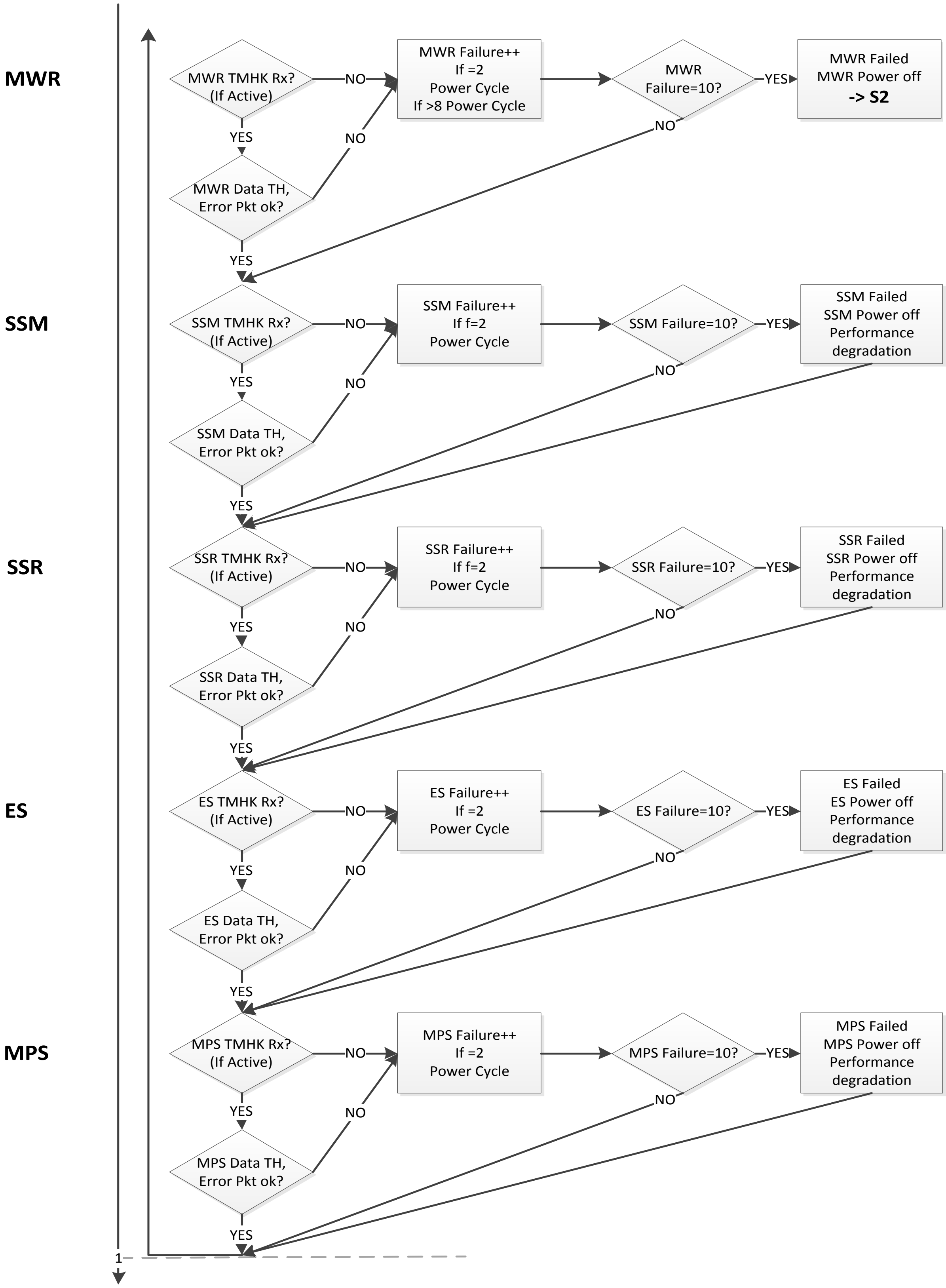

MWR
SSM
SSR
ES
MPS
MWR TMHK Rx? (If Active)
NO
YES
MWR Data TH, Error Pkt ok?
NO
YES
MWR Failure++ If =2 Power Cycle If >8 Power Cycle
MWR Failure=10?
YES
NO
MWR Failed MWR Power off -> S2
SSM TMHK Rx? (If Active)
SSM Data TH, Error Pkt ok?
SSM Failure++ If f=2 Power Cycle
SSM Failure=10?
SSM Failed SSM Power off Performance degradation
SSR TMHK Rx? (If Active)
SSR Data TH, Error Pkt ok?
SSR Failure++ If f=2 Power Cycle
SSR Failure=10?
SSR Failed SSR Power off Performance degradation
ES TMHK Rx? (If Active)
ES Data TH, Error Pkt ok?
ES Failure++ If =2 Power Cycle
ES Failure=10?
ES Failed ES Power off Performance degradation
MPS TMHK Rx? (If Active)
MPS Data TH, Error Pkt ok?
MPS Failure++ If =2 Power Cycle
MPS Failure=10?
MPS Failed MPS Power off Performance degradation
1

Figure 4.17 ACS FDIR-2

In the following diagram is explained the check performed on the magnetometer unit. It is an automatic sub-routine executed by the OBDH to check the status of the faulty unit in manner to mark it as reliable or not depending on the result. Immediately after an error reported by the magnetometer, the ACS FDIR switch to redounded unit, to ensure high data availability. Meanwhile the check routine is started, the temporization of this process have been thought to ensure a full reaction of the SW. For example six try, at least, have to be allowed in order to ensure a CAN bus switch, fixed after five failures of the main path.

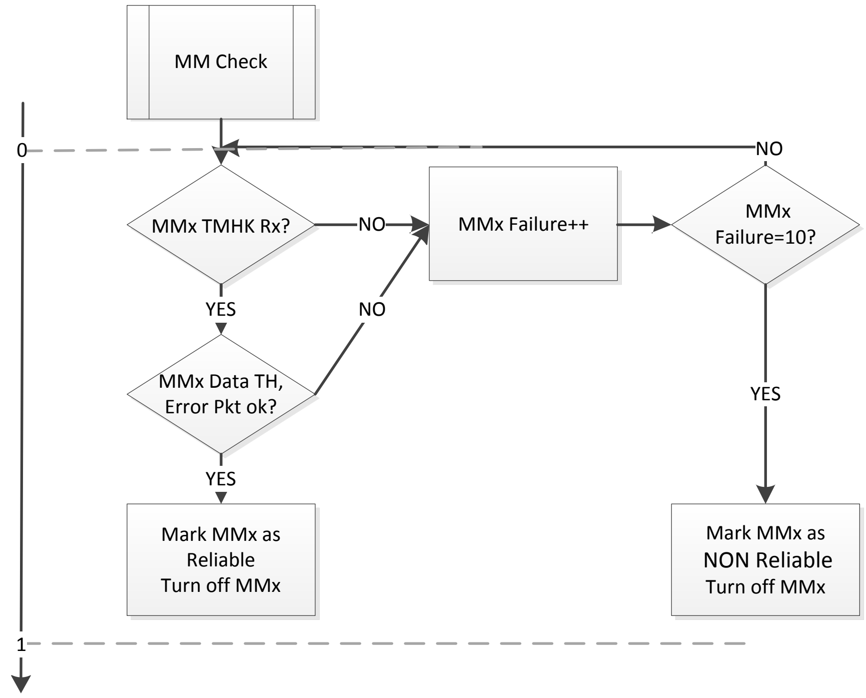

MM Check
0
MMx TMHK Rx?
NO
MMx Failure++
MMx Failure=10?
NO
YES
NO
MMx Data TH, Error Pkt ok?
YES
YES
Mark MMx as Reliable Turn off MMx
Mark MMx as NON Reliable Turn off MMx
1

Figure 4.18 MM Check

- Power bus failure and management

Power bus failures are monitored by PMU and OBDH by means of HK data analysis.

