HERSCHEL / PLANCK

System Operations & FDIR Requirements

H-P-1-ASPI-SP-0209

Product Code : 000 000

Rédigé par/*Written by*	Responsabilité-Service-Société *Responsibility-Office -Company*	Date	Signature
P.Couzin	Electrical & Functional Architect - ASP	30/11/03	
Vérifié par/*Verified by*			
P.Rideau	System Engineering Manager - ASP	2/12/03	
Approbation/*Approved*			
Ch.Masse	Product Assurance - ASP	03/12/03	
J.J.Juillet	Project Manager - ASP	1/12/03	

Data management : G. SERRA

Entité Emettrice : Alcatel Space - Cannes
(détentrice de l'original) :

HERSCHEL/PLANCK	DISTRIBUTION RECORD
DOCUMENT NUMBER : H-P-1-ASPI-SP-0209	Issue / Rev. : 4.3 Date: 27-November-2003

EXTERNAL DISTRIBUTION		INTERNAL DISTRIBUTION	
ESA	X	HP team	X
ASTRIUM	X		
ALENIA	X		
CONTRAVES			
TICRA			
TECNOLOGICA			
		Clt Documentation	Orig.

ENREGISTREMENT DES EVOLUTIONS / *CHANGE RECORD*

ISSUE	DATE	§ : DESCRIPTION DES EVOLUTIONS *§ : CHANGE RECORD*	REDACTEUR *AUTHOR*
1.0	30/01/02	First issue	E. BAGLIERI
1.1	13/03/02	First Release presented as a DRAFT version during PM7 FDIR splinter	E. BAGLIERI
2.0	*16/05/02*	*Second Issue – DRAFT version* *Following comments from the PM7 FDIR splinter, this new issue of the document supersedes the previous draft.* *Presentation has been reviewed and section have been reorganized.*	*E. BAGLIERI*
2.0	29/05/02	Second Issue – Configured Following FDIR meeting #4 (24/05/02 in Cannes) the second issue has been configured in accordance with the conclusions of the meeting and with some ESA and ALENIA comments (see minutes of FDIR#4 meeting : H-P-ASPI-MN-1505)	E. BAGLIERI
2.1	16/07/2002	Second Issue – First Release Update to be in accordance with PDR Design Report content. Taking into account minutes of the FDIR splinter of SVM Progress Meeting Nr.9. (doc. H-P-1-ASPI-MN-1740) Add a synthesis on failure Recovery Strategy Changes are identified by change bars.	E. BAGLIERI
3.0	06/11/02	Third Issue – This document has been updated in accordance with the Minutes of Meeting "H-P-ASPI-MN-1917" from the 10 September 2002 FDIR Meeting, the minutes of meeting H-P-ASPI-MN-2151 from the 24/10/02 and the System PDR conclusions.	R.YAKOUBI P.COUZIN
3.1	05/12/02	Third Issue – First Release First issue generated by DOORS/TREK. This document has been updated for traceability purpose. Identified Parent requirements (AD-1 and AD-3) are now indicated in the document. There are not other changes w.r.t. Issue 3.0	E. BAGLIERI

ISSUE	DATE	§ : DESCRIPTION DES EVOLUTIONS *§ : CHANGE RECORD*	REDACTEUR *AUTHOR*
4.0	25/03/03	This issue takes into account ESA proposal for the satellites mode and introduce the corresponding changes An annex specifying the 1553 CDMS Bus FDIR has also been introduced.	P.COUZIN
4.1	16/06/03	This issue takes into account ESA proposal Issue 2.1 for the satellites mode and introduces the corresponding changes : the maintenance mode is suppressed MTL requirements are modified to take into account ESA TN SCI-PT-16783 Isse 1.2. 1553 FDIR requirements in annex 1 are refined.	P.COUZIN
4.2	30/07/03	The agreement on ALS comments on issue 4.1 and stated in : - MOM H-P-MI-AI-0310 dated 23/07/03 - MOM H-P-ASP-MN-3476 dated 16/07/03 Are taken into account. Annex 1 (1553 FDIR) : - Clarifications as a result of SES comments are introduced - Requirements on Bus context saving are added. Requirements on failures recovery in AFS are added (GEF-180 and GEF-181).	P.COUZIN
4.3	27/11/03	This issue takes into account the Minutes of meeting H-P-ASP-MN-3591 dated 10/9/03. This includes the clarifications / corrections following SES comments on 1553 Bus FDIR. An additional test on the healthiness of alternate Bus before recovery has been added to 1553 DLL FDIR. A requirement has been added upon ALS request (F. Rame mail) to specify the data wrap around implementation. GEF-169 has been moved, as is, into section 2.2.2.2 for consistency purpose. GEF-144 has been made more clear and consistent. ESA comments (mail A.Elfving dated 26/11) are taken into account : - Requirement to reverse the FDIR procedure has been added in GEF-097, in line with SRS MOFM 060 - Requirement to prevent spurious Survival Mode triggering has been added in GEF-185 - Requirement for recovery procedure in case of loss of ground contact has been added (GEF-186).	P.COUZIN

TABLE OF CONTENTS

LIST OF FIGURES AND TABLES

1. INTRODUCTION

1.1 Scope

This document presents the specification of the satellite operational concept and of the Failure Detection Isolation and Recovery (F.D.I.R.) concept for both Herschel and Planck missions.

The purpose is to establish system level requirements which will drive the FDIR implementation at the different levels : system, subsystems and units.

It is the intention to have this requirements referenced and/or expanded in lower level specifications.

First of all, some general information are provided. The main points are the description of the satellite life phases and a presentation of the functional baseline.

Herschel and Planck missions have been defined in accordance with their life time. Some main phases have been highlighted and will directly influence the satellite's design. These phases shall be taken into account in the spacecraft design and shall lead to the definition of spacecraft modes (internal configurations).

The adopted internal structure will then be presented as a functional description. FDIR concept will later be based on the functional analysis.

Then, in a second step, the operational concept is presented :

Ground Operations are described. Communication link, data rates and TM/TC capabilities are presented for each life phase. Then On-Board operations and on-board command types are detailed.

As the spacecraft have a different configuration for each life phase, each mode (system and subsystem) is detailed.

Finally, in a third chapter, FDIR requirements are specified :

After a presentation of the fault tolerance high level requirements, FDIR concept is developed. Hierarchical Failure Detection and FDIR modes are introduced. Then, the FDIR strategy is fully argued and it allows to establish system level requirements.

1.2 Definitions

To avoid misunderstandings and to contribute to the document comprehension, the adopted terminology is given in the present section. The following definitions are general and are applicable to the whole document.

Computing Subsystem	SVM subsystem, which includes a computer. In the case of Herschel and Planck spacecraft, the two computing subsystems are the CDMS (Command and Data Management Subsystem) and the ACMS (Attitude Control and Measurement Subsystem).
Equipment unit	An equipment unit defines the functional equipment entity.
Failure	Any cause which lead to malfunction, performance degradation at unit, function or system level. In the following document the "failure" word is often used. Even if it is not precisely defined it shall always be understood as a "single failure event".

Feared Events	It is a potential failure which can endanger the mission and can be associated to satellite configuration operational phase and failure combination. It is defined without any regard to potential causes which could lead to the situation. The goal of the FDIR analysis is to prevent feared event occurrence upon single failure.
Flight Program	Set of commands, loaded on board by the ground, to execute a part of the satellite mission.
Function	Each function is in charge of the control and the management of a subsystem or payload. Each function directly depends on one of both computer (i.e. ACC & ACMS S/W or CDMU & CDMS S/W). Herschel and Planck spacecraft have common functions, which are : - The Spacecraft Monitoring and Control function, which is in charge of the Command and Data Management Subsystem (CDMS). - The Spacecraft Positioning function, which is in charge of the Attitude control and Measurement subsystem (ACMS). The function also includes the propulsion management. - The Power Supply function, which is in charge of the Power Control Subsystem (PCS) and depends on the CDMS. - The Thermal Monitoring and Control function, which is in charge of the Thermal Control Subsystem (TCS)and is under CDMS control. - The Payload Management function, which is managed by the CDMS.
Health Check Status	Result of Build-in-test or internal consistency check, this parameter is delivered by a unit and can be used by the OBSW to detect a failed equipment unit.
High Level Alarms	High Level Alarms are hardwired signals generated by failure detection devices and routed to the Reconfiguration Module of the associated computer. Two different types of high level alarm have been defined : **- System alarms** are received by the computer to signal anomalous system behavior. They shall lead to a system reconfiguration (switch over from nominal to redundant equipment units). **- Computer alarms** are generated internally to signal computer failures. They shall lead to a computer reconfiguration (reset or internal switch over from nominal to redundant functions).
High Priority Command (HPC)	HPC are generated by the computer upon request of : - The Reconfiguration Module without any support of the OBSW - The TC Decoder (Direct TC) without any support of the OBSW - The OBSW Upon alarm, the RM activates HPC relative to : - Computer reconfiguration (Computer alarm) - System reconfiguration (System alarm) to guarantee the satellite integrity and enter in the survival mode - HPC of a reconfiguration sequence can be generated / overridden by ground request (Direct TC).
Low Level Alarms	Low Level Alarms are detected and managed by dedicated on-board Software application. Two different types of low level alarm have been defined : **- Function alarms** are detected by the computer software to signal anomalous function behavior. They can lead to the reconfiguration of the whole functional chain. **- Equipment unit alarms** are generated by the equipment unit and detected by the on-board software to signal a failure on a specific equipment unit. They should lead to a switch over from the nominal to the redundant equipment unit.

MTL service	Mission Timeline service is an on-board service dedicated to the management of time-tagged commands. The mission Timeline is a sequence of time-tagged commands, which are stored in mass memory of the CDMS and are used to control the nominal operation of the satellite and its instruments for up to 48 hours.
Reconfiguration Module (RM)	A unit, independent from the Processor Module and the On Board Software, capable of processing some alarm signals (identifying major failures) via dedicated links. This processing unit is then able to send a series of command requests (according to the alarm detected) to the command generator. The commands generated are used, for example, to switch ON or OFF some equipment units or to reset a processor.
Reconfiguration Sequence	Set of elementary commands leading to a steady configuration of the system (i.e. without failure). Reconfiguration sequences issued by the RM are pre-defined sequences of High Priority Commands (HPC) called "**critical reconfiguration commands**". Reconfiguration sequences issued by PM are pre-defined sequences of commands routed via communication bus and Command Generator module inside the computer.
Safeguard Memory (SGM)	The SGM is accessible by both PM and used by the OBSW to store : - The failure history buffer - The OBSW context - The back up equipment units list
Satellite life phase	Part of the mission life cycle. For Herschel and Planck missions, it is possible to distinguish 6 common life phases : - Launch phase - Initial Orientation phase - Platform Commissioning and Performance verification phases - Science Commissioning phase - Observation phase - Telecommunication phase
Satellite mode	A Satellite mode is a given satellite configuration corresponding to a given satellite life phase of the mission. Satellite mode terminology includes system and subsystem modes : - System modes - ACMS modes - Telecommand/Telemetry modes - Power Control Subsystem modes - Thermal Control Subsystem modes - CDMS modes
Standby	Powered on but passivated.
Subsystem	A subsystem is a set of elements, which are able to carry out a function when they are associated to a computer. The System (SVM+PLM) is composed of 5 subsystems : - The Attitude Control and Measurement Subsystem (ACMS) - The Command and Data Management Subsystem (CDMS) - The Power Control Subsystem (PCS) - The Thermal Control Subsystem (TCS) - The Payload (PLM).

Subsystem mode	A subsystem mode is a given configuration of the considered subsystem. Nota : Telecommand and Telemetry entity is not considered as a subsystem on its own, but TM/TC subsystem modes will be defined in order to relieve CDMS modes and to help in comprehension.
System	For the present document, the system is constituted of the service module (SVM) and the payload module (PLM).
System mode	A System mode is a given configuration of the system, depending on the life phase of the mission. For each system mode, subsystem modes (i.e. ACMS modes, TM/TC modes, PCS modes, TCS modes and CDMS modes listed above) are associated. For Herschel/Planck mission, it is possible to distinguish 7 System modes : - Launch mode - Sun Acq Mode – Maintenance Mode – Science Mode – Earth Acq Mode – S/C Survival Mode

1.3 Documentation

1.3.1 Applicable Documents

AD1 :	Herschel/Planck System Requirements Specifications (SRS) Doc. n° SCI-PT-RS-05991
AD2 :	Packet Structure ICD Doc. n° SCI-PT-ICD-7527
AD3 :	Herschel/Planck Operation Interface Requirement Document (OIRD) Doc. n° SCI-PT-RS-07360
AD4 :	Herschel/Planck Space/Ground Interface Requirement Document (SGICD) Doc. n° SCI-PT-RS-07418
AD5 :	Instrument Interface Document Part B - Instrument “SPIRE” SCI-PT-IIDB/SPIRE-02124
AD6 :	Instrument Interface Document Part B - Instrument “HIFI” SCI-PT-IIDB/HIFI-02125
AD7 :	Instrument Interface Document Part B - Instrument “PACS” SCI-PT-IIDB/PACS-02126
AD8 :	Instrument Interface Document Part B - Instrument “HFI” SCI- PT-IIDB/HFI-04141
AD9 :	Instrument Interface Document Part B - Instrument “LFI” SCI-PT-IIDB/LFI-04142
AD10 :	Herschel/Planck Safety requirements for subcontractors Doc. n° H-P-1-ASPI-0029
AD11	H/W S/W Sizing cases Doc n° H-P-1-ASPI-TN-0398

1.3.2 Reference Documents

RD1 :	Herschel/Planck Design Report Doc. n° H-P-1-ASPI-RP-0049
RD2 :	Herschel/Planck functional Analysis Doc n° H-P-1-ASPI-AN-0074
RD3 :	Herschel/Planck Autonomy Doc n° PT-MOC-SYS-TN-0101-TOS-OGH
RD5 :	CDMU Technical Design Report Doc n° H-P-4-SES-NT-00021
RD6 :	ACMS baseline Design Overview Doc n° H-P-4-DS-TN-009
RD7 :	Deleted
RD8	Satellites States at Launch Doc n° H-P-1-ASPI-TN-0439 Issue 2.1
RD9	On the Use of H/P Mission TimeLine Doc n° SCI-PT-16783
RD10	Inhibits / Separation Function Doc n° H-P-1-ASPI-TN-0195
RD11	SVM requirement Specification Doc n° H-P-4-ASPI-SP-0019
RD12	Reference Mission scenario SCI-PT/12759 issue 2.1

1.4 Order of Precedence

In the event of a conflict between the requirements of this specification and those of the applicable documents here above, the requirements of this specification shall take precedence.