The procedures reported below, Figure 4.19 OBDH FDIR and Figure 4.20 PMU FDIR, are part of the Unit FDIR but, due to their high priority in the system hierarchy, are inserted at this level. The most important step of the two is represented by the power shedding condition. In case of OBDH active, the PMU inform the On-Board Computer thanks to its telemetry, after the internal check performed on the Power Distribution Unit to evaluate all the specific power parameters and/or shedding flags. While in case of OBDH failed is responsibility of the TMTC main to question the Power Management Unit and eventually establish a shedding occurrences invoking then a safe state of the spacecraft; only S3 and S4 modes are allowed for the TMTC system, see Platform FDIR.

PMU collects data received from PDU and delivers HK to OBDH or TMTC upon request. The following data are collected by PMU:

- Shedding status
- Temperatures of the PS units (PMU, PDU, SP, BP)
- Voltages
- Currents
- LCL and R-LCL status

LCLs and R-LCLs autonomously switch-off power supply to the units, including payloads, in case of under-voltage or current consumption exceeding the allowable value at the primary side of the DC/DC. LCL reset is performed by TC while R-LCL reset is automatic. LCL and R-LCL status are monitored by PMU delivered as part of the HK dataset to the OBDH. The Power recovery actions performed at this level by the On Board Computer have the purpose to check the LCL status of the equipment and recover the system configuration.

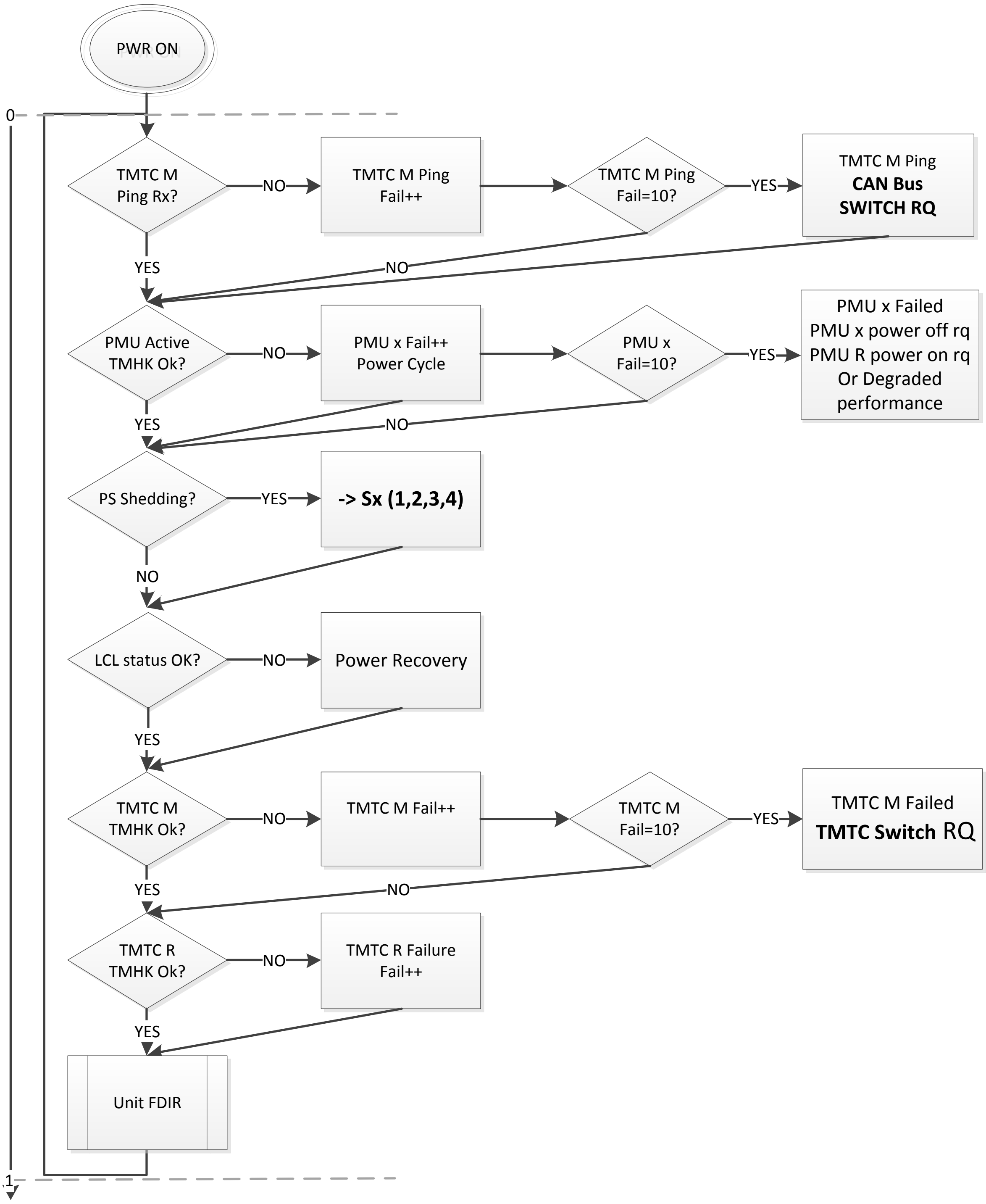


Figure 4.19 OBDH FDIR

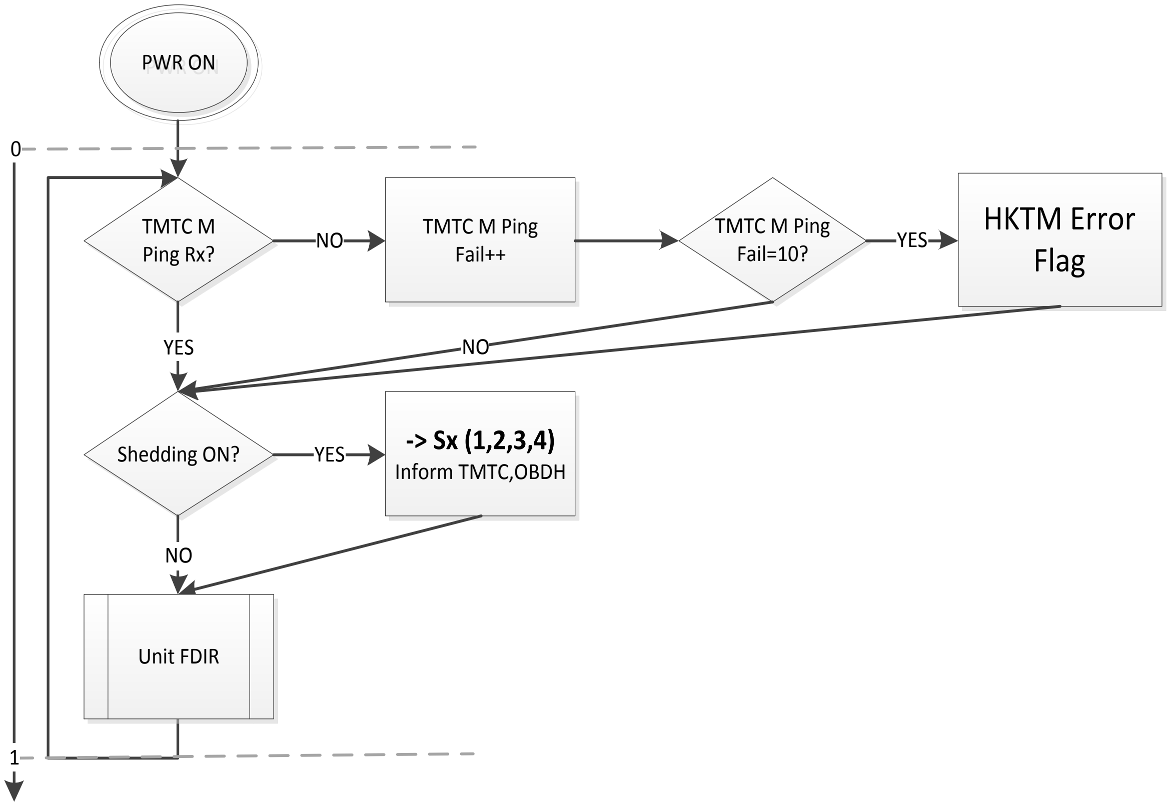


Figure 4.20 PMU FDIR

4.3.3 Unit FDIR

On ESEO satellite, all the ACS units are intelligent, equipped with the STM microcontroller. The on board software include a failure monitoring system and thus is able to detect failures at different levels. Once detected, the failures are reported to the higher level FDIR through an error packet sent over the CAN bus. In detail, the failure detection is decentralized in the following units:

- Telemetry and Telecommand (TMTC)
- On Board Data Handling (OBDH)
- Power Management Unit (PMU)
- Sun Sensor (SS)
- Earth Sensor (ES)
- Momentum Wheel Main (MWM)
- Momentum Wheel Redundant (MWR)
- MagnetoMeter (MM)

· Magneto-Torquers (MT)

All the ESEO units, connected on the CAN bus are able to send error packets onto this link, except the momentum wheel main connected through RS485 interface.

- CAN bus failure

Each subsystem embed a CAN bus failure routine, capable to detect a failure on the main bus channel. The active devices are in charge to sense and decode the heartbeat broadcasted by the master node and, in case of failure, inform the TMTC (responsible for the system CAN operations, see paragraph 4.3.1) through the redounded CAN channel in order to switch to the reliable path.

CAN bus failure detection and isolation is managed through Heartbeat function of the CANopen protocol. Each active unit shall use Heartbeat message to set the current active CAN bus.

During nominal operation the CAN bus master node, periodically sends an Heartbeat message on the active CAN bus. Each active unit receives and elaborate the message. In absence of errors and failures no reply is produced.

In case of failure of the active CAN bus each unit reply with a Heartbeat message on the redundant CAN bus in order to allow the master node to switch from the failed CAN bus to the redundant one.

TMTC is the CAN bus master node for the platform buses (main and redundant), while OBDH is the CAN bus master node for the payload buses (main and redundant).

CAN bus failure detection procedure is reported in the following figure.

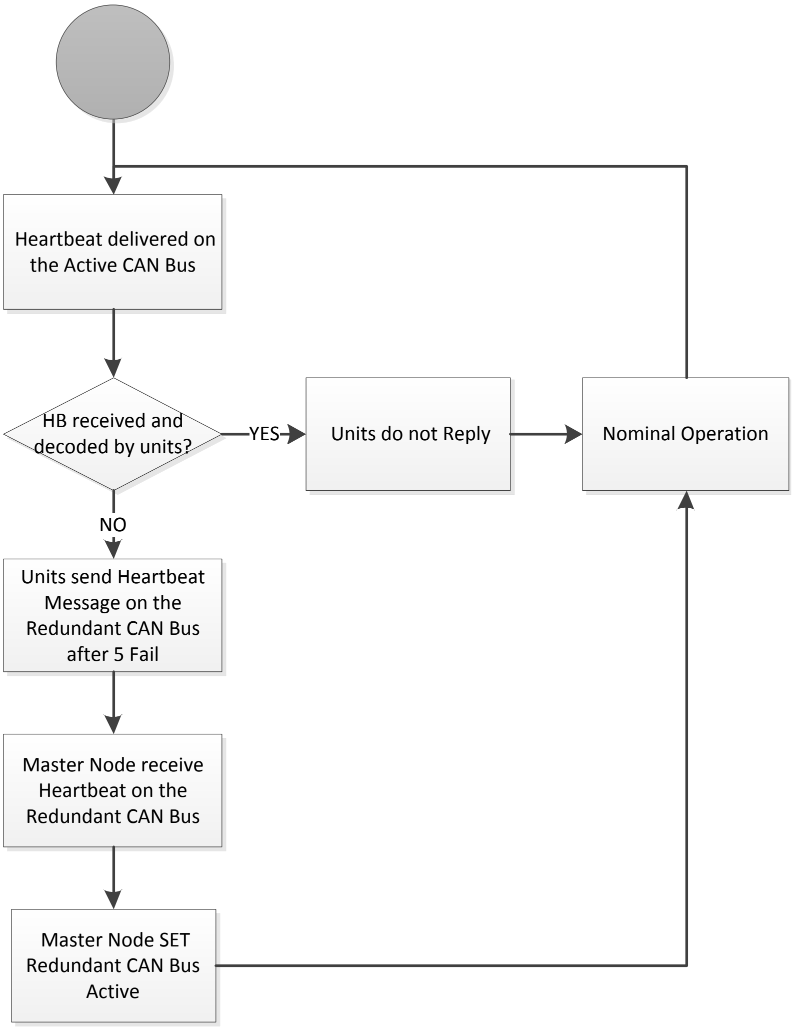

Heartbeat delivered on the Active CAN Bus
HB received and decoded by units?
YES
Units do not Reply
Nominal Operation
NO
Units send Heartbeat Message on the Redundant CAN Bus after 5 Fail
Master Node receive Heartbeat on the Redundant CAN Bus
Master Node SET Redundant CAN Bus Active

Figure 4.21 CAN Bus failure detection

The CANopen protocol implemented on the ESEO platform does not allow that units deliver data on the active CAN bus without explicit request from OBDH (or HSTX in case of payloads data). Therefore units delivering random data on the active CAN bus without permission will be switched-off.

- RS-422 failure

The OBDH and TMTC, each composed of Main and Redundant unit, are connected using a cross-strapped USART interface based on RS-422 standard. The configuration ensures reliable communication between any combination of Main and Redundant. The HW interface implements a hardware flow control mechanism in order to synchronize the data transfer and improve the reliability of the link. The communication protocol make use of CRC, built-in protections, in order to detect bit flips or errors on the data and autonomously request the failed packet again. The communication protocol implements also a packet re-synchronization procedure in order to allow the receiver to align the data in the proper order. The SW procedures for the automatic process are implemented directly at unit level.