1.5 Acronyms

ACC	Attitude Control Computer
ACMS	Attitude Control and Measurement Subsystem
AFO	Autonomous Fail Operational
AFS	Autonomous Fail Safe
AIV	Assembly, Integration and Verification
BC	Bus Controller
BDR	Battery Discharge Regulation
CCU	Cryogenic Control Unit
CDMS	Command and Data Management Subsystem
CDMU	Central Data Management Unit
CVV	Cryostat Vacuum Vessel
DoD	Depth of Discharge
DTCP	Telecommunication Phase
FDIR	Failure Detection Isolation and Recovery
FMECA	Failure Mode Effect & Criticality Analysis
H/K	Housekeeping
HPLM	Herschel Payload Module
I/F	Interface
IOP	In Orbit Phase
ITT	Invitation to Tender
LGA	Low Gain Antenna
MGA	Medium Gain Antenna
MM	Mass Memory
MTL	Mission Timeline
N/A	Non Applicable
NOM	Nominal Operation Mode
OBCP	On Board Control Procedure
OBSW	On Board Software
OCM	Orbit Correction Mode
PACS	Photoconductor Array Camera and Spectrometer
PCDU	Power Conditioning and Distribution Unit
PCS	Power Control System

PLM	Payload Module
PPLM	Planck Payload Module
RCS	Reaction Control System
RM	Reconfiguration Module
S/C	Spacecraft
SA	Solar Array
SPIRE	Spectral and Photometric Imaging Receiver
SREM	Standard Radiation Environment Monitor
SVM	Service Module
TCS	Thermal Control Subsystem
TL	Time Line
TTC	Telemetry and TeleCommand
VMC	Visual Monitoring Camera
WUM	Wheel Unloading Mode
WUP	Wheel Unloading Phase

1.6 Requirements Numbering System

All requirements within this specification are numbered : **XXY-nnn-Z**

XX stands for the subsystem :

GE	General
AC	Attitude Control and Management Subsystem
CD	Command and Data Management Subsystem
PC	Power Control subsystem
TC	Thermal Control subsystem
IN	Instruments

Y stands for the type of requirement

F	Functional
P	Performance
D	Design
I	Interface
V	Verification

nnn is a sequential number

Z stands for the satellite applicability

H Requirement applicable to Herschel only

P Requirement applicable to Planck only

C Requirement Common to Herschel and Planck

For traceability purpose, parent requirements are indicated as following :

[P:<Parent_Specification_Reference>#<Parent_Paragraph_Number>-<Parent_Requirement_Identifier>

Example : [P:SCI-PT-RS-05991 - Ch.4#4.2.7-MISS-130 H

This example indicates that the requirement "MISS-130 H" in §4.2.7 of the specification SCI-PT-RS-05991 - Chapter 4 (SRS) is a parent of the current requirement.

1.7 Satellite Operational Life Phases

Satellite mission has to be carried out within a predefined lifetime. Then satellite life cycle can be split into several life phases, representing the main part of the mission.

Three main phases have been distinguished. For each of them, the satellite will associate a specific configuration (i.e. a combination of ACMS configuration, TM/TC configuration, power configuration….) in order to realize its mission.

Considering the life time of each spacecraft, the following operational phases can be highlighted :

- **Launch phase**, which corresponds to the wait phase of the OBSW up to the spacecraft separation from ARIANE.
- **Transfer Phase**, composed of :
  - Initial Orientation phase, which starts at launcher separation, gathers sun acquisition, star acquisition and positioning maneuver.
  - Platform Commissioning and Performance verification phases are commanded to perform satellite orbit observation and any routine action when no scientific operations are performed.
- **Routine scientific phase** is to accomplish the spacecraft mission. It is composed of :
  - Science Commissioning phase, during which Instruments are calibrated.
  - Observation phase, during which all science data are stored in the Mass Memory.
  - Telecommunication phase, which corresponds to the communication with Earth including uplink of observation program, downlink of stored data and housekeeping activities.

1.8 Functional Description

The following section aims to present a functional description of the Herschel/Planck spacecraft. It is a general section which should permit to have functional basis for further sections. The goal is to be clear on the functional terminology used across the document.

Considering FDIR requirements, each functional subsystem (thermal monitoring and control, power supply, spacecraft monitoring and control, spacecraft positioning) has to be analyzed and managed to ensure satellite survival.

From the functional description, means to carry out FDIR strategy have been defined. They are presented in the § 3. (FDIR). The logical building of FDIR strategy has been elaborated on the basis of the functional levels of the spacecraft :

- System level has been analyzed to highlight the failures which can endanger the mission
- System failures are dependent on one or several functional subsystems, which are described in the present section.
- Functional subsystems are defined by the association of equipment units. For both reliability and failure tolerance reasons, most of the equipment are redundantly implemented (although it does not appear on the functional analysis) .
- All functional subsystems are directly depending on either the ACC or CDMU. Moreover the computers ensure the management of the FDIR strategy.

1.8.1 Scope

The functional description is used to define the limits and the environment of the system, and to represent its main functions, their internal links and the outside interfaces, through top-down and structured diagrams. The iterative approach taken can be summarized as following : The system is firstly considered as a black box, in its environment. It is then divided into a limited number of functions (modules) with specific interfaces. Each module is further divided into several modules, so that each step of the analysis brings some more details about the system.

The functional description underlines the links and exchanges between functional subsystems.

Such a preliminary functional approach allows to perform a systematic and exhaustive FMECA. However, it has to be noted that the following representation of the system still remains a functional model.

As redundancy does not provide any useful information in a functional breakdown, this will not be represented in this section.

As developed in the “Functional Analysis” document (RD-2), 3 main functional levels have been clearly defined:

- System level
- Functional subsystem level
- Equipment level

This analysis leads to the definition of F.D.I.R. levels (cf. §3.3.3) and allows the association of coherent F.D.I.R. tasks/actions.

In the following part of the section, system level and functional subsystem level will be presented and detailed to have a significant idea of the functional model composition.

1.8.2 System Level

As early described in the document (§1.2 - Definitions) the “System” word defines the association of the Service module (SVM) and the Payload module (PLM). The system is in charge of operating and controlling instruments.

Therefore, for functional description, each spacecraft is composed of a system and its scientific instruments.

System modules are :

- the SVM, Service Module for platform and for experiment units at warm temperature
- the PLM, Payload Module for experiment units at cryogenic temperature. Distinguish have to be made between the two spacecraft PLM :
  - H-PLM for Herschel Payload Module, composed of the Cryostat and the Telescope
  - P-PLM for Planck Payload Module, composed of the Baffles and the Telescope

The main external modules interfaced with the System are :

- The Scientific Instruments :
  - SPIRE, PACS and HIFI (cryogenic and warm units) for Herschel spacecraft
  - HFI and LFI (cryogenic and warm units) for Planck spacecraft
- The Launcher, ARIANE 5
- The Ground, by the way of TM/TC exchange
- Some external perturbations

The following graphs represent the system data interfaces relevant for FDIR analysis (respectively the figure 1.8.1 represents the system external data interfaces relevant for FDIR and figure 1.8.2. represents system data internal interfaces relevant for FDIR).

A global functional subsystem level view is given on figure 1.8.3. It aims to present the functional architecture of the SVM used to develop the FDIR concept.

The external perturbations, which do not appear on the figures are especially the following :

- Solar Radiation
- Earth Radiation
- Radiation environment
- Launcher environment

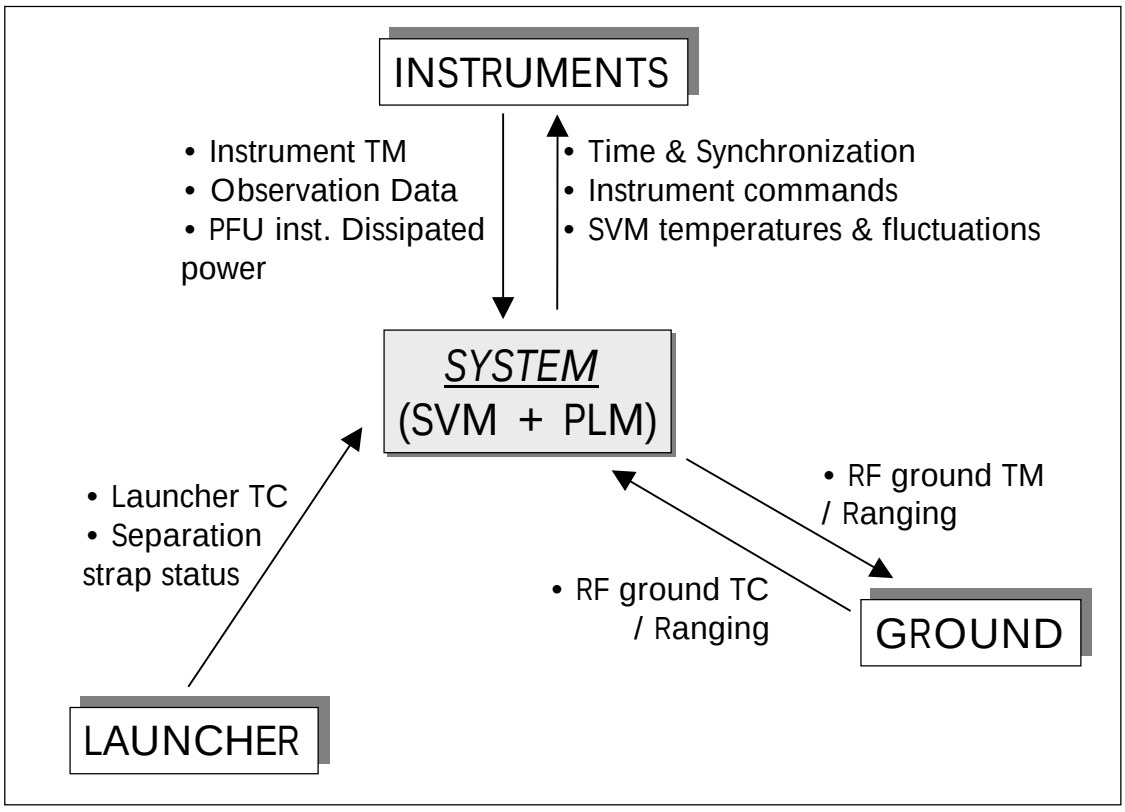

Figure 1.8.1 : System data external interfaces (relevant for FDIR analysis)

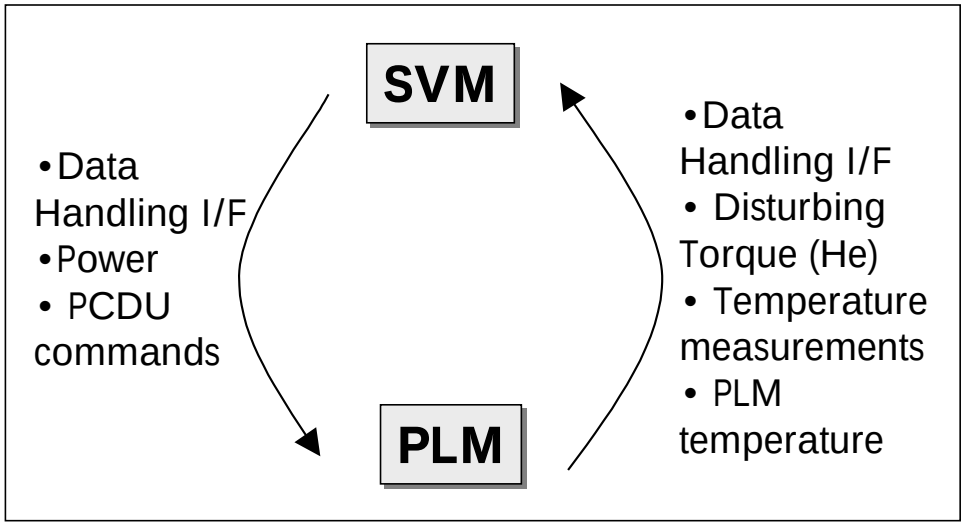

Figure 1.8.2 : System internal data interfaces -SVM / PLM (relevant for FDIR analysis)

1.8.3 Functional Subsystem Level

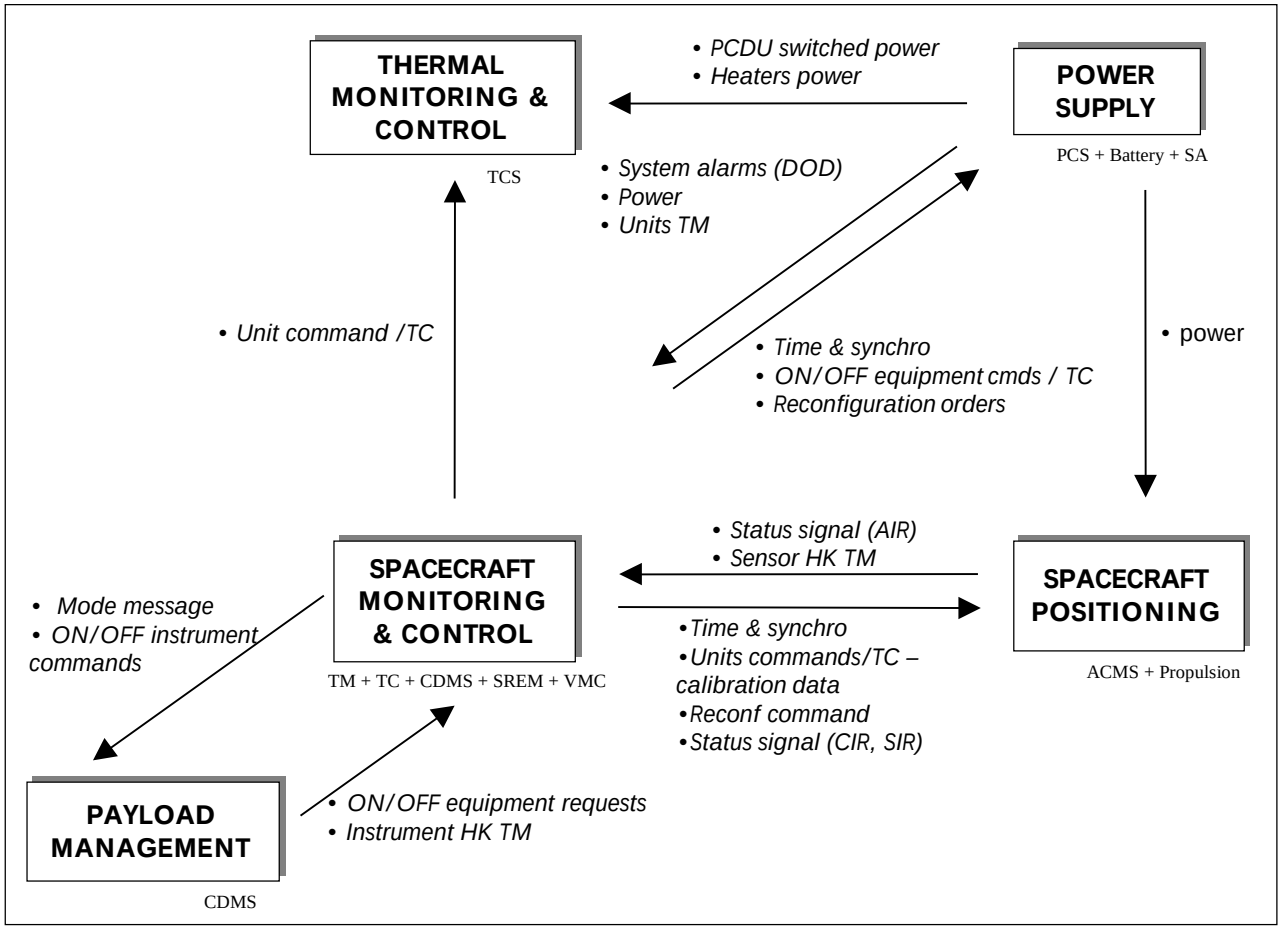

Figure 1.8.3 : System functional view of the SVM

2. SATELLITE OPERATIONAL CONCEPT

2.1 Scope

This chapter aims to present the operational concept of both spacecraft : Herschel and Planck.

First of all, the operational concept will be specified in agreement with ESA Applicable Document, *Herschel/Planck Operation Interface Requirement Document* (AD-3). Especially all the means used for mission operations are addressed (e.g. Mission TimeLine, On Board Control Procedures, Ground station features …) and a description of the satellite autonomy concept is provided (i.e. ground and on-board means to carry out satellite management).

Operational concept will be associated to a System modes definition.

Indeed, to reach and maintain the orbit and configuration required for their respective scientific mission, Herschel and Planck spacecraft have to go through several System modes depending on the satellite operational life phases[1].

Then, in a second step, satellite operational life phases will be clearly described and will lead to a complete definition of the System modes.

At the end, to conclude this section, a recapitulative schematic will present the logic of transitions between system modes previously defined. For each spacecraft, a table associating ACMS modes, TM/TC modes and system modes will also be provided.

2.2 Operation Concept

The Herschel/Planck mission presents an intermediate status for operation between missions such as ISO or XMM/integral which are in constant ground contact, and deep space missions like ROSETTA for which long period of autonomy are foreseen. The basic operation concept in which the spacecraft in orbit around L2 are operated from one single ground station (nominally New Norcia) leads to a ground contact of **3 hours per day** for each spacecraft (DTCP: Daily Telecommunication Period).