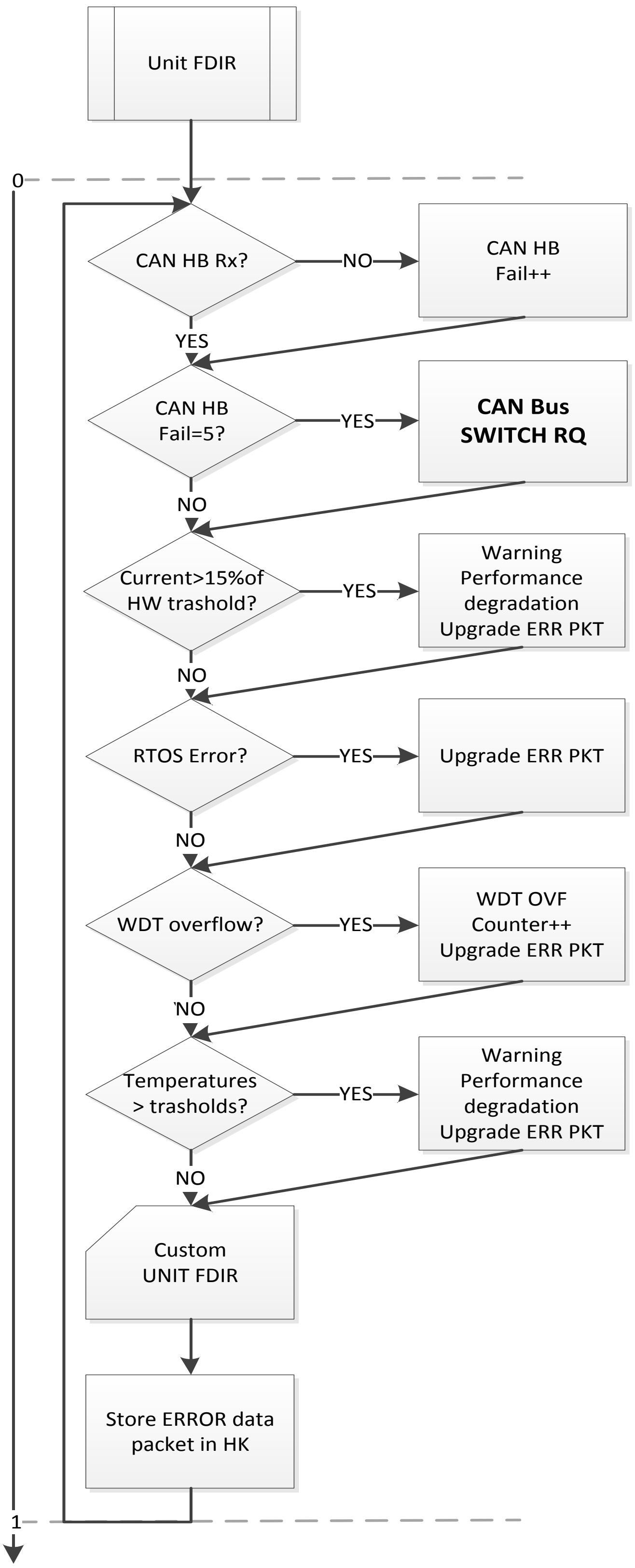
At system point of view it's TMTC responsibility to power on the OBDH main or redounded unit, thus the right RS422 communication link, to the main or to the redounded unit, is identified. Meanwhile the OBDH will keep active only the path corresponding to the system, TMTC A or B, which is marked as main. The TMTC unit could switch the roles, thanks to the Platform FDIR, without affecting OBDH/ACS operations.

- RS-485 failure

The main momentum wheel communication interface is implemented with a dedicated serial port based on RS485 standard. The bus connect both the OBDH main and redundant to the actuator. A failure of the MW, mainly detected trough the communication link and the PS's HK parameters (LCLs status), leads to the safe mode S2. The recovery actions are performed by ground as well as the switch to the redundant unit.

- PDU Failure Management

At the present state of the project a detailed failure strategy for the PDU is not available due to the system development stage. The Power Distribution unit, supplied by BME (Budapest University for Technology and Economics), is based on FPGA hardware in a hot redounded and cross-strapped architecture. Half of the system, a single PDU unit, has been already subjected to a full test campaign and several communications test have been performed with the PMU, in order to verify the correct matching. Thanks to the cross-strapped implementation, it is always possible, for the active PMU, to control and read the LCLs status, even in case of faulty internal control logic of the distribution unit. In nominal operations the loads are managed by both FPGA in hot redundancy directly controlled by the active PMU, in case of failure of the logic, the complete management of the LCLs related to the faulty unit is switched to the system still working. The failures are detected by TCHK reception and analysis, and power status verification.



Unit FDIR
0
CAN HB Rx?
NO
CAN HB Fail++
YES
CAN HB Fail=5?
YES
CAN Bus SWITCH RQ
NO
Current>15%of HW trashold?
YES
Warning Performance degradation Upgrade ERR PKT
NO
RTOS Error?
YES
Upgrade ERR PKT
NO
WDT overflow?
YES
WDT OVF Counter++ Upgrade ERR PKT
NO
Temperatures > trasholds?
YES
Warning Performance degradation Upgrade ERR PKT
NO
Custom UNIT FDIR
Store ERROR data packet in HK
1

Figure 4.22 Unit FDIR

In Figure 4.22 Unit FDIR, the common procedures implemented by every subsystem are reported. The units on board of the spacecraft perform a series of check shared between all the systems due to the modularity of the architecture. In the diagram are shown the controls performed on the CAN bus, the errors generated by the RTOS and the currents and temperatures threshold monitoring. On the other hand the Custom Unit FDIR strategies are specific for each subsystem and depend on the custom architecture or interface implemented at design level. In the following are reported the detailed strategies implemented for the fundamental equipment on board and then the payloads.

Momentum Wheel Redundant FDIR strategy

The status of the MW is monitored by means of two main sensors implemented on board:

- The encoder, installed directly on the brushless motor, monitoring the angular velocity of the MW;
- The current sensor, monitoring on each phase of each brushless motor the current absorption.

On the basis of these two information, the following scenarios can be recreated:

Scenario A:

Subject	Target/ Response
MW Driver	Set point (angular velocity) imposed
MW Encoder	No anomalies detected: Set point (angular velocity) reached
MW Current Sensor	No anomalies detected: Nominal current supply
Result	Status: OK

Table 4.3 MW FDIR Scenario A

The momentum wheel works normally.

Scenario B:

Subject	Target/ Response
MW Driver	Set point (angular velocity) imposed
MW Encoder	No anomalies detected: Set point (angular velocity) reached
MW Current Sensor	Anomaly detected: non nominal current supply (up to 130% nominal value)
Result	Status: OK – Wear detected

Table 4.4 MW FDIR Scenario B

The MW works normally, thus with performances degradation due to the wear of the bearings or of the motor stator/rotor circuitry.

Scenario C:

Subject	Target/ Response
MW Driver	Set point (angular velocity) imposed
MW Encoder	No anomalies detected: Set point (angular velocity) reached
MW Current Sensor	Anomaly detected: non nominal current supply (> 130% nominal value)
Result	Status: NOT OK – Short circuit detected on the motor phase

Table 4.5 MW FDIR Scenario C

The MW is failed and will be switched off. Up to three re-boots will be attempted to try the recovery of the circuitry.

Scenario D:

Subject	Target/ Response
MW Driver	Set point (angular velocity) imposed
MW Encoder	Anomalies detected: Set point (angular velocity) not reached
MW Current Sensor	Anomaly detected: non nominal current supply (> 130% nominal value)
Result	Status: NOT OK – Mechanical failure on RMW flywheel

Table 4.6 MW FDIR Scenario D

The MW is failed and will be switched off. Up to three re-boots will be attempted to try the recovery of the flywheel positioning, thus the affordability of the MW will be considered low.

Scenario E:

Subject	Target/ Response
MW Driver	Set point (angular velocity) imposed
MW Encoder	Anomalies detected: Set point (angular velocity) not reached
MW Current Sensor	No anomalies detected: Nominal current supply
Result	Status: NOT OK – Control algorithm failure

Table 4.7 MW FDIR Scenario E

The MW is failed and will be switched off. Up to three re-boots will be attempted to try to restart correctly the MW driver.

Magneto Torquers FDIR Strategy

Two different electrical failures have been considered in the MT design:

- Communication error
- Control current error

If the MT driver returns no response to any particular command, the MT driver is not fully operative because some communication errors have been encountered. In order to recover the peripherals a reboot is performed. If the failure persist a hardware failure (electronic failure or wiring physical disconnection) may cause the malfunctioning.