When ground contact is not available (OP: Observation Period), the spacecraft are fully autonomous, performing science observation according to a pre-defined schedule uploaded during the previous ground contact period. The spacecraft have been designed to cope with this autonomy requirement, allowing operation without ground contact **for 48 hours** especially by means of Mission TimeLine service. The goal is to maximize the scientific data return and to put the spacecraft in safe condition in case of major anomaly only.

In order to allow a significant autonomy, commands to the spacecraft have been separated into :

- On-board commands (e.g. time-tagged commands from the MTL service), allowing autonomous function of the satellite
- Ground commands (e.g. ground TC), to load on-board program, get back the observation data and operate on the satellite in case of necessity.

[1] A System mode defines the spacecraft configuration to realize a specific activity when a satellite operational life phase defines a period on which the satellite is operating one or several specific activities.

Another major driver is to maximize commonality in the way the two spacecraft are operated. Even if they may exhibit differences (Herschel is a 3-axis stabilized spacecraft while Planck is a slow spinner), they share a number of commonalties :

- similar orbits around L2
- use of the same ground stations
- identical sharing of daily operations between OP and DTCP
- common design for electrical subsystem of Herschel and Planck
- identical data rates to ground.

Commonality in operation concepts will lead to reduction of the operational costs by allowing the use of the same procedure for the two spacecraft.

2.2.1 Ground Operations

The Herschel and Planck spacecraft will be operated from the MOC (Mission Operation Center) at ESOC which interfaces with the Herschel Science Center (HSC) and Herschel Instrument Control Centers (ICCs) and for Planck with the Data Processing Centers (DPC). Commanding of both spacecraft will be conducted by MOC based on inputs received from these centers. Housekeeping telemetry received from both platform and instruments will be processed by the MOC. Science telemetry as well as relevant housekeeping will be transferred to the scientific centers.

During scientific operation, both spacecraft will be operated from the New Norcia 35 m ground station. However other ground stations (eg. VILSPA or KOUROU as LEOP stations) are envisaged during the various phases of mission. The planned usage of ground stations during the various phases of mission is shown in Table hereafter :

MISSION PHASE	GROUND STATION	
Initial Orbit Phase (IOP)	ESA Network (New Norcia, Kourou)	
Platform Commissioning Phase	New Norcia 35m (routine)	Kourou (emergency)
Performance Verification Phase	New Norcia 35m	Kourou (TBD)
Routine Scientific Phase	New Norcia 35 m	Kourou (emergency)

Communication to ground relies on X-Band for both TM and TC. TC is nominally via the Medium Gain Antenna (MGA). TC via the Low Gain Antenna (LGA) is a backup solution.

For telemetry, various TM modes are envisaged as shown in the following table . For commonality reasons, the same data rates have been selected for Herschel and Planck.

		Antenna	Ground Station	Herschel	Planck	TM modes
TM Hi-rate		MGA	New Norcia	1.5 Mbps	1.5 Mbps	Real time HK Real time science Dump S/C & Science HK Dump Science
TM medium-rate		MGA	New Norcia/ Kourou	150 kbps	150 kbps	Real time Science Real time HK Dump S/C & Science HK
TM low-rate	Low 2	LGA	New Norcia	5 kbps	5 kbps	Real time essential HK + 1kbps of stored HK
	Low 1		Kourou	500 bps	500 bps	Real time essential subsampled HK

Nominal TC rate is 4 kbps via LGA when communicating via New Norcia, and 125 bps when Kourou is used. In addition, commanding via MGA at 4 kbps is also possible. The various TC mode are summarized in the following table; they are identical for Herschel and Planck.

	S/C ANTENNA	GROUND STATION	DATA RATE	REMARKS
TC low rate	LGA	Kourou	125 bps	
TC nominal	LGA or MGA	New Norcia	4 kbps	

The figure hereafter summarizes the ground segment for Herschel and Planck satellites.

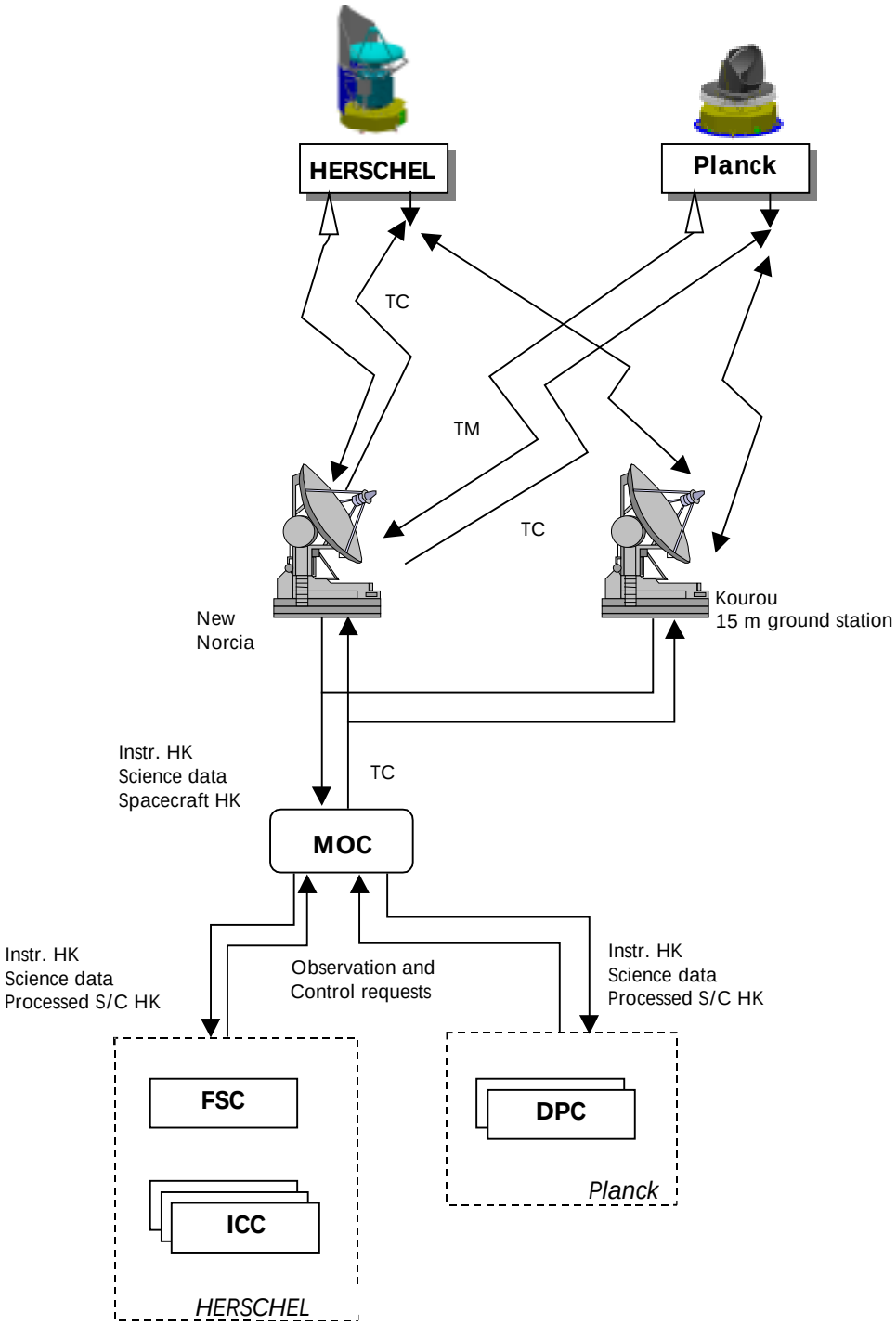

Figure 2.2.1 : Ground segment for Herschel and Planck spacecraft

2.2.2 On board Operations

2.2.2.1 General

The basic concept of operations for the satellites is that in nominal all activities will be performed through the on-board Mission TimeLine (MTL) service (see AD2). This is the operational way to command the spacecraft in open loop during nominal scientific operations, even if the spacecraft is in ground visibility.

Actions from ground are limited to receiving telemetry (real time and stored in the mass memory) and sending commands to update the Mission Timeline.

Another main concept of operation of the spacecraft is to execute On board procedures (OBCPs). They are more specifically dedicated to control procedures, but they can be activated in nominal scientific operations.

Real time commanding of the spacecraft is also possible. However, when the spacecraft is under ground control, autonomy functions are still active on-board and ground commands are not required to maintain spacecraft safety. This is in accordance with the requirement that ground reaction within less than 3 minutes shall not be required (OIRD, CTRL-1).

During all operating modes, HK TM must be continuously generated and acquired when relevant (ie the unit is ON and valid)

Reference **GEF-141-C**

The Housekeeping telemetry shall be continuously generated and acquired in all S/C operating modes, including Survival Modes. Obvious agreed exceptions are when the monitored unit is OFF/invalid.

*

2.2.2.2 Mission TimeLine (MTL)

Reference **GEF-001-C**

The MTL service shall be defined according to the Packet Structure Interface Control Document (AD2)

*

The MTL service supports the concept of subschedules (AD2).

Subschedules are constituted of one or several Time-tagged commands. A time-tagged command can perform direct commanding, initiate On-board Control Procedures or activate functions.

The H/P Mission Timeline is composed of time tagged commands of different nature which can be identified by addressees :

- ACMS commands
- Instruments commands
- CDMS commands comprising configuration commands for the CDMU (SSMM), power S/S, TTC S/S, possibly thermal control and CCU (for Herschel only).

To have straightforward interfaces with ground and operation, we consider a centralized MTL management. It means that there is a single MTL manager, the CDMU, which distributes the commands based on the Central Time reference.

Reference **GEF-112-C**

[P:SCI-PT-RS-07360#3.9-MTL-2.

The Mission Timeline service shall be centralized within the CDMU.

*

Reference **GEF-142-C**

The accuracy and resolution of the MTL shall be 1s

*

Reference **GEF-159-C**

MTL commands time tagged at t1 shall be released in the [t1, t1 + 1s] time frame.

*

Reference **GEF-143-C**

Commands loaded into the MTL with the same execution time shall be executed in the same order they were uploaded.

*

To be compatible with the Packet Structure ICD and for FDIR reasons (developed in the chapter 3.), the Time-tagged commands dedicated to one or several users will be grouped into subschedules or sequenced depending on their activity.

Reference **GEF-002-C**

Deleted

*

Reference **GEF-113-C**

Deleted.

*

Overall concept for subschedules and overall MTL management principles retained for H/P are described in RD9. It basically leaves the MTL management responsibility to the Ground entity ; to this purpose :

- The notion of permanent and transient subschedules is introduced,
- the mechanism to enable / disable telecommands for a given destination (identified by the TC APID), or belonging to a given subschedule, is proposed to make use of service 11 type commands, inserted inside the MTL by the Ground entity as part of the MTL elaboration process.

Reference **GEF-160-C**

A permanent subschedule is defined by the fact that it is always enabled at the start or re-start of the MTL (eg. when the MTL service gets enabled)

*

Reference **GEF-161-C**

A transient subschedule is defined by the fact that it is always disabled at the start or re-start of the MTL (eg. when the MTL service gets enabled).

*

Reference **GEF-162-C**

The permanent subschedules ID's shall be below 256. The transient subschedules ID's shall be above or equal 256.

*

Reference **GEF-163-C**

It shall be possible to enable/disable the release of telecommands from transient subschedules via an explicit TC.

*

Reference **GEF-164-C**

Deleted (covered by PS ICD)

*

Reference **GEF-165-C**

Deleted (covered by PS ICD)

*

Reference **GEF-166-C**

Deleted (covered by PS ICD)

*

Reference **GEF-144-C**

A given destination shall generally be prevented to "miss" MTL commands : in case of anomaly in the processing of a MTL command belonging to a transient subschedule, before sending (eg. wrong APID, erroneous length, CRC), the whole transient subschedule shall be disabled. This does not apply to permanent subschedules.

*

Reference **GEF-169-C**

In the case (unpredictable) where a MTL commands would get overdue,

- an event shall be raised
- if the overdue command belongs to a transient subschedule, the subschedule shall be disabled

- if the overdue command belongs to a permanent subschedule, it shall be sent at the earliest possible time, and the MTL commands order shall still be maintained.

*

Reference **GEF-003-C**

Deleted.

*

The following tables illustrate 2 possible MTL implementations. Both of them make use of the mechanisms specified in the present section. Actual flight Implementation will be managed under ground responsibility.

Line	Subschedule	Telecommand	Destination
1	2	Start slew	ACMS
2	1	Configure packet store	CDMU
3	1	Select Bus profile	CDMU
4	1	Enable Release Subschedule 300	CDMU
5	300	Select filter wheel	Instrument 1
6	300	Select mode	Instrument 1
7	300	Start observation	Instrument 1
8	300	End observation	Instrument 1
9	1	Disable Release Subschedule 300	CMDU
10	1	Enable Release Subschedule 400	CDMU
11	2	Perform Slew	ACMS
12	400	Select mode	Instrument 2
13	400	Start observation	Instrument 2
14	400	End observation	Instrument 2
15	1	Disable Release Subschedule 400	CDMU
16	1	Enable Release Subschedule 300	CDMU
17	300	Select mode	Instrument 1
18	300	Start observation	Instrument 1
19	300	End observation	Instrument 1
20	1	Disable Release Subschedule 300	CDMU
…	…	…	…

Sample 1 : the subschedules are tightly connected to a certain instrument.

Line	Subschedule	Telecommand	Destination
1	1	Enable Release Subschedule 1005	CDMU
2	1005	Select Bus profile	CDMU
3	1005	Configure Packet Store	CDMU
4	1005	Start slew	ACMS
5	1005	Select filter wheel	Instrument 1
6	1005	Select mode	Instrument 1
7	1005	Start observation	Instrument 1
8	1005	End observat ion	Instrument 1
9	1	Disable Release Subschedule 1005	CDMU
10	1	Enable Release Subschedule 2100	CDMU
11	2100	Perform Slew	ACMS
12	2100	Select mode	Instrument 2
13	2100	Start observation	Instrument 2
14	2100	End observation	Instrument 2
15	1	Disable Release Subschedule 2100	CDMU
16	1	Enable Release Subschedule 1006	CDMU
17	1006	Perform Slew	ACMS
18	1006	Start observation	Instrument 1
19	1006	End observation	Instrument 1
20	1	Disable Release Subschedule 1006	CDMU
…	…	…	…

Sample 2 : transient subschedules are more related to complete observations

Figure 2.2.2 : MTL Service possible implementations

Subschedules are time-referenced. They can be identified from APID, subschedule ID as specified in AD02.

Considering a centralized MTL, running from the CDMS, interfaces with instruments and ACMS (more specifically with ACC) have to be considered.

2.2.2.2.1 MTL Interface with ACMS

Reference **ACF-005-C**

[P:SCI-PT-RS-07360#3.9-MTL-3.

Nominally, at ACMS level , the MTL service shall be in charge of :

- Modes/sub-modes changes :pointing modes, orbit correction….
- Transmission of the requested pointing parameters, pointing target… in line with the spacecraft modes and the scientific operations to carry out.

*

Reference **ACF-007-C**

To avoid conflict between commands, basic communication rules for ACMS commanding shall be defined.

*

These address the mechanism of acceptance/rejection/chaining of ACMS TC's.

Reference **ACF-006-C**

The ACMS shall not reject any command issued by the CDMS, except in case of syntactic error or pointing outside of pointing domain, invalid modes transitions and violations of pre defined restrictions agreed by the Prime contractor.

*

Reference **ACF-008-C**

The mechanism of Commands rejection shall be overridable

*

Reference **ACF-009-C**

The ACMS shall accept commands in all the modes.

*

Indeed, the ACMS (actually the ACC) does not implement any high priority commanding mechanism allowing to bypass the nominal command path which would permit to recover from a locked condition.

In that case, the nominal path has to be used, and must always remain available at least for access by ground.

Some protections, however, have to be implemented to cover the problem of false commanding by the CDMS :

Reference **CDF-007-C**

All critical and modes change Commands shall use a secure command protocol (e.g. based on arm and fire mechanism).

*

2.2.2.2.2 MTL Interface with Instruments

Reference **INF-004-C**

[P:SCI-PT-RS-07360#3.9-MTL-3.

Nominally, at instrument level, the MTL shall be in charge of :

– Instrument turn on procedure
– Operational mode change
– Parameters setting for the scientific observation to run.

*

2.2.2.3 On-Board Control Procedure (OBCP)

One mode of operation of the Spacecraft will be by execution of pre-defined on-board control procedures (OBCPs) initiated from different way (mission timeline service, ground…). OBCPs are flight procedures, which are resident on-board of the Herschel or Planck satellite. They are written by using a Spacecraft Control Language (SCL).

After activation they are executed in the on-board system, e.g. the CDMS, and possibly other intelligent on-board users (except ACMS), like instrument control units). They serve for controlling processes, which may be active for an extended period of time and which may involve the (conditional) execution of a (longer) sequence of commands. These on-board Telecommands may affect one or several application processes or functions. More than one on-board unit may be involved.

In order to retain predictable and robust behavior of the spacecraft and its systems the number of OBCPs has to be kept to a minimum, and the internal design of each OBCP must be kept simple.

OBCPs can be activated by :

– Mission TimeLine (MTL) service
– Ground command
– On-board functions and events.

Reference **GEF-167-C**

An OBCP Shall only be stopped under one of the following conditions :

– it has run to its end
– it stopped itself
– it was stopped by an OBCP runtime error
– an explicit TC[18,4] (« stop OBCP ») has been executed
– the overall OBCP service is stopped
– the Processor Module is started, reset or re-started

*

Reference **GEF-145-C**

Mechanisms shall be designed to allow the execution of and management of up to 16 OBCP's simultaneously

*

2.2.2.4 FDIR Commands and Direct Telecommands

Direct Telecommands

Most telecommands will be stored on board for later execution at a defined time, via the MTL service. Others may be intended for immediate execution. Indeed, real time ground commanding of the spacecraft is possible during DTCP.

These direct telecommands are asynchronous signals and will be executed independently from the MTL service (i.e. at any instant).

One possible task using direct telecommand is to enable or disable the on board FDIR function.

FDIR Commands

On board, in case of alarm occurrence, the FDIR function will engage a reconfiguration sequence. A reconfiguration sequence is composed of elementary commands leading to a steady configuration of the system (i.e. without failure). Each elementary command is called FDIR command.

They also are asynchronous commands and can activate OBCPs.

Considering Direct Telecommands and FDIR commands, both asynchronous, a priority management shall be implemented to handle the case of commanding conflicts.

2.2.2.5 Priority Management

Considering the essentially different nature of the telecommands sources on board Herschel/Planck satellites, a priority order based on their respective criticality in the frame of the baseline operation principles is established. This permits to make the most efficient usage of the bandwidth of the on board communication links. It is applicable to all onboard systems, where meaningful :

The retained order is :

- **(0) High Priority Ground commands** : this source has been artificially created in order to provide to the Ground the highest priority access to the S/C commanding resources in very exceptional conditions. The S/C design is not supposed to take into account the occurrence of these priority 0 TC's in routine mode of operation, but is required to execute them with the highest priority whenever they occur. Should the High priority ground command start a routine software function (AD02 service 8), all the telecommands possibly generated by this function will have the routine SW function priority order.
- **(1) FDIR commands** : they are by definition critical and need to be executed first, whenever such commands occur. A specific allocation for these commands has to be implemented in the commanding task. Should a FDIR process start a routine software function (AD02 service 8), all the telecommands possibly generated by the function will have the SW Function process priority order. Should a FDIR process start an identified FDIR SW function, all the telecommands possibly issued by this function will have the FDIR process priority order.
- **(2) MTL Commands** : These commands are, by definition, On Board Time related within a second and the communications protocol must guarantee their execution. A specific allocation for these commands has therefore to be implemented in the commanding task. Although GEF-169 explicitly requires a mechanism to be implemented to handle the late permanent subschedule MTL commands, the operational baseline as stated in AD11 is built to avoid this configuration. Should the MTL start a routine software function (AD02 service 8), all the telecommands possibly generated by this function will have the routine SW function priority order.

– **(3) Ground commands** : due to the limited ground visibility, and the spacecraft distance, the real time commanding by ground is not entirely possible, and nominal (by opposition to the High Priority ones above) ground commands must be considered as not time critical compared to above sources. Should the ground command start a routine software function (AD02 service 8), all the telecommands possibly generated by this function will have the routine SW function priority order.

– **(4) SW routine Functions commands** : these are the commands issued by routine SW functions (eg. Thermal control). Their time criticality is low then the time criticality of the commands directly issued by the previous sources. Note that these do not comprise specific, and well identified FDIR SW functions which have the FDIR priority as mentioned in (1).

– **(5) OBCP's commands** : the OBCP mechanism is by principle and due to its implementation, reserved to those on board operations which are not considered as time critical within few seconds. Note that all commands issued by OBCP's, even those started by FDIR processes, ground, or possibly MTL, enter in this non critical category.

An overall allocation for the Ground, SW routine and OBCP's commands has to be implemented in the commanding task.

Reference **GEF-140-C**

The execution of commands within the on board systems shall be based, where meaningful, on the following priority scheme

0- High Priority Ground Commands

1- FDIR Commands

2- MTL Commands

3- Ground Commands

4- Routine SW functions Commands

5- OBCP Commands

*

The above priority scheme provides rules to solve the case of conflicts between commands in case a bottleneck exists in the commanding throughput (eg. at the level of the 1553 data bus).

Reference **GEF-182-C**

The sizing figures to apply for each command category shall be as specified in AD11. The On Board Data Handling shall be demonstrated to comply with AD11.

*

Furthermore

Reference **GEF-146-C**

Each FDIR procedure shall include the commanding (eg subschedule disabling, TC APID disabling) necessary to avoid any of its action identified as critical for the safety of spacecraft elements or science mission, to be later contradicted by lower priority commands.

2.3 Satellite modes

The satellite modes aim to predefine a spacecraft configuration for a given life phase of the mission in order to simplify the testing and the design cases.

This chapter will present all the modes used for spacecraft configuration. After having detailed system modes, each subsystem modes will be presented.

2.3.1 System Modes

Spacecraft system modes have been defined following the definitions given in the SRS (*AD1*). Correspondence between the defined modes and the various phases of the mission is also presented to ensure that all the mission phases are properly covered. The main drivers for definition of the spacecraft modes are the following :

- to provide the instruments with the required observation modes for their scientific objectives,
- to provide the necessary modes logically sequenced to ensure efficient and inherently safe operations of the satellite when an unplanned event may endanger the instrument detectors, the optical components, the lifetime of the spacecraft on-board equipment.
- to minimize the number of modes and maximize commonality between Herschel and Planck, in order to simplify on-ground operations.

2.3.1.1 Overview

To each satellite operational Life Phase is associated one or several System modes. The following graph illustrates the correspondence between both.

Satellite Life Phase		System mode
Launch Phase		Launch Mode
Transfer Phase	Initial Orientation Phase	Sun Acq Mode
	Platform Commissioning and Performance Verification Phases	Nominal Mode
Routine Scientific Phase	Science Commissioning Phase	Nominal Mode
Recovery Phase	CDMS computer level failure	Earth Acq Mode
	CDMS system failure	S/C Survival Mode
Attitude Recovery Phase	ACMS failure	Sun Acq Mode

Figure 2.3.1: Operational life phase vs. System modes

In the following sections each System mode will be presented and described.

Reference **GEF-168-C**

In each System Mode, self transition shall be authorised, and shall result in the application of the default setting defined for the current Mode.

*

2.3.1.2 Pre-launch/Launch Mode

This mode corresponds to a wait mode of the spacecraft : some equipment units have to be powered on and on-board S/W is in a standby state.

Reference **GEF-004-C**

Launch Mode shall be the active mode from launch pad CheckOut Test Equipment disconnection up to completion of the On board activities performed after separation from the Launcher, aiming to set the spacecraft in flight operational configuration. S/C status and mandatory transition during Launch Mode shall be as described in RD8, unless specified in the present document.

*

For example, detection can be made by majority voting in the CDMU Reconfiguration Module (RM).

Reference **GEF-005-C**

[P:SCI-PT-RS-05991 - Ch.4#4.2.3.2-MISS-055 H/P

During launch mode, at a minimum, :

– TC reception and processing (both for ACMS and CDMS) shall be active

– TM collection and storage shall be performed

– Power shall be autonomously generated and distributed

– Herschel PLM monitoring and control shall be performed (CCU nominal + redundant is ON)

The spacecraft shall be configured such that the attitude control system can be operational 20s after separation and in compliance with the attitude domain constraints specified in RD11 [ACP-016-H].

– The spacecraft shall be configured such that the telemetry can be downloaded 20s after separation

*

Reference **GEF-006-C**

During launch mode, HK data shall be stored in Mass Memory.

*

Reference **GEF-007-C**

[P:SCI-PT-RS-05991 - Ch.4#4.2.3.1-MISS-020 H/P

During launch mode, power shall be provided by the batteries.

*

During launch mode, after fairing separation, orientation of the launcher will be such that the Herschel Sun Aspect Angle requirements will be fulfilled (i.e. the Herschel Solar Array will be exposed to Sun allowing battery charging.)

Nota :This is however not the case on Planck as its Solar Array will not be exposed to Sun.

Reference **INF-001-C**

[P:SCI-PT-RS-05991 - Ch.4#4.2.3.1-MISS-020 H/P

During launch, instruments shall all be switched off, except HFI which is in launch mode to provide power to the 4K cooler for launch lock.

*

Planned operations are :

Before launch, HFI DPU is turned ON and power is supplied to HFI 4K cooler. HFI DPU controls the switch of the 4K cooler into Launch locked mode, then, HFI DPU is turned OFF during launch. HFI DPU is turned back ON TBDmn after launch to remove the 4K cooler launch lock condition.

Reference **GEF-008-C**

When physical separation is detected :

– Post separation activities shall be performed to exit the spacecraft from the launch configuration before engaging the S/C Sun Acq mode

– The sequence to transition to S/C Sun Acq Mode shall be implemented in compliance with AD10 requirements.

– The Visual Monitoring Camera shall be turned ON

*

As a consequence to RD8

Reference **GEF-011-C**

[P:SCI-PT-RS-05991 - Ch.6#6.9.4-SMAC-125 H/P
[P:SCI-PT-RS-05991 - Ch.4#4.2.3.2-MISS-055 H/P

As a design goal considering the major launcher safety constraints, 20 seconds after separation the spacecraft shall be able to transmit telemetry and the ACMS shall be fully operational.

*

It shall be pointed out that it is not allowed to activate thrusters or transmit TM earlier than 20s after separation.

2.3.1.3 Sun Acquisition mode

Reference **GEF-009-C**

Deleted

*

The aim of this mode is to reach and maintain a safe sun-pointed attitude .

Launcher separation detection initiates the separation sequence program running in the CDMU and ACC which commands all activities to perform Sun acquisition and acquire data link with Earth.

Reference **GEF-147-C**

The Sun Acquisition Mode shall be entered (OR) :

– At separation from the Launcher, after all immediate post separation On Board activities
– Upon Ground command
– Upon ACMS attitude alarm triggering
– Upon ACMS computer switch over

*

Reference **GEF-010-C**

– deleted

*

Reference **GEF-012-C**

[P:SCI-PT-RS-05991 - Ch.4#4.2.3.2-MISS-045 H/P

In Sun Acquisition Mode mode, the spacecraft shall be in Sun-pointed attitude.

*

Reference **PCF-001-C**

[P:SCI-PT-RS-05991 - Ch.4#4.2.3.2-MISS-050 H/P

Once sufficient Sun pointing is achieved, power generation shall be automatically switched to Solar Array.

*

Sun pointing will be observed by the Sun Acquisition Sensors of the ACMS.

Reference **GEF-013-P**

[P:SCI-PT-RS-05991 - Ch.4#4.2.7-MISS-120 P

On Planck the initial spin direction shall be defined by the launcher and shall not be changed during the mission.

*

Reference **GEF-148-C**

The satellite Sun Acquisition Mode shall make use of :

- The nominal set of ACMS sensors/actuators when the Mode is triggered by the separation, by ground commands or by an ACMS computer reset
- A set of sensors/actuators (including thrusters) which are not used in any other modes when the Sun Acq Mode is triggered by ACMS System alarms or by an ACMS computer switchover. This set is named “Survival Set”

*

Reference **GEF-149-C**

The Survival Set of sensors/actuators which may be used in Sun Acq Mode shall be modifiable by ground TC’s.

*

Reference **GEF-158-C**

In Sun Acq Mode, the units which are not involved in the Mode operation shall be turned OFF by default.

*

Reference **GEF-040-C**

In Sun Acq Mode, Instruments shall be put in a safe mode following a sequence defined by each instrument

*

Reference **GEF-131-C**

When the spacecraft switches to Sun Acq Mode upon ACMS System alarm triggering, subsequent alarms conditions shall be properly handled to avoid repetitive re-triggering of the S/C Sun Acq Mode.

*

Reference **CDF-001-C**

When the Sun Acquisition Mode is reached at separation from the Launcher, communication with Earth for TC shall be performed using omni-directional coverage provided by the LGA. By default, the TC Nominal rate (4kbps) shall be used.

*

Indeed, up to distance of 350000 km, although the angle between Earth and Sun seen from the spacecraft can be high, the link is favorable, and permits the use of the Nominal TC rate. In that case, if the spacecraft is Sun pointed, communication is ensured by the antennas covering the - Z hemisphere on Herschel and the + X hemisphere on Planck.

Reference **CDF-008-C**

When the Sun Acquisition Mode is reached from any condition apart from separation from the Launcher, communication with Earth for TC shall be performed using omni-directional coverage provided by the LGA. By default, the TC low rate (125bps) shall be used.

*

In Sun Acquisition, after separation from the launcher, the TM link budget permits to download at 5 kbps with both New Norcia and Kourou.

Reference **GEF-014-C**

In Sun Acquisition, the spacecraft real time HK rate shall be kept low enough (4kbps max) such that progressive download of the HK data stored during launch can be performed, upon ground request, when the Sun Acq Mode is reached after separation from the launcher.

*

Reference **GEF-150-C**

In Sun Acq Mode, the downlink TM rate shall be the Low1 rate (500bps) and use the omni directional antennae. Exception is when the Sun Acq Mode is engaged upon separation from the Launcher ; in that case the TM shall be set to Low2 (5kbps).

*

Reference **INF-002-C**

In this Sun Acquisition mode, the payload instruments shall be :

- OFF except power to the HFI 4K cooler for launch lock if the Mode is entered at separation from the Launcher
- In standby or OFF if the Mode is entered from the other events

*

Reference **GEF-015-C**

Deleted (superseded by GEF-020-C)

*

2.3.1.4 Maintenance Mode

The maintenance mode is suppressed.

Reference **GEF-016-C**

Deleted

*

2.3.1.5 Nominal mode

Reference **GEF-019-C**

Nominal mode shall be the spacecraft mode of operation during platform commissioning and performance verification phases and during scientific mission

*

Reference **GEF-020-C**

Transition to Nominal mode shall be performed from Sun Acquisition Mode or Earth Acquisition Mode only upon telecommand.

*

Reference **GEF-025-C**

Nominal Mode shall be used to validate proper functioning of the satellite and payload and to operate the spacecraft during science observation.

*

Reference **GEF-017-C**

Deleted.

*

Reference **ACF-001-C**

Nominal mode shall allow transition to an operational pointing mode under ground or MTL control.