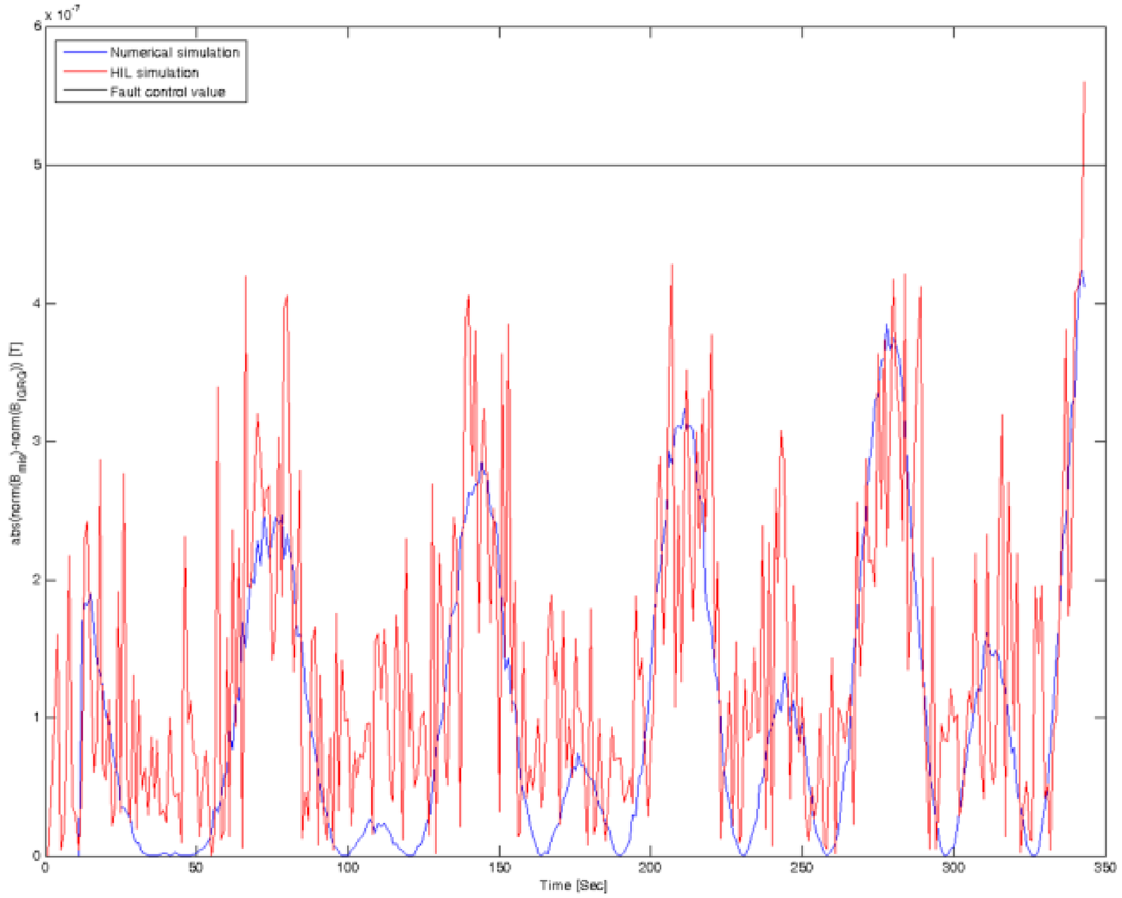
If the MT current acquired by the driver is lower than the 20% with respect to the operational current, the actuator is failed and the MT is not able to guarantee the nominal dipole. Also in this case a power cycle is performed on the control driver. If the failure persist is necessary to notify the unavailability of the actuator.

In both cases the failure is notified through the error packet to the ACS system, in order to use the magnetic actuator is necessary to switch the control to the redundant unit.

- **Magnetometer FDIR Strategy**

A MATLAB based magnetometer simulator has been developed in order to test the fault detection routine, which procedures are outlined in chapter 4.3.2 ACS/OBDH FDIR, with the same data used in the ACS fault detection simulation. The FDIR routine has been statistically characterized by using the Hardware-in-the-Loop (HIL) philosophy. During the simulation an artificial fault on the main magnetometer unit is injected. The HIL simulations results differ from the numerical simulation because a numerical truncation in the serial communication is necessary. The result is an additional sensibility with respect to the numerical simulation.

The controlled variable is represented by the difference between the norm of measured field and the norm of the IGRF[10]. The results are summarized in Figure 4.23.



[10] IGRF: International Geo-magnetic Reference Field, is a standard mathematical description of the Earth's magnetic field. It is the product of a collaborative effort between magnetic field modellers and the institutes involved in collecting magnetic field data from satellites and observatories around the world.

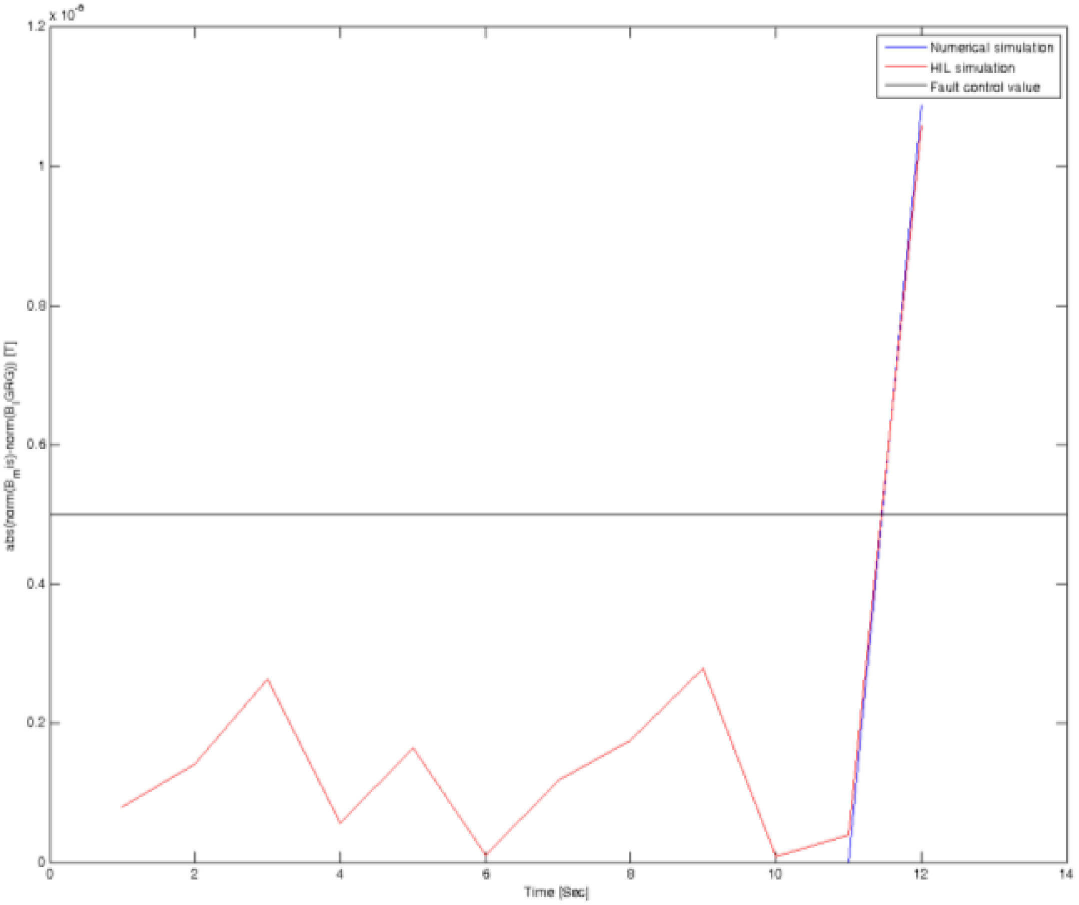


Figure 4.23 Comparison between fault control variable in the HIL simulations (red curves) and numerical simulations (blue curves) in two different configurations

The MM fault is detected in both cases before in the HIL simulation than the numerical one. If the magnetic interference with the on-board instrumentation is significant, it can provide a further noise. In order to prevent false fault detection the fault control variable can be increased.