*

Reference **GEF-018-C**

Deleted

*

Reference **ACF-002-C**

Deleted

*

Reference **GEF-170-C**

It shall be possible to use ACMS Nominal (SCM and HCM for Planck) and Orbit Control Modes in Satellite Nominal Mode.

*

In particular, it is possible to perform orbit control manoeuvres required at the beginning of mission and during science operation.

Reference **CDF-002-C**

It shall be possible to use the following CDMS modes in Satellite Nominal mode[2] :

- TTR in Full mode
- PM Off, PM Init, PM ASW & BSW Init , PM Standby for the non active computer
- PM Nominal Operation for the active computer
- MM nominal
- I/O System ON

*

Reference **INF-005-C**

It shall be possible to operate all (or a subset of) Payload and Instruments modes in Satellite Nominal mode.

*

Reference **INF-003-C**

The instruments shall be individually powered ON by ground TC or MTL service and set to a safe mode (e.g. instrument safe mode), following procedures defined in the relevant IIDBs (AD5 to 9) and using services from the PS-ICD (AD2).

*

Reference **GEF-024-C**

[P:SCI-PT-RS-05991 - Ch.4#4.3.2.1-MOOM-100 H
[P:SCI-PT-RS-05991 - Ch.4#4.3.2.2-MOOM-130 P

Line of sight calibrations shall be conducted in Nominal Mode

*

It will consist in measuring the relative angles between instruments line of sight with respect to the attitude reference sensors, or to calibrate attitude sensors between them. On Planck, line of sight calibration will be performed by observing sources in the instrument detectors.

[2] CDMS modes are described in section 2.3.2.2

Reference **CDF-003-C**

It shall be possible to use all TM/TC modes[3] in Satellite Nominal Mode. Default TTC mode shall be :

- TM : on MGA at Medium rate
- TC : on MGA at Nominal rate

*

Communication nominally uses the MGA for high rate telemetry.

Telecommanding nominally uses the MGA (in the Planck –X axis and Herschel +Z spacecraft axis) with the LGA (-X/+Z) kept in back-up, ie connected to the redundant TC path. This permits to have the nominal TC rate (4kbps) available from both New Norcia and Kourou ground stations.

Reference **PCF-002-C**

It shall be possible to use all Power Control Subsystem modes[4] in Satellite Nominal mode. Default shall be SA mode.

*

Reference **TCF-001-C**

It shall be possible to use all Thermal Control Subsystem modes in Satellite Nominal mode.

*

During non visibility periods, in Nominal Mode, Herschel spacecraft will nominally be in operational pointing mode, 3-axis stabilized.

During non visibility periods, in Nominal Mode , Planck will nominally remain in operational pointing mode with the spin axis oriented in the Sun direction. Spin axis re-orientation manoeuvres are periodically commanded in order to maintain the S/C Sun pointed.

Reference **CDF-004-C**

During Nominal Mode, all Housekeeping and science data from the instruments (if switched ON) and housekeeping from the spacecraft shall be stored in the mass memory.

*

Reference **GEF-021-C**

It shall be possible to perform transition from Nominal modes to Sun Acquisition Mode or Earth Pointing Mode upon telecommand.

*

[3] TM/TC modes are described in section 2.3.2.3

[4] PCS modes are described in section 2.3.2.4

Reference **GEF-022-C**

– deleted

*

Reference **GEF-023-C**

deleted

*

Reference **GEF-026-C**

During Nominal mode, the operations on both Herschel and Planck shall follow the commands defined by the on-board Mission TimeLine service defined in section 2.2.2.2.

*

On Herschel, the science observations will consist in a succession of slew and fixed pointing. Complex TC (observation) sequences will be executed from subschedules of the MTL without ground contact. These observation modes, executed from the MTL are typically :

– Raster pointing with or without OFF position

– Position switching

– Nodding.

In addition, a scanning mode is also specified for Herschel. It is used for Line scanning with or without OFF position.

Similarly, orbit control manoeuvres can be programmed in the timeline and performed without ground link.

– The Herschel scientific observation is basically performed by one instrument, which is in Prime mode while the other instruments are in standby (or Safe Mode for PACS). There are two other possible operational modes for the payload :

  - SPIRE in Prime mode, PACS in parallel[5] mode performing photometer observations with a degraded sensitivity and spatial resolution. HIFI is in standby mode.
  - During slew, HIFI is in standby and PACS in Safe Mode [6]. SPIRE can perform useful observations with its photometer in the so-called “serendipity” mode.

The following table summarises the Herschel payload modes.

MODE	HIFI	PACS	SPIRE
# 1	**Prime**	Safe	Standby
# 2S	Standby	**Prime (Spectrometer)**	Standby
# 2P	Standby	**Prime (Photometer)**	Standby
# 3S	Standby	Safe	**Prime (Spectrometer)**

[5] *Parallel Mode* : Parallel means PACS is operated simultaneously with SPIRE. This could allow more efficient large-scale multi-band mapping.

[6] *Standby* mode is characterized by the fact that no science data is produced by the Instruments (only HK)

# 3P	Standby	Safe	**Prime (Photometer)**
# 4	Standby	**Prime (Photometer)**	Parallel (Photometer)
#5	Standby	Safe	Serendipity (Photometer)

– On Planck, the basic operational mode is based on parallel operation of HFI and LFI. Alternative modes exist with one of the experiment in Prime mode and the other in standby mode, as shown in the following table.

MODE	HFI	LFI
1	Prime	Prime
2	Prime	Standby
3	Standby	Prime

The instruments are constantly scanning the celestial sphere and the spin axis direction is adapted regularly to follow the Planck scanning law at up to 10 deg. from the Sun, as defined in the on-board mission timeline.

Reference **GEF-027-C**

deleted

*

Reference **CDF-005-C**

Deleted.

*

Reference **GEF-028-C**

[P:SCI-PT-RS-05991 - Ch.4#4.2.7-MISS-130 H

During Nominal mode, when ground link is available, the spacecraft shall be Earth pointed to download the scientific data stored in the mass memory during the whole duration of the visibility period.

*

Communication nominally uses the MGA for high rate telemetry.

Telecommanding nominally uses the MGA (in the Planck –X axis and Herschel +Z spacecraft axis) with the LGA (-X/+Z) kept in back-up, ie connected to the redundant TC path. This permits to have in nominal, the 4kbps TC rate available from both New Norcia and Kourou ground stations.

Reference **GEF-029-P**

[P:SCI-PT-RS-05991 - Ch.4#4.3.1.4.2-MOOM-095 P

Planck shall allow full scientific observation and telecommunication in parallel.

*

Reference **GEF-030-H**

Herschel shall allow scientific observation and telecommunication in parallel.

*

This is ensured by a ± 15 deg field of view MGA, compatible with the maximum Sun/SpaceCraft/Earth (SSCE) angle during mission.

On Herschel, the scientific observations will be limited to attitude compatible with Earth pointing and compliance with the ACMS sensors constraints. As a MGA field of view of ± 10 deg. has been considered for Herschel, some flexibility exists in Herschel pointing, allowing to perform raster pointing or line scanning (with a limitation in the line length). Scientific data collected during telecommunication mode are either transmitted real time or stored in the mass memory for transmission at the end of the telecommunication period or during a subsequent one.

Reference **GEF-031-H**

Deleted.

*

2.3.1.6 Survival mode

Survival mode is essentially reached in case of major on-board failures (i.e. system failures) detected by the CDMS.

Reference **GEF-032-C**

[P:SCI-PT-RS-07360#2.2.1-AUT-1.
[P:SCI-PT-RS-05991 - Ch.4#4.3.3-MOOM-160 H/P

In survival mode, the spacecraft shall be put in **safe conditions** and it shall be able to survive for at least 7 days without ground contact.

*

Safe conditions are defined from :

- Spacecraft safe state : It is a configuration of ACMS, thermal S/S, Power S/S and communications states, which allow the spacecraft to be safe.
- **and** an instrument state (i.e. OFF).

Reference **GEF-033-C**

[P:SCI-PT-RS-05991 - Ch.4#4.3.3-MOOM-140 H/P

The Spacecraft safe condition shall be defined by :

- the acquisition and maintenance of a safe attitude,
- the acquisition and maintenance of safe power and thermal conditions by minimising the power consumption : all units not used within the Survival Mode shall be turned OFF by default.

*

Reference **GEF-043-C**

As this could result in the loss of a significant mission time (e.g. to bring back the Planck cooling system to the right temperature), spacecraft shall switch to Survival Mode only in case of major power loss.

*

*Reference **ACF-003-C**

Deleted

*

Reference **CDF-006-C**

[P:SCI-PT-RS-05991 - Ch.4#4.3.3-MOOM-145 H/P

Communication with ground in TM and TC during survival mode shall be performed using the LGAs. The TC path shall use the low rate. The TM path shall use the 500bps low rate.

*

Omni-directional coverage is provided by the LGAs which allows to receive TC and send TM in any spacecraft attitude. It is allowed to ensure the omni coverage in TM via consecutive antennae configuration changes.

Reference **GEF-034-C**

Transition to survival mode from any System mode shall only be initiated :

[P:SCI-PT-RS-05991 - Ch.4#4.3.3-MOOM-155 H/P

– From a ground command

[P:SCI-PT-RS-05991 - Ch.4#4.3.3-MOOM-135 H/P

– After a major on-board failure detected by CDMS (CDMS level 4, see §3.3.3.1.5)

[P:SCI-PT-RS-05991 - Ch.4#4.3.3-MOOM-135 H/P

– deleted

*

Reference **GEF-035-C**

Survival Mode shall, as much as possible, rely on a set of equipment which are not used in other modes.

Deviations shall be clearly identified and approved by the Prime.

*

Reference **GEF-130-C**

The set of units to be used in S/C Survival Mode shall be modifiable by ground TC's.

*

Reference **GEF-038-C**

– deleted

*

Reference **GEF-036-C**

Deleted.

*

Reference **GEF-037-C**

[P:SCI-PT-RS-05991 - Ch.4#4.3.3-MOOM-155 H/P

The only way to exit from survival mode shall be on ground TC.

**

Reference **GEF-041-C**

– deleted

*

Reference **GEF-039-C**

Deleted

*

Reference **GEF-132-C**

[P:SCI-PT-RS-05991 - Ch.4#4.3.3-MOOM-135 H/P

– Deleted

*

Reference **GEF-042-C**

– deleted

*

#

Reference **GEF-133-C**

When the spacecraft switches to S/C Survival Mode, the alarm inputs able to trigger S/C Survival shall be inhibited.

*

2.3.1.7 Earth Acquisition mode

Earth Acquisition Mode is defined to support failures at the level of the CDMS computer (CDMU) and authorise a fast recovery from ground.

Reference **GEF-151-C**

Transition to Earth Acquisition Mode shall be performed (OR) :

– Upon Telecommand

– Upon CDMS computer failure (level 3a or 3b, see §3.3.3.1.4)

*

Reference **GEF-152-C**

In Earth Acquisition Mode the spacecraft shall be maintained in an Earth pointing attitude using the nominal ACMS set of equipment

*

NB : the above is not an ACMS design requirement and does not ask for an explicit ACMS earth pointing mode. Especially, it is accepted to have the Earth co-ordinates stored and periodically uploaded from ground.

* Reference **GEF-153-C**

The Default TM/TC configurations in EAM shall be:

- communication with ground in TM shall be performed using the MGA
- the TM rate shall be the Medium rate.
- communication with ground in TC shall use the MGA in nominal (LGA in back up)
- the TC rate shall be the Nominal one (4kbps), (125bps in back up on LGA)

*

* Reference **GEF-154-C**

In EAM, instruments shall be turned into a safe (eg. standby) mode (defined by the instruments) or remain OFF.

*

* Reference **GEF-155-C**

The EAM shall be exit upon :

- TC
- ACMS System (ACC level 3 and 4, see §3.3.3.1.4 & 3.3.3.1.5) alarms
- CDMS System alarm

*

Modes transition logic

The mode transition logic is shown on the following figure. The main modes have been defined for Herschel and Planck, allowing to have the same transition logic for the two spacecraft.

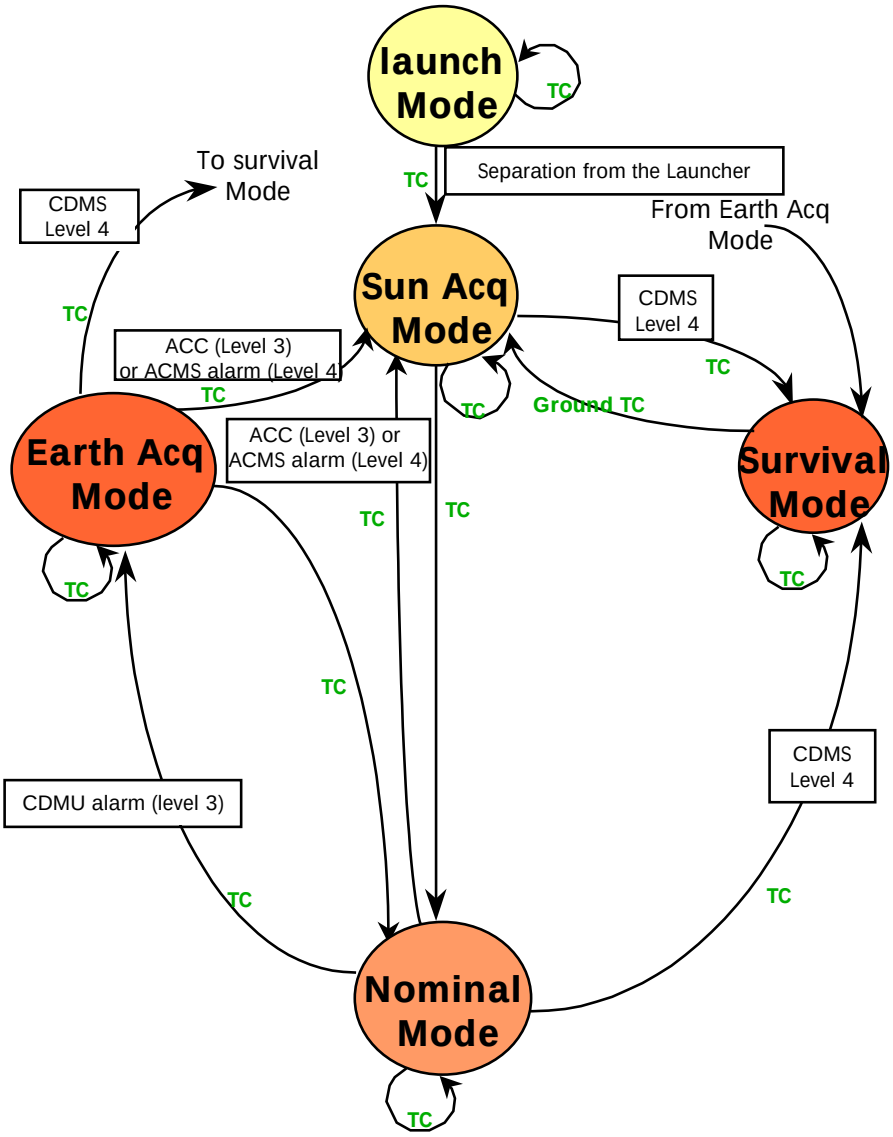

Figure 2.3.2 : Mode Transition logic

2.3.2 Subsystem modes associated to system modes

2.3.2.1 ACMS Modes

2.3.2.1.1 Herschel ACMS Modes

Normal Mode (NOM)

This is the Normal Operation Mode during science activities. It relies on the inertial attitude determination based on an Star Tracker (STR) and gyro (GYR) accurate measurement and fine control of Reaction Wheels. This mode is used to establish the correct initial attitude for orbit correction.

Wheel unloading is a function of this mode.

Sun Acquisition Mode (SAM)

Attitude determination is based on ACMS gyros and Sun acquisition sensors (SAS).

Sun is acquired and maintained along Z axis using thrusters.

Survival Mode (SM)

In case of ACMS system alarms, ACMS is put in Survival mode and relies on an independent set of hardware. 7 days of autonomy are required.

Stand By Mode (SBM)

Stand By mode is the ACMS mode for pre-launch and launch phases. ACC only is running. No control law is implemented.

The Standby mode is also a transition mode after a reconfiguration.

Exit from Stand By Mode can be made to either Sun Acquisition Mode (nominal transition) or Survival Mode (FDIR transition).

Note that 2 standby modes are actually implemented, SBM_Nom and SBM_SM depending on whether the ACC on which the boot is performed is identified as “Nominal” or “Survival”, and corresponding to 2 different init sequences.

Orbit Control Mode (OCM)

The orbit correction are performed on 3-axis Thruster control. STR is nominally used in Delta V mode.

2.3.2.1.2 Planck ACMS Modes

Science Mode (SCM)

This is the routine ACMS mode for scientific operations.

ACMS data are collected to provide the telemetry necessary for the payload data exploitation but also to determine the satellite inertial attitude.

Sun Acquisition Mode (SAM)

SAM is used after launch to acquire and maintain the sun close to X axis. It is based on SAS, QRS and main thrusters.

Stand By Mode (SBM)

Planck Stand By mode is the same as Herschel Stand By mode

Orbit Correction Mode (OCM)

This mode enables to perform the necessary orbit correction.

Survival Mode (SM)

In case of ACMS system alarms, ACMS is put in Survival mode and relies on an independent set of hardware. 7 days of autonomy are required.

Angular Momentum Correction Mode (HCM)

The Angular Momentum Correction mode is used to correct the direction and magnitude of the angular momentum. The Momentum correction is based on on-board STR attitude determination.

2.3.2.2 Herschel & Planck CDMS Modes

The CDMS consists of the following main blocks :

- The TTR, Telemetry Telecommand and Reconfiguration board
- The PM, Processor Module
- The MM, Mass Memory
- The I/O system, In/Out system
- These are supported by the hot and cold power converters
- The OBSW, On-Board Software

2.3.2.2.1 TTR Modes

Off

No FCL power present.

Init

The unit has received power. A hardware power on reset and initialization is performed. The basic TM/TC is initialized. A decision is taken, based on the configuration PROM and the position of the RM Enable/Disable relay, if the RM shall be activated or not.

Basic

In this mode all functions except the RM are fully operational. This includes TC, TM, OBT, SGM.

RM Init

In this mode the RM is initialized. The mode includes a programmable activation delay.

Full

Same as Basic mode with the addition of the RM.

2.3.2.2.2 PM Modes

Off

No LCL power present.

PM Off

The LCL power is present but the PM relay is in its OFF position. The entire cold converter is switched Off which also has impact on the I/O system. The PM relay is latching so it remembers its position even if there is an LCL power cycling.

PM Init

The LCL power is present and the PM relay is on its On position. A hardware power on reset and initialization is performed.

ASW and BSW Init

The BSW then ASW is initialized. This includes the Boot S/W.

Nominal Operation

Both the ASW and the BSW are fully operating.

Standby Operation

Both the ASW and the BSW are fully operating. No access to internal communication buses.

2.3.2.2.3 MM Modes

Off

No FCL power present.

MM Off

The FCL power is present but the MM electronic switch is in its Off position. The MM relay is latching so it remembers its position even if there is a FCL power cycling.

MM Init

The FCL power is present and the MM electronic switch is its On position. A hardware power on reset and initialization is performed.

MM Nominal

The MM is operating under control from the PM. If the SSMM is set ON, the MM returns to MM Init mode

2.3.2.2.4 I/O SYSTEM Modes

Off

Both cold converters are switched Off. Could also be that both LCL power lines are Off.

I/O SYSTEM On

All I/O groups are operating and accessible from any of the PMs. This mode is entered as long as at least one of the cold converters are On. Note that the cold converters are controlled by the PM On/Off commands.

2.3.2.3 TM/TC Modes

2.3.2.3.1 TM Modes

		Antenna	Ground Station	Herschel	Planck	TM modes
TM Hi-rate		MGA	New Norcia	1.5 Mbps	1.5 Mbps	Real time HK Real time science Dump S/C & Science HK Dump Science
TM medium-rate		MGA	New Norcia/ Kourou	150 kbps	150 kbps	Real time Science Real time HK Dump S/C & Science HK.
TM low-rate	Low 2	LGA	New Norcia	5 kbps	5 kbps	Real time essential HK + 1kbps of stored HK
	Low 1		Kourou	500 bps	500 bps	Real time essential subsampled HK

2.3.2.3.2 TC Modes

The various TC mode are summarized in the following table; they are identical for Herschel and Planck.

	S/C ANTENNA	GROUND STATION	DATA RATE	REMARKS
TC low rate	LGA	Kourou	125 bps	
TC nominal	LGA or MGA	New Norcia	4 kbps	

2.3.2.4 PCS Modes

SA Mode

The SA mode is the configuration of the PCS using the Solar Array to get the power.

Battery Discharge Mode

The Battery discharge mode is the configuration of the PCS using the Battery to support spacecraft power generation, possibly as a complement to SA.

Battery Charge Mode

This is the configuration during which part of the SA power is used to recharge the battery.

2.3.2.5 TCS Modes

2.3.2.5.1 Nominal TCS Mode

The overall active thermal control is performed by the CDMS software using heaters power generated by the PCS.

2.3.2.5.2 Survival TCS Mode

The thermal control of the spacecraft relies on thermostats and applies only to critical units (eg. the battery)

2.3.3 Modes links

The following table summarizes the **Herschel** operational modes. For each of them, the TM/TC mode is driven by the downlink rate and the virtual channels allocation and prioritization. It shall be pointed out that the table here below specifies the status at entry or re-entry into the mode. It shall remain possible, via subsequent relevant telecommand, to individually change each of the subsystem and functional mode while in any of the S/C mode.

Spacecraft Mode	TTC mode		MTL Mode	ACMS Mode	EPS Mode	Instruments Mode
	Antennae Configuration : Nominal branch (*backup branch*)	TM/TC Configuration				
Launch Mode	Rx : LGA +Z (*MGA*)	Low rate	Disabled	SBM	Battery Discharge	OFF
	Tx : LGA +Z	OFF				
Sun Acquisition Mode	Rx : LGA +Z (*LGA –Z* when initiated by separation) (*MGA* otherwise)	Low rate (Nominal rate after separation)	Disabled	SAM or SM	Battery Charge or SA	OFF or Standby
	Tx : LGA +Z	Low2 Rate (5kbps) when initiated by separation Low1 Rate (500bps) otherwise				
Nominal Mode	Rx : MGA (*LGA+Z*)	Nominal rate	Enabled	NOM,OCM	BatteryCharge /discharge or SA	OFF, standby or Science
	Tx : MGA	Medium Bit Rate (transition to High Bit Rate by TC)				

Earth Acquisition Mode	- Rx MGA (*LGA+Z*)	Nominal rate	Disabled	NOM	Battery Charge/discharge or SA	OFF or Standby
	- Tx MGA	Medium Bit Rate				
Survival Mode	- Rx : LGA+Z (*LGA-Z*)	Low rate	Disabled	SAM, SM	Battery Charge/discharge or SA	OFF
	- Tx : LGA+Z	Low1 rate (500bps)				

NOM : Normal Mode – SAM : Sun Acquisition Mode – SM : Survival Mode – SBM : Stand By Mode – OCM : Orbit Correction Mode

Figure 2.3.3 : Herschel Modes links and transitions

The following table summarizes the **Planck** operational modes. For each of them, the TM/TC mode is driven by the downlink rate and the virtual channels allocation and prioritization. It shall be pointed out that the table here below specifies the status at entry or re-entry into the mode. It shall remain possible, via subsequent relevant telecommand, to individually change each of the subsystem and functional mode while in any of the S/C mode.

Spacecraft Mode	TTC mode		MTL Mode	ACMS Mode	EPS Mode	Instruments Mode
	Antennae Configuration : Nominal branch (*backup branch*)	**TM/TC Configuration**				
Launch Mode	Rx : LGA -X (*MGA*)	Low rate	Disabled	SBM	Battery Discharge	OFF except 4K cooler in Launch Lock
	Tx : LGA -X	OFF				
Sun Acquisition Mode	Rx : LGA -X (*LGA –Z/+Z* when initiated by separation) (*MGA* otherwise)	Low rate (Nominal rate after separation)	Disabled	SAM or SM	Battery Charge or SA	OFF or Standby
	Tx : LGA -X	Low2 Rate (5kbps) when initiated by separation Low1 Rate (500bps) otherwise				
Nominal Mode	Rx : MGA (*LGA -X*)	Nominal rate	Enabled	SCM, HCM, OCM	BatteryCharge/ discharge or SA	OFF, standby or Science
	Tx : MGA	Medium Bit rate (transition to High Bit Rate by TC)				

Earth Acquisition Mode	- Rx: MGA (*LGA -X*)	Nominal rate	Disabled	OCM, HCM, SAM	Battery Charge/discharge or SA	OFF or Standby
	- Tx: MGA	Medium rate				
Survival Mode	- Rx : LGA -X (*LGA +Z/-Z*)	Low rate	Disabled	SAM, SM, OCM, HCM	Battery Charge/discharge or SA	OFF
	- Tx : LGA -X	Low rate (500bps)				

SCM : Science Mode – SAM : Sun Acquisition Mode – SM : Survival Mode – SBM : Stand By Mode – OCM : Orbit Correction Mode – HCM : Angular Momentum Correction Mode

Figure 2.3.4 : Planck Modes links and transitions

3. FDIR

3.1 Scope

The Failure Detection Isolation and Recovery (FDIR) process is related to the operational concept, as it is in charge of the autonomous failure management.

Herschel and Planck spacecraft's FDIR concept has been elaborated around :

- FDIR Objectives
- Operational constraints
- Functional analysis of the spacecraft

As the daily Telecommunication period is about **3 hours per day** for each spacecraft, on-board process have to be designed and implemented to react autonomously against potential failures.

FDIR has been elaborated, doing the distinguish between two main goals :

- Required FDIR to guarantee the satellite survival. In case of major anomaly only, the spacecraft will be put in safe conditions to survive **at least 7 days** without ground contact.
- Required FDIR to ensure the autonomy along the whole mission. Operation have to be guaranteed without ground contact for **48 hours**

3.2 FDIR Drivers and High Level Requirements

Spacecraft FDIR is defined according to the following system objectives :

Reference **GEF-044-C**

[P:SCI-PT-RS-05991 - Ch.4#4.5-MOFM-010 H/P
[P:SCI-PT-RS-05991 - Ch.4#4.5-MOFM-050 H/P

Satellite survival shall be ensured for any single failure.

*

Reference **GEF-045-C**

[P:SCI-PT-RS-07360#2.2.1-AUT-1.

Satellite mission shall be maintained without ground contact for any 48 hours period during the operational life, assuming no major failure condition.

*

Nota : Mission has to be maintained as far as possible on the main cases of the single failures.

Reference **GEF-186-C**

In case of no ground contact for a period greater than 60hrs, the spacecraft shall initiate a periodical toggling of the TT&C equipment.

*

The purpose of this toggling is to give a chance to re-establish the contact with ground by using all possible TT&C paths.

Reference **GEF-046-C**

[P:SCI-PT-RS-05991 - Ch.4#4.3.3-MOOM-160 H/P

The spacecraft shall survive without ground contact for any 1 week period during the operational life

*

Reference **GEF-047-C**

Satellite resources shall be economised.

*

Nota : For example, fuel consumption has to be optimised, Herschel cryostat Helium has to be preserved, and reconfiguration and equipment loss have to be minimised.

Reference **GEF-048-C**

[P:SCI-PT-RS-07360#2.2.1-AUT-3.
[P:SCI-PT-RS-05991 - Ch.4#4.5-MOFM-005 H/P

The FDIR process shall provide means to :

– Detect failure of any equipment which can induce satellite loss, mission interrupt or performance degradation.

*

Reference **GEF-049-C**

[P:SCI-PT-RS-05991 - Ch.4#4.5-MOFM-045 H/P

The FDIR shall provide means to :

– Isolate and recover failure by switching over the satellite equipment from a failed configuration to a back up configuration

*

Reference **GEF-050-C**

[P:SCI-PT-RS-05991 - Ch.4#4.5-MOFM-045 H/P

The FDIR process shall provide means to :

– Continue the mission when satellite integrity is not endangered

*

Reference **GEF-051-C**

[P:SCI-PT-RS-05991 - Ch.4#4.5-MOFM-045 H/P

The FDIR process shall provide means to :

– Enter satellite in a survival mode or safe mode depending on the failure and mission phase

*

Reference **GEF-052-C**

The FDIR shall provide means to :

– Maintain the current spacecraft configuration in a context memory.

*

Reference **GEF-134-C**

The context memory storing the Survival Mode Context is called “Survival Context”. The Survival Context update shall only be made from, or authorised by, the Ground. As far as ACMS is concerned, “Ground” is to be understood as “external to ACMS”.

*

Reference **GEF-118-C**

Suitable mechanisms shall protect the Survival Context from being corrupted in case of single failure in flight. In this particular case, any software failure shall be considered as a result of single failure.

*

In the same manner,

Reference **GEF-183-C**

Suitable mechanisms shall prevent the software from corrupting the registers and relays involved in the levels 3 & 4 alarms processing.

*

Reference **GEF-054-C**

[P:SCI-PT-RS-07360#2.2.1-AUT-22.

The context memory storing the current configuration is called “SafeGuard Memory” (SGM). Any reconfiguration shall be reflected by an update of the SGM.

*

Reference **GEF-053-C**

[P:SCI-PT-RS-05991 - Ch.4#4.5-MOFM-075 H/P
[P:SCI-PT-RS-05991 - Ch.4#4.5-MOFM-120 H/P

Any identified failure shall be suitably reported in Telemetry

*

3.3 FDIR concept

Herschel and Planck share a number of commonalties (orbit in L2, use of common ground stations, common design for electrical subsystem, identical data rates to ground…), which will lead to reduction of the operational costs by allowing the use of the same FDIR principle for both spacecraft.

3.3.1 General

As the consequence of the main FDIR requirements, The FDIR strategy is based upon a layers breakdown. Each levels is defined according to :

- The severity of the failure
- The functions involved on the failure detection (H/W or S/W)

In addition to this, the levels have to be managed together in a hierarchical way, each level being identified by its functional application. The highest level is called System level.

It will be then necessary to mark the boundaries of each range of influence by the use of, for example, threshold or timeout.

The present section will provide a description of each level with its associated strategy.

3.3.2 Vital Functions

Generally, FDIR is focused on the vital spacecraft functions listed below :

- The Spacecraft Monitoring and Control function.
- The Spacecraft Positioning function. The function also includes the propulsion management.
- The Power Supply function, which is performed by the PCDU and monitored by the CDMS.
- The Thermal Monitoring and Control function, which is under CDMS control.
- The Payload Management function, which is managed by the CDMS.

3.3.3 Failure Classification

3.3.3.1 Failure classification concept

According to potential effects on equipment units, function, computers (CDMU and ACC) or system performance, several failure levels have been defined.

The different levels are detailed in the following sections, while the overall breakdown is summarized in Table 3.3.1 and illustrated in Figure 3.3.2.

Level 4	Level 3	Level 2	Level 1	Level 0
SYSTEM	ACC	Spacecraft positioning function	Eqpt 1 Eqpt 2 Eqpt 3	
	CDMU	Thermal monitoring and control function	Eqpt 1 Eqpt 2 Eqpt 3	
		Power supply function	Eqpt 1 Eqpt 2 Eqpt 3	
		Spacecraft monitoring and control function	Eqpt 1 Eqpt 2 Eqpt 3	
			Eqpt 1 Eqpt 2 Eqpt 3	
		Payload Management function	Eqpt 1 Eqpt 2 Eqpt 3	

Figure 3.3.1 : Failure classification

Reference **GEF-055-C**

[P:SCI-PT-RS-07360#2.2.1-AUT-9.
[P:SCI-PT-RS-05991 - Ch.4#4.5-MOFM-090 H/P

Failure levels shall be split up into **5 main levels** (Level 0 to Level 4) characterized by :

– The failure **severity**

– The **recovery** sequence

– Functions involved in the **detection** (H/W or S/W functions)

*

3.3.3.1.1 Level 0

Reference **GEF-056-C**

[P:SCI-PT-RS-05991 - Ch.6#6.5.3-SMPC-152 H/P

Level 0 failure shall be associated to an internal single failure in one equipment unit (including ACC, CDMU and PCDU) which can be automatically recovered by the unit itself without any impact on the rest of the system (H/W devices or S/W applications).