- Payloads FDIR

The OBDH is in charge to supervise the payloads operations. The P/L CAN bus is completely independent from the main platform communication bus due to the spacecraft architecture. Moreover the OBDH has the capability to check the LCL status of the payloads through the PS TM. Each P/L unit provides a set of HK data and operational parameters to be constantly monitored by the On-Board Computer and a series of actions has to be performed as soon as discrepancies with the allowable values are detected. The general approach is reported in the following figure.

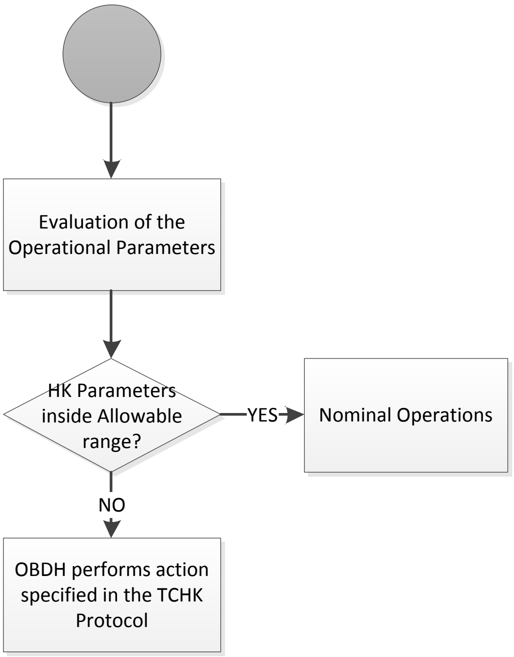

Evaluation of the Operational Parameters
HK Parameters inside Allowable range?
YES
Nominal Operations
NO
OBDH performs action specified in the TCHK Protocol

Figure 4.24 General Payload FDIR approach

Post-processing of HK on-ground is necessary in order to verify the conditions for a safe re-activation of the failed unit.

4.4 FAILURE SCENARIO

The most critical aspect related to the FDIR strategy is about the timing. It is necessary to properly set every system's reaction times in order to allow all the check and/or mechanism provided to be executed without overlapping, which could potentially lead the platform in a wrong configuration. The overlap has to be avoided also to prevent a partial coverage of the recovery actions planned, in order to perform a complete diagnosis. As described previously, the whole system embed a series of built-in, HW and SW protections or mechanisms in order to avoid: critical damages, failure propagation or power issues. The HW protections timing, as per definition, are configured on ground by means of discrete components and the reaction times have been considered immediate, in the order of milliseconds by test, with respect to the main platform timing, 1 second. The built-in, directly managed by SW, are transparent at system level and didn't affect other categories. Different considerations have been taken regarding the various SW mechanism: evaluations and counting of the failures, power cycling, and communications errors. As reported in chapter 4.3 Level 2: Software, the main parameters checked are related to the CAN bus, managed by the CANopen protocol, HKTM analysis and power conditions, which recovery procedures are well defined and executed taking into account the whole behavior of the spacecraft.

In order to allow the proper recovery, if possible, at the first issue detected the specific internal counter is started and incremented, to keep a safety margin in respect to the communications propagation delay, the first symptom is just counted; at the second attempt the unit is subjected to a power cycle with the purpose to eventually reset the Over Voltage and Over Current Protections or remove transitory malfunctioning. At this point is fundamental for the mechanism to wait, still counting, at least six more retry, due to the fact that the CAN bus switching procedure has been set to five consecutive failures, in case of system recovered the heartbeat will be detected the cycle after.

The number of retry is composed as follows: 1 (safety margin) +1 (power cycle) +5 (CAN bus switch) +1 (Heartbeat) +2 (safety margin) = 10 cycles, then the unit under inspection is declared failed. Every cycle correspond to one second, in this way a complete recovery procedure took at maximum ten seconds. The timing here exposed have been extracted thanks to the analysis of all the procedures and steps provided before, comparing each phase of the subsystems involved, in the proper temporization of the platform.

In the following several failure scenario have been reported highlighting for each the system time and the subsystems reactions. The failures evaluated have been applied with the idea to clarify the operations and in particular the timings of the main mechanisms implemented on board.

Single Event Latch-Up on the CAN transceiver of the Magnetic-Torquer main interface in the middle of the system cycle.

Time	Cycle	Subsystem action/reaction	Note
50% cycle	0	ACS TMHK Rq to MTm: SEL on MTm CAN TRX-> Latch-up, 3.3v OCP intervention Equipment OFF MTm NACK, Fail++	ACS FDIR Fail =1
	1	ACS TMHK Rq to MTm: MTm NACK, Fail++, =2 -> Power Cycling Rq to active PMU	ACS FDIR Fail =2
	2	ACS TMHK Rq to MTm: A) MTm ACK -> Nominal OP. Fail=0 B)MTm NACK, Fail++	ACS FDIR Fail =3 If active Unit FDIR Fail=1
	3	ACS TMHK Rq to MTm: A) MTm ACK -> Nominal OP. Fail=0 B)MTm NACK, Fail++	ACS FDIR Fail =4 If active Unit FDIR Fail=2
	4	ACS TMHK Rq to MTm: MTm NACK, Fail++	ACS FDIR Fail =5 If active Unit FDIR Fail=3
	5	ACS TMHK Rq to MTm: MTm NACK, Fail++	ACS FDIR Fail =6 If active Unit FDIR Fail=4
	6	ACS TMHK Rq to MTm: A) MTm Unit FDIR CAN HB Fail=5, CAN bus Switch Rq B) MTm NACK, Fail++	ACS FDIR Fail =7 If active Unit FDIR Fail=5
	7	TMTC CAN bus Switch ACS TMHK Rq to MTm: A) MTm HB Rx on CAN Red, ACK -> Nominal OP. Fail=0 B)MTm NACK, Fail++	ACS FDIR Fail =8
	8	ACS TMHK Rq to MTm: MTm NACK, Fail++	ACS FDIR Fail =9
<10 S	9	ACS TMHK Rq to MTm: MTm NACK, Fail++ MTm Failed MTm Power Off MTr Power On-> Nominal OP.	ACS FDIR Fail =10 Switch to redounded unit

Over Voltage condition on the driver of the Momentum Wheel redundant, at the beginning of the system cycle.