*

Level 0 failures are typically :

EDAC single bit error. EDAC device can detect and correct one bit flip in data read from RAM memory. There is no impact in data reading operation when the corrupted data in RAM is re-written locally in a background function

Level 0 failures and their handling are typically described in the units FMECA.

Reference **GEF-057-C**

Level 0 failure single occurrence shall have no impact on the mission.

*

Reference **GEF-119-C**

Detected level 0 failures shall be reported to the higher level.

*

Reference **GEF-058-C**

Deleted.

*

Multiple (number selectable by ground) occurrences of Level 0 failure may lead to higher level recovery actions (unit / coupler / computer reconfiguration).

3.3.3.1.2 Level 1

A **level 1** failure is a failure, as seen by the ACMS computer (ACC) or the Data handling one (CDMU), in a unit connected to either computer via the data bus (1553 bus), or dedicated acquisition lines and which can not be

autonomously recovered by the unit itself. The surveillance of the unit is performed by the appropriate ACMS S/W or CDMS S/W via simple health check, and recovery actions are ordered by the same software.

Reference **GEF-059-C**

[P:SCI-PT-RS-05991 - Ch.5#5.3.4-SPER-100 H/P

The status of each equipment unit shall be monitored by the CDMS S/W or the ACMS S/W depending on the unit. This status shall be compared to unambiguous expected values to possibly initiate recovery actions.

*

Reference **GEF-060-C**

In case of level 1 failure, the ACMS or the CDMS, depending on the failed equipment unit, shall provide the necessary actions to recover from the detected failure.

*

Reference **GEF-061-C**

Two sub levels shall be considered, depending on the failure origin :

- Level 1a for unit failures
- Level 1b for communication unit failures

*

Level 1a relates to failure which can be attributed to the unit level :

- ACMS sensors,
- ACMS actuators,
- PCDU,
- TTC transponders,
- CCU for Herschel,
- TWTA,
- Thermal Control Equipment.
- Instruments

Reference **GEF-062-C**

[P:SCI-PT-RS-05991 - Ch.5#5.3.4-SPER-100 H/P

A failure detected by the ACC or CDMU software application shall be classified as a Level 1a failure when it does not imply more than one equipment unit. The failure detection shall be based on unit specific health data and operational parameters.

*

Reference **GEF-063-C**

Any ACMS unit reconfiguration action shall be reported to the CDMS, with the past and current unit contexts.

*

Level 1b relates to failures at communication units level, and as such can be considered as multi-application related.

Reference **GEF-064-C**

[P:SCI-PT-RS-05991 - Ch.5#5.3.4-SPER-100 H/P

Every bus coupler shall be checked by the mean of :

- Specific internal health status depending on coupler design,
- 1553 protocol errors including I/O timeouts.

*

As described in Annex 1, the MIL Bus FDIR has the capability to manage the bus redundancy switch-over. This function collects the data necessary to monitor the status of the communications on the bus, isolates bus medium failure, and performs an automatic reconfiguration of the bus.

Reference **GEF-065-C**

CDMS 1553 bus FDIR shall be implemented as described in Annex 1.

*

3.3.3.1.3 Level 2

A **level 2** failure is related to an anomaly of one of the 5 satellite functions. The objective is to detect failures which have not / cannot be flagged at Level 1 by simple unit / communication health check, and, if possible, to process them before they may turn into a more severe (i.e. more mission impacting) system alarm.

Reference **GEF-066-C**

[P:SCI-PT-RS-05991 - Ch.5#5.3.4-SPER-100 H/P

For each function, depending on the current System mode, observed performances shall be compared to non ambiguous expected value and in case of failure a recovery strategy shall be engaged.

*

The level 2 failure detection and recovery are performed, depending on the function implicated in, by either the two CDMS or ACMS on-board Software.

Reference **GEF-067-C**

In case of level 2 failure, the ACMS S/W or the CDMS S/W, depending on the failed function, shall provide the necessary actions to recover from the detected failure.

*

3.3.3.1.4 Level 3

A level 3 failure is considered as an internal computer unit (CDMU or ACC) failure, more severe than Level 0, such that the computer unit cannot neutralize it autonomously.

Reference **GEF-068-C**

[P:SCI-PT-RS-05991 - Ch.5#5.3.4-SPER-100 H/P
[P:SCI-PT-RS-05991 - Ch.6#6.12.2-SMSW-105 H/P

FDIR Level 3 corresponding errors shall be detected either by Hardware or Software while the recovery is performed by H/W, via the relevant reconfiguration module (i.e. CDM_RM or the ACC_RM).

*

Level 3 failures are typically :

- PM bus error, detected by H/W
- Memory protection violation, detected by H/W
- Any hardware watchdog
- CPU instruction error, detected by S/W

The first occurrence of these alarms corresponds to the **Level 3a**, and the second occurrence to the **Level 3b**.

Reference **GEF-069-C**

Depending on the computer alarm sub-level (3a or 3b), the reconfiguration sequence shall be different (reset for a 3a alarm or switch to the redundant unit for a 3b alarm).

*

3.3.3.1.5 Level 4

A level 4 failure is defined as a major on-board failure, which has not been able to be detected or recovered by lower level FDIR procedures.

Reference **GEF-070-C**

[P:SCI-PT-RS-05991 - Ch.5#5.3.4-SPER-100 H/P

The failure which induces global system malfunction and which detection time is inconsistent with the spacecraft safety shall be detected by system alarms independent from software.

*

The following table lists the minimum failure cases to be detected and recovered by FDIR at system level (via reconfiguration or change to safe mode). Those potential failures result from an analysis describing system feared events considered for each operational satellite life phase.

Function	Potential failure
Spacecraft positioning and control function (including propulsion management)	Sun out of specified angles
	Excessive angular velocity
Power supply function	Bus undervoltage
	Power loss

From this list of system feared events, 3 system alarms have been considered. Retained alarms are at a minimum :

- Loss of proper Sun Pointing (**SP**)
- Depth of Discharge (**DOD**)
- Rate Anomaly (**RA**)

SP and RA alarms are handled by the ACC_RM.

DOD alarm is handled by the CDM_RM.

Reference **GEF-071-C**

[P:SCI-PT-RS-05991 - Ch.6#6.9.2-SMAC-075 H/P

At a minimum SP, RA, DOD system alarms shall be implemented. Any deviation from this shall be fully justified.

*

It has to be pointed out that the failures ultimately leading to the listed alarms may be first processed by lower level reconfigurations.

Reference **GEF-072-C**

[P:SCI-PT-RS-05991 - Ch.5#5.3.4-SPER-100 H/P

Each level 4 failure shall be detected by dedicated hardware means and directly hardwired to the relevant reconfiguration module (ACC_RM or CDM_RM).

*

Reference **GEF-185-C**

No level 4 alarm shall be triggered in case of transient spurious or single event.

*

Reference **GEF-073-C**

When a level 4 alarm is activated on ACC, it shall be instantaneously taken into account and satellite shall directly go to Sun Acq Mode with ACMS in SM using the “survival set” of equipment and the redundant ACC Processor Module.

*

Reference **GEF-117-C**

When a level 4 alarm is activated on CDMU, it shall be instantaneously taken into account and satellite shall directly go to S/C Survival Mode.

*

Reference **GEF-074-C**

Level 4 recovery action shall be initiated by the proper reconfiguration module (CDM_RM or ACC_RM).

*

3.3.3.2 Application of the failure classification to the SVM system

Failure Level	Failed Unit of function	Detection principle
0	All	N/A
1a	Equipment failure	Detected by OBSW Acquisition of the health status and critical parameters
1b	Communication interfaces failure	Detected by OBSW Communication protocol and bus couplers monitoring
2	Vital satellite function performance anomaly Main function failure	Detected by OBSW Function performance monitoring
3a	CDMU or ACC failure ***First occurrence***	Nominal processor module H/W alarm or S/W watch dog
3b	CDMU or ACC failure ***Second occurrence***	Nominal processor module H/W alarm or S/W watch dog
4	Global satellite malfunction	System alarms

Figure 3.3.2: Failure classification synthesis

3.3.4 Failure classification implementation

As seen in the previous chapter, the FDIR concept has been defined by classifying failures into 5 distinguished levels. It aims to recover each failure case by the most adapted method (switch to the redundant equipment, subsystem reconfiguration, system reconfiguration… depending on the failure impact).

This section presents the failure classification implementation in Herschel/Planck spacecraft. It also provides figures to clarify the relationship between the functional architecture of the system and the FDIR concept.

First, failure classification and functional levels will be analyzed and compared.

Then, in a second time the Failure classification implementation will be presented on a graphical form. It aims to visualize the way that the FDIR will act on the whole spacecraft.

3.3.4.1 Failure classification and functional levels

FDIR concept previously described (failure classification in 5 levels) has been considered to fit with the FDIR Higher level requirements.

The principle is to elaborate a FDIR strategy based on 5 independent levels of detection. Nevertheless these 5 levels are linked together to ensure a cohesion between levels. Non-recovered lower alarms have to be supervised by higher alarm activation.

The ordering of the failures via 5 levels permits “scaled” recoveries.

Each FDIR level is in charge of one or part of a functional level :

Functional Levels	FDIR Levels
System level	Level 4 (system)
Functional Subsystem level	Level 2 (function)
Equipment level	Level 0 (internal equipment)
	Level 1 (equipment unit)
	Level 3 (computer unit)

System and functional subsystem levels have their homonymous FDIR levels.

The functional Equipment level is treated through 3 FDIR levels :

- The FDIR level 0 concerns the internal failures of the equipment unit. The functional analysis doesn’t make appear this level of detail.
- The FDIR level 1 concerns the failures of the equipment unit itself.
- The FDIR level 3 concerns the failures of specific equipment units, the computers. Indeed, a failure on a computer could have severe impact on the rest of the system (e.g. on function management, on satellite control…). This is the reason why computer failures have to be treated in a specific FDIR level (i.e. FDIR level 3).

It can also be presented on a graph form, as shown in figure 3.3.3.

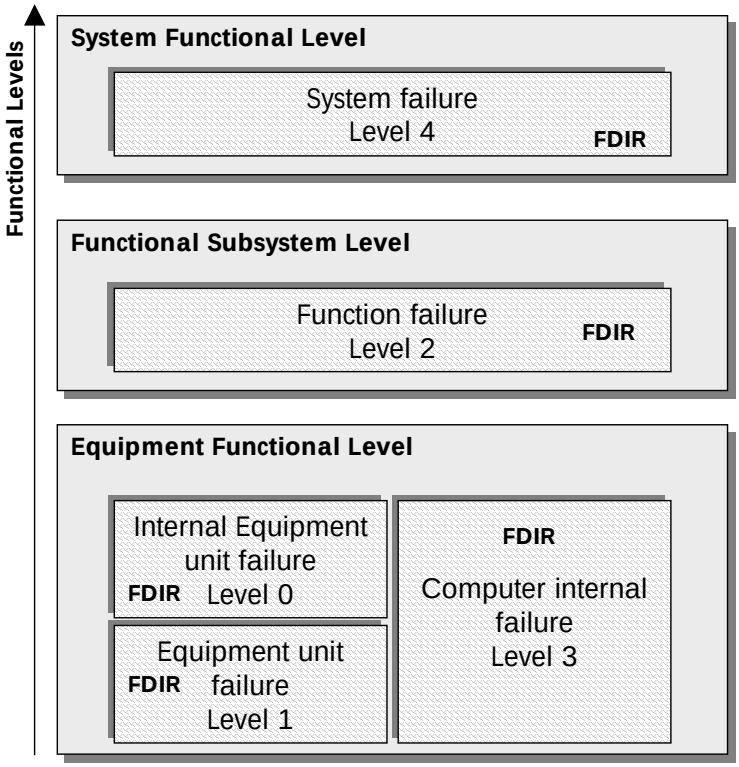

Figure 3.3.3 : FDIR levels and associated functional description

3.3.4.2 Failure classification implementation : graphical view

From this FDIR concept based on 5 detection levels, the Failure classification implementation can be represented by 5 independent boxes.

Each box is associated to an FDIR level and symbolizes the associated FDIR task :

- Inputs of the box are the alarms and configuration parameters (i.e. FDIR mode)
- Outputs of the box are the FDIR actions to carry out on the system.

The figure 3.3.4 illustrates the generic FDIR implementation. It gives a global view of the action of the FDIR on the system.

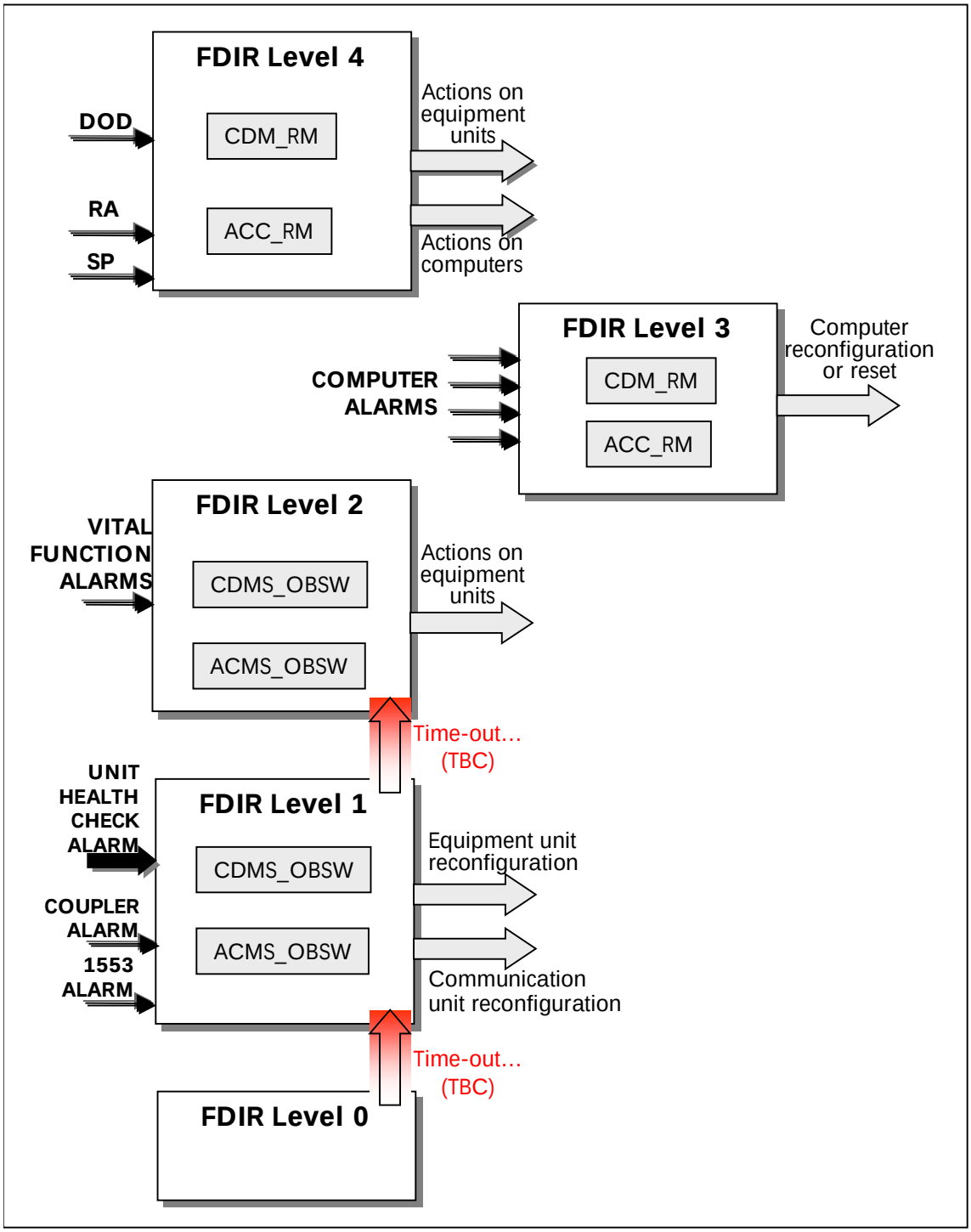

Figure 3.3.4 : FDIR Boxes

3.3.5 FDIR Modes

The FDIR concept is organized around two main points :

- The failure classification, which has been exposed in the two last sections (3.3.3. and 3.3.4.).
- The FDIR modes

To fit the mission requirements (e.g. #GEF-045-C and #GEF-046-C) the FDIR concept has been developed in creating two FDIR modes. These modes aim to support the S/C operation.