Time	Cycle	Subsystem action/reaction	Note
0% cycle	0	OV on MWr driver -> OVP intervention Equipment OFF ACS TMHK Rq to MWr: MWr NACK, Fail++	ACS FDIR Fail =1
	1	ACS TMHK Rq to MWr: MWr NACK, Fail++, =2 -> Power Cycling Rq to active PMU	ACS FDIR Fail =2

	2	ACS TMHK Rq to MWr:
		A) MWr ACK -> Nominal OP. Fail=0
		B) MWr NACK, Fail++
			ACS FDIR
			Fail =3
			If active, Unit FDIR
			Fail=1

	3	ACS TMHK Rq to MWr:
		A) MWr ACK -> Nominal OP. Fail=0
		B) MWr NACK, Fail++
			ACS FDIR
			Fail =4
			If active, Unit FDIR
			Fail=2

	4	ACS TMHK Rq to MWr:
		MWr NACK, Fail++
			ACS FDIR
			Fail =5
			If active, Unit FDIR
			Fail=3

	5	ACS TMHK Rq to MWr:
		MWr NACK, Fail++
			ACS FDIR
			Fail =6
			If active, Unit FDIR
			Fail=4

	6	ACS TMHK Rq to MWr:
		A) MWr Unit FDIR CAN HB Fail=5, CAN bus Switch Rq
		B) MWr NACK, Fail++
			ACS FDIR
			Fail =7
			If active, Unit FDIR
			Fail=5

	7	TMTC CAN bus Switch ACS TMHK Rq to MWr: A) MWr ACK on CAN Red -> Nominal OP. Fail=0 B) MWr NACK, Fail++	ACS FDIR Fail =8
	8	ACS TMHK Rq to MWr: MWr NACK, Fail++	ACS FDIR Fail =9
<10 S	9	ACS TMHK Rq to MWr MWr NACK, Fail++ MWr Failed MWr Power Off	ACS FDIR Fail =10 Safe mode S2

Short Circuit on the Dc/Dc of the MagnetoMeter main interface at the end of the system cycle.

Time	Cycle	Subsystem action/reaction	Note
100% cycle	0	ACS TMHK Rq to MMm: MMm ACK, Nominal OP. Dc/Dc S.C. on MMm -> PDU LCL intervention Equipment OFF	
	1	OBDH LCL set ACS TMHK Rq to MMm: MMm NACK, Fail++ MMm check. MMr Power On	ACS FDIR MMm Fail =1
	2	OBDH Lcl set ACS TMHK Rq to MMm and MMr: MMm NACK, Fail++, =2 -> Power Cycling Rq to active PMU MMr ACK, Nominal OP.	ACS FDIR MMm Fail =2 (Check)
	3	OBDH Lcl set ACS TMHK Rq to MMm and MMr: A) MMm ACK ->Reliable. Fail=0 B) MMm NACK, Fail++ MMr ACK, Nominal Op	ACS FDIR MMm Fail =3 (Check) If active, Unit FDIR Fail=1

	4	OBDH Lcl set
		ACS TMHK Rq to MMm and MMr:
		A) MMm ACK ->Reliable. Fail=0
		B) MMm NACK, Fail++
		MMr ACK, Nominal Op
			ACS FDIR
			MMmFail =4
			If active Unit FDIR
			Fail=2

	5	OBDH Lcl set ACS TMHK Rq to MMm and MMr: A) MMm ACK ->Reliable. Fail=0 B) MMm NACK, Fail++ MMr ACK, Nominal Op	ACS FDIR MMm Fail =5 (Check) If active Unit FDIR Fail=3
	6	OBDH Lcl set ACS TMHK Rq to MMm and MMr: A) MMm ACK ->Reliable. Fail=0 B) MMm NACK, Fail++ MMr ACK, Nominal Op	ACS FDIR MMm Fail =6 (Check) If active Unit FDIR Fail=4
	7	OBDH Lcl set ACS TMHK Rq to MMm and MMr: A) MMm ACK ->Reliable. Fail=0 B) MMm NACK, Fail++ MMr ACK, Nominal Op	ACS FDIR MMm Fail =7 (Check) If active Unit FDIR Fail=5
	8	OBDH Lcl set ACS TMHK Rq to MMm and MMr: A) MMm ACK on CAN main->Reliable. Fail=0 B) MMm ACK on CAN red-> Reliable on red, Fail=0 C) MMm NACK, Fail++	ACS FDIR MMm Fail =8 (Check)

		MMr ACK, Nominal Op	
	9	OBDH Lcl set ACS TMHK Rq to MMm and MMr: A) MMm ACK ->Reliable. Fail=0 B) MMm NACK, Fail++ MMr ACK, Nominal Op	ACS FDIR MMm Fail =9 (Check)
10S + **Δ failure**	10	OBDH Lcl set ACS TMHK Rq to MMm and MMr: A) MMm ACK ->Reliable. Fail=0 B) MMm NACK, Fail=10 Unreliable. MMm Failed MMm Power Off MMr ACK, Nominal Op	ACS FDIR MMm Fail =10 (Check) Performance degradation

5 CONCLUSIONS

The objective of this research, focused on allowing the success of the ESEO mission and its spacecraft in particular, is pointed to improve the probability of the space segment to survive for at least six month in the space environment, performing meanwhile the in-orbit validation required to verify and demonstrate the actual design reliability and selected philosophy.

The ESEO spacecraft, being developed by a private company needs to satisfy not only the common technical requirements but also needs to take into account typical trade-offs like: costs vs. performance, complexity vs. feasibility and time vs. human resources. The study and the results have been possible thanks to the key-position covered as part of the design team and also as Ph.D. student, since the beginning of the mission, coinciding with the start of the doctorate at the end of 2012.

Several tools have been used throughout the years to inspect, verify and characterize every phase of the development and to help improving the overall concept. From a reliability point of view many solutions have been adopted and applied both during the design and as a result of the FMEA analysis (both at system and subsystem level) and this includes safety margins, custom procedures and also FDIR implementation.

The FMEA analysis shows that the architecture design, to enhance the system reliability, makes use of:

- Redundancy: greatly increasing the numerical reliability. For instance in a system which reliability is ranked e.g. 0.8, if a spare identical unit is employed, the probability of both non failing raises to 0.96 = 1- (1-0.8) (1-0.8), in case of redounded unit switched off until needed, the probability rise again[11].
- Design diversity: applied to rise the reliability relative to a same function, employing devices produced by different manufacturers. In this case the momentum wheel main is provided by Astro-und Feinwerktechnik Adlershof GmbH while the redounded unit has been developed by ALMASpace.

[11] Reliability theory, hot and cold redounded systems.

- Effects limitation and protections: several mechanisms have been implemented in the subsystem and system design to stop the failures propagation such as the Latching Current Limiters, the Over Current Protections, the radiator panel or invoking safe modes.
- Derating of parts: used to reduce the stress and then the failure rate of the components.
- Radiation screening: all the components have been chosen from lists of official selected parts containing radiations reports or inherited from previous missions. Moreover the only industrial device used in the project, the STM microcontroller, have been subjected to radiations tests.
- Assembly controls: applied in the manufacturing facilities to avoid introducing damages to the devices.
- Testing to demonstrate the reliability: several tests have been performed on the whole system in order to rise the confidence levels and ensure a proper reliability of the architecture. Tests are reported in chapter 3.

The FMEA analysis is well ruled by the ECSS-Q-ST-30-02C standard but due to its strong relation whit the architecture and design, in addition to the “known faults” or those identified thanks to the analyst wisdom, the process includes a creative phase of research and evaluation. Because of these reasons it is necessary a very thorough study and knowledge of the platform, both at system than unity level, to perform this investigation particularly costly in terms of time.

The performed test campaign has been, and still is, a fundamental tool involved in the design verification and confirmation, processes iteratively applied with respect to the FMEA analysis. The tests were also aimed to provide the starting point of the overall FDIR philosophy in accordance with the results or outputs, and the architecture of the spacecraft. The tests executed since now, after the Critical Design Review and right before the AI&V phase, showed the full conformance of the devices checked in the conditions estimated by the mission plane. The subsystems have been verified about every aspect, to satisfy all the mission requirements related to the operational conditions; allowing also the proper characterization of the units in order to establish the right control strategies.

The FDIR strategy is part of the harmonization of the spacecraft behavior in particular under severe occurrences, which derive mainly by the impossibility to operate the required maintenance to the system. The procedures highlighted the conditions that lead to the loss of the mission. Three are the main critical systems identified: the Power System, the magnetic sensors and the magnetic actuators. The occurrence of a hard fault on both the Power Management Units will lead the spacecraft out of control, denying the possibility to further configure the subsystems. A severe failure on the power generation devices instead could lead to a critical power down and then the shut-down of the platform. The magnetic equipments are the main tools involved in the attitude determination and control procedures and a complete loss of those function will carry the spacecraft into tumbling. The FDIR actions ensure a safe management of the platform in a known state in order to allow the proper operation and the recovery. The automatization of the mechanism is always capable to induce a reaction to every first failure covered by analysis and/or detected on board. The only causes leading to a safe condition entrusted to ground control at first hard fault, in addition to the power thresholds, are the loss of the On-Board Computer or the Momentum Wheel. This policy has been chosen to ensure a double check of the platform parameters before a sure recovery to nominal mode. Indeed the failure symptoms detection and reaction are performed directly on board while a detailed fault identification will be ensured only by post-analysis on ground, thanks to the platform housekeeping and telemetry exchange. The entire set of HW, device or procedure, involved in those functions have been completely tested and validated at equipment level while those SW related are still under external inspection.

Part of this research has been conducted during the internship period at spent at the ESA ESTEC facility (February-May 2015), during which it has been possible to stay in close contact with the ESEO technical manager, the ESEO mission review board and several ESA experts in order to cover all the technical aspects. In particular: Fabio Restagno, reviewer and supervisor for the FMEA analysis and Jorge Lopez Trescastro, responsible for the software supervision of the ESEO mission.

The reliability confidence of the whole project, in accordance with the stated objectives, allowed the overcome of the Critical Design Review, thanks to the implementation of a redounded structure philosophy and the fulfillment of the requirement specifying the first point of failure as the only condition to be avoided before the complete mission loss. It has also been qualitatively estimated a failure rate of the on-board electronics around half a year, increasing the expectations about the mission accomplishment. The last step right after the AI&V phase will be the in-orbit validation, estimated in late 2016, fundamental to definitely consolidate the technologies and solutions developed.

Like for the tray-based structure and the electronic design, the modularity of the FDIR structure will allows the transfer of the architecture developed to new missions with less effort and higher confidence. The stratification ad distribution of the FDIR strategy will allow, in the future, the implementation of a more fine control, acting also on the custom parameters of the equipment in order to improve the on-board automation. This direction, enforced also by the fast growth of the electronic performances and integration, will ensure higher probability of the mission success even with severe performance degradation, ensuring low costs, fast development time and sufficient reliability to support the increasingly ambitious goals set for the category of micro and mini satellites in the near future.

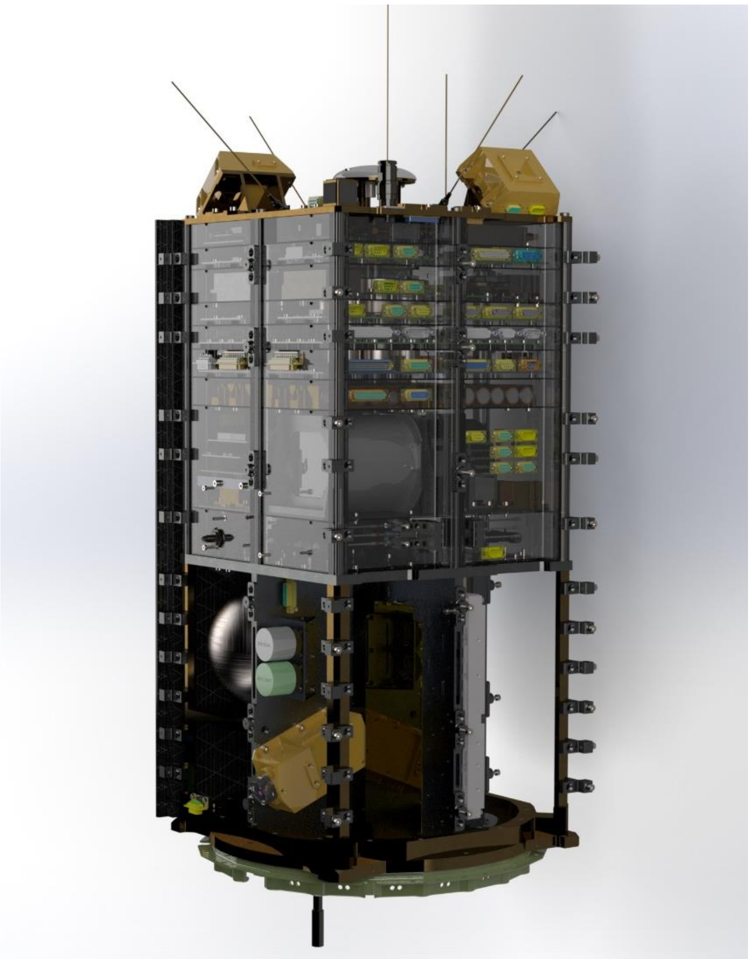


Figure 5.1 Render of the ESEO satellite

6 BIBLIOGRAPHY

Books:

- *Fortescue P., Swinerd G., Stark J.* Space Systems Engineering. *WILEY, 2011.*
- *Shewhart W. A., Wilks S. S., System Reliability Theory. Models, statistical methods and applications, WILEY, 2004.*
- *Jaeger R. C., Travis N. B.,* Microelettronic Circuit Design*. McGraw Hill, 2010.*
- *Whitaker J. C.,* The Electronics Handbook*. Taylor & Francis, 2005.*
- *Spitzer C. R.,* The Avionics Handbook*. CRC press, 2001.*

Articles:

- *Wander A., Förstner R. "*Innovative fault detection, isolation and recovery strategies on-board spacecraft: state of the art and research challenges." *2012.* *http://www.dglr.de/publikationen/2013/281268.pdf [20.2.16]*

ECSS Standards:

- ECSS-E-ST-70-11C, Space engineering: Space segment operability, 2008.
- ECSS-Q-ST-30-02C, Space product assurance: Failure modes, effects (and criticality) analysis (FMEA/FMECA), 2009
- ECSS-E-ST-40C, Space engineering: Software, 2009.
- ECSS-E-ST-70-01C – Space engineering: Spacecraft on-board control procedures, 2008.
- ECSS-Q-ST-40-09C Space product assurance: Software dependability and safety, 2012.

Datasheets:

- ST-Microelectronic: STM32F407xx: ARM Cortex-M4 32b MCU+FPU, 210DMIPS, 2015.
- Texas Instruments: SN65HVD233-HT 3.3-V CAN Transceiver, 2015.
- Maxim Integrated: MAX3232 Multichannel RS-232 Line Driver/Receiver, 2015.
- VPT: DVCH, DVSA, DVHF, DVTR series and EMI filters, v 2.0.
- Microchip: MCP2515 stand-alone CAN controller, 2005.
- Fairchild Semiconductor: NDP6020P P-channel logic level FET, 1997.
- ON Semiconductor: MMBT3904, MMBT3906 NPN and PNP Transistor, 2012.
- TT electronics: 4N49U optically coupled isolator, 2009.

- Analog Devices: OP295 operational amplifier, 2009.
- Maxim Integrated: MAX825 Microprocessor Supervisory Circuit, 2005.
- Positronic, military and space grade connectors, 2015.