In fact this has been set up to define two reconfiguration strategies depending on the mission life phase : the method to apply in order to detect, isolate and recover failures is basically dependent on this spacecraft life phase.

Reference **GEF-075-C**

FDIR strategy shall be defined according to the 2 current status of the mission (i.e. satellite is doing scientific observations and acquisitions or not), each one being associated with one of the two FDIR autonomy modes :

- autonomous fail operational (AFO), when the satellite is in nominal scientific observations and acquisitions phase
- autonomous fail safe (AFS), the rest of the time

*

Reference **GEF-079-C**

In AFO or AFS mode, On board time shall be maintained after any single case of failure.

*

Reference **GEF-120-C**

In both Autonomous Fail Operational (AFO) and Autonomous Failed Safe (AFS) Modes, in case of alarm occurrence, sufficient information shall be stored on board to identify the alarm which occurred and recovery actions taken.

*

Each System mode can be associated to one or both of these FDIR autonomy modes.

Reference **GEF-180-C**

Transition from one autonomy mode to the other shall be performed upon telecommand.

*

3.3.5.1 Autonomous Fail Safe (AFS)

This FDIR autonomy mode is required to answer to physical (e.g. possible RF link unavailability…) or operational constraints of the mission. It is typically applicable to the early phases of the Herschel & Planck mission, when the spacecraft subsystems in flight calibration is not done, the scientific observations are not yet entered and the main concern is to preserve the spacecraft safety while minimizing the risks and avoiding erroneous, spurious reconfiguration actions.

The AFS mode basically assumes that the spacecraft in flight status is not sufficiently known to rely on complex reconfiguration strategies.

Reference **GEF-076-C**

In AFS mode, the flight program, uploaded during ground contact, is autonomously executed. On alarm occurrence, the spacecraft safety shall be given more importance than to the mission continuation.

*

The low level failures (i.e. level 0 to 2 failures) are nominally not isolated nor recovered by related FDIR processes, and the spacecraft safety is eventually based on level 4 recovery. However, to increase the robustness of the mission, a limited and well identified set of low level failures isolation and recovery could be authorised.

Reference **GEF-181-C**

The isolation and recovery of low level failures (0 to 2) in AFS mode shall be strictly limited to well identified and agreed cases for which the interest of enabling the recovery shall be demonstrated.

The set of enabled/disabled low level failures isolation and recovery functions in AFS shall be maintained and shall be modifiable by TC.

*

Reference **GEF-077-C**

Deleted

*

Reference **GEF-078-C**

Deleted

*

3.3.5.2 Autonomous Fail Operational (AFO)

This autonomy mode directly answers to the system requirements to maintain the continuity of the mission and performance as long as healthy alternative functional path exists. It essentially applies for both spacecraft, to the scientific observation modes, including the ground communications periods.

Reference **GEF-130-C**

In AFO mode, on level 0 to 2 alarm occurrence, the continuation of the mission shall be favored by suitable elementary recoveries. On level 3 or 4 alarm occurrence, one shall give priority to spacecraft safety over mission continuation.

*

Reference **GEF-081-C**

Deleted.

*

Reference **GEF-082-C**

Deleted.

*

Reference **GEF-083-C**

Deleted.

*

Reference **GEF-084-C**

Deleted.

*

Reference **GEF-085-C**

Deleted.

*

3.3.5.3 Relation between Satellite modes and FDIR modes

A FDIR strategy is applied according to the current satellite mode, this FDIR strategy being defined by an adapted FDIR mode (i.e. AFO or AFS). As stated in GEF-180-C, FDIR modes transition is NOT automatic, and will be commanded by TC.

Reference **GEF-086-C**

For each satellite mode, the corresponding FDIR modes shall be as described in the table hereafter. For each satellite mode, the authorised FDIR Modes are marked by a **X**. The FDIR mode at entry into the satellite mode is marked ❐.

Satellite Modes	AFS	AFO	N/A
Launch Mode	(1)		
Sun Acq Mode	❒ X	X	
Survival Mode	(2)		
Nominal Mode	X	❒ X	
Earth Acq Mode	❒ X	X	

(1) see Req. #GEF-156-C

(2) see Req. #GEF-157-C

Figure 3.3.5 : Relation between satellite et FDIR modes

*

Launch Mode and Survival Mode are specific cases; the reconfiguration strategy associated to these Modes is strongly linked to the satellites configuration.

Reference **GEF-156-C**

In Launch Mode :

- level 3 failures detection and recovery shall be authorised for both CDMU and ACC
- level 4 failures detection shall be disabled both for CDMU and ACC
- all lower level failures shall be detected
- Recovered low level failures shall be limited to the bare minimum necessary to guarantee the spacecraft safety:
  - thermal control failures
  - 1553 Bus Data Link Layer failures
  - internal CDMU and ACC low level failures
  - other failures to be agreed by the Prime

*

Reference **GEF-157-C**

In spacecraft Survival Mode :

CDMS :

- level 3a failures detection and recovery shall be authorised for CDMU.
- Level 3b and 4 failures shall not be recovered
- all lower level failures shall be detected
- Recovered low level failures shall be limited to the bare minimum necessary to guarantee the spacecraft safety:

• thermal control failures
• 1553 Bus Data Link Layer failures
• internal CDMU low level failures
• TTC toggling after ground outage (see GEF-186)
• other failures to be agreed by the Prime

ACMS :

- if ACMS is in Sun Acquisition Mode

• ACMS shall be in AFS

- If ACMS is in Survival Mode

• level 3a failures detection and recovery shall be authorised for ACC
• Level 3b and 4 failures shall not be recovered
• all lower level failures shall be detected
• Recovered low level failures shall be limited to the bare minimum necessary to guarantee the spacecraft safety:

- internal ACC low level failures
- other failures to be agreed by the Prime

*

3.4 FDIR Strategy

As seen in a previous section, FDIR has to be applied to the whole spacecraft including Payload Module (PLM) and instruments.

The adopted strategy is fully developed for the system (SVM + PLM) and a description of the instrument FDIR strategy is also given.

3.4.1 Platform

The requirements declined in the FDIR objectives presentation (§ 3.2.1) strongly suggest a hierarchical failure detection identification and recovery architecture.

It allows to satisfy the top level requirement to have a visible impact on the mission operation, only in case of a major, high level failure, the equipment level failures being possibly processed and recovered autonomously at lower levels.

The association of FDIR modes allows to satisfy the requirements on mission integrity (see #GEF-046-C & #GEF-047-C).

Reference **GEF-087-C**

The failure processing essentially depends on the current System mode, and the reconfiguration actions, in AFO mainly, shall be graduated with regards to failure severity.

*

Reference **GEF-088-C**

Major failures which can endanger the spacecraft security, shall be detected by dedicated hardware alarms and handled independently from on-board software features (by the mean of high level commands issuing).

*

Reference **GEF-089-C**

Each computing subsystem, CDMS and ACMS, shall apply a similar strategy to recover from a single failure:

[P:SCI-PT-RS-05991 - Ch.6#6.12.2-SMSW-110 H/P

- Software monitoring for the surveillance of low level failures, associated to a reconfiguration managed by S/W
- Hardware monitoring for the surveillance of high level failures, then a hardware based reconfiguration.

*

Reference **GEF-090-C**

For the function units and their proper interfaces, software monitoring shall be implemented within one of both computing subsystem (i.e. ACMS and CDMS), depending on their respective control.

*

3.4.1.1 FDIR Repartition between ACMS and CDMS

ACMS Management is carried out by the ACC and the ACMS S/W. In the same way, management of the CDMS is done by the CDMU and the CDMS S/W.

Each function is managed by either the ACMS or the CDMS. This means that they run independently.

Reference **GEF-091-C**

The FDIR function shall be divided into CDMS FDIR part and ACMS FDIR part, with simple interfaces between them.

*

Reference **GED-001-C**

Each FDIR subset (i.e. CDMS FDIR and ACMS FDIR) shall comprise :

- A hardware reconfiguration module with direct hard-wired links from critical units, for alarm inputs. The CDMS reconfiguration module is called CDM_RM, while the ACMS reconfiguration module is called ACC_RM.
- An associated non-volatile safeguard memory (see GEF-054-C), respectively the CDM_SGM for the CDMS safeguard memory, and the ACC_SGM for the ACMS safeguard memory.
- An associated Survival Context write-protected memory (see GEF-134-C).

*

Reference **GED-002-C**

Each hardware reconfiguration module (i.e. ACC_RM and CDM_RM) shall be independently powered from the rest of the Processor Module (respectively the rest of the ACC_PM and the rest of the CDMU_PM)

*

Reference **GEF-092-C**

[P:SCI-PT-RS-05991 - Ch.6#6.12.1-SMSW-065 H/P
[P:SCI-PT-RS-07360#2.2.1-AUT-22.

The context of the satellite shall be kept up to date and saved in the suitable non-volatile safeguard memory (i.e. ACC_SGM or CDM_SGM depending on the considered equipment unit).

*

Reference **CDD-002-C**

The SGM shall be split into two areas A and B in hot redundancy.

*

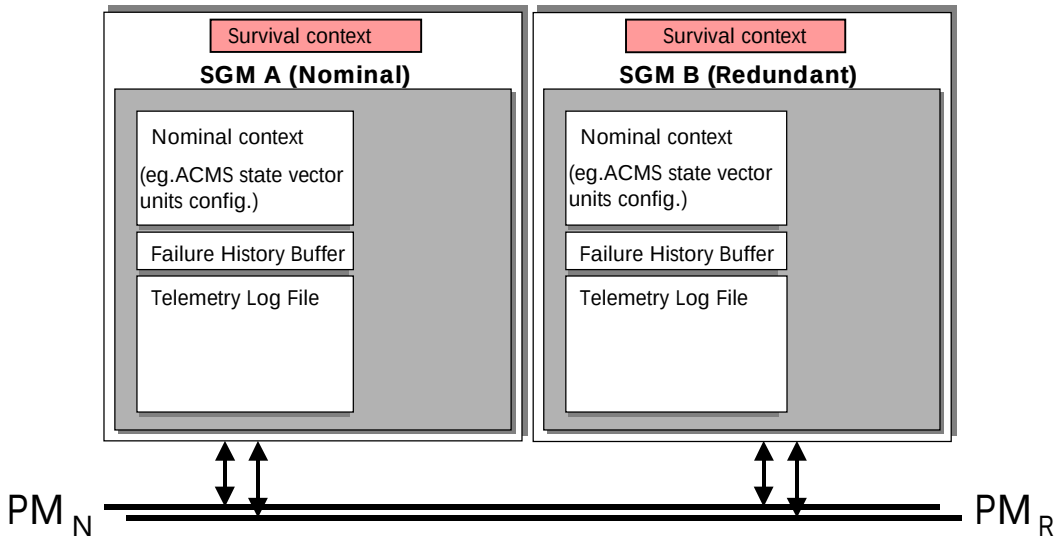

Figure 3.4.1 : Safeguard Memories Breakdown

Reference **GEF-095-C**

[P:SCI-PT-RS-07360#2.2.1-AUT-22.
[P:SCI-PT-RS-07360#2.2.1-AUT-5.

The CDM_SGM and ACC_SGM shall memorize all the system and units configuration necessary to be used for autonomous failure recovery, and to save the failure context.

*

Note that the design of CDMU is such that the Central Time Reference, keeps running in case of computer reconfiguration.

Reference **GEF-099-C**

Configuration to be restarted form after failure shall be the one stored in :

- ACC_SGM for ACMS level failures
- CDM_SGM for CDMS level failures

Exceptions are

- When an ACMS level failure induces a S/C transition to S/C Sun Acq Mode (see Fig. 2.3.2), the configuration to be restarted from shall be the one stored in the ACC_SGM (if the ACMS transitions to SAM) or in the ACC Survival Context memory (if the ACMS transitions to SM)
- When a CDMS level failure induces a S/C transition to S/C Survival Mode (see Fig. 2.3.2), the configuration to be restarted from shall be the one stored in the CDMU Survival Context memory

*

Reference **GEF-093-C**

The CDMS S/W and the ACC S/W shall detect low level alarms (i.e. Levels 1 and 2 alarms).

*

Reference **GEF-094-C**

[P:SCI-PT-RS-05991 - Ch.6#6.7.3-SMCD-140
H/P

the CDM_RM and the ACC_RM shall detect high level alarms in input and order any reconfiguration by means of CPDU telecommand packets issuing High Priority Command called HPC_CDM when originated from the CDM_RM, and HPC_ACC when originated from the ACC_RM.

*

Reference **GEF-096-C**

CDMS FDIR and ACMS FDIR shall communicate via either S/W messages (e.g. events TM packets, TC acceptance report packets) for low level alarms, or H/W signals for high level/system alarms.

*

Reference **GEF-097-C**

[P:SCI-PT-RS-07360#2.2.1-AUT-16.
[P:SCI-PT-RS-05991 - Ch.4#4.5-MOFM-060 H/P

It shall be possible to enable and disable any failure detection, isolation and recovery procedure by ground commands. Agreed exceptions are power distribution, DC/DC converters and over voltage protection. Any other exception has to be identified and agreed by the Prime Contractor. It shall be possible to reverse any FDIR procedure.

*

3.4.1.2 CDMS/ACMS Interface

The CDMS is in charge of the management of the Mission TimeLine and sends dedicated time tagged commands to the ACMS. It is thus necessary to ensure a coherence in the satellite behavior even in case of failure of the CDMS-ACMS communication link.

Additionally, in case of ACC or CDMU reconfiguration, the ACMS or the CDMS respectively is unavailable for a certain time (e.g. reboot/init time).

The following paragraphs address the way these 3 cases are handled from a system point of view : ACMS is not available, CDMS is not available, ACMS-CDMS communication is not available.

It has to be noticed that ACMS and CDMS are considered as unavailable only in case of levels 3 and 4 failures. Analysis and recommendations partly driving the present implementation are detailed in RD7.

3.4.1.2.1 ACMS unavailability

Reference **GED-003-C**

Deleted

*

Reference **GED-004-C**

ACC_RM shall report a status signal to the CDMS, via a reliable and hardware status link called AIR[7], to inform of its unavailability due to an ACMS level 4 alarm or an ACC level 3 alarm.

*

Reference **CDD-004-C**

Deleted.

*

Reference **GED-005-C**

For failure tolerance reason the status link shall be hardware and independent from the nominal ACMS-CDMS communication link.

*

Reference **GED-006-C**

When the AIR signal is raised, spacecraft shall be put in S/C Sun Acquisition Mode.

*

3.4.1.2.2 CDMS unavailability

During the CDMS unavailability, Herschel and Planck spacecraft have to be maintained in a safe mode (see ***#ACF-004-C***), command/control function and Mission Timeline service being temporarily unavailable.

Reference **GEF-098-C**

During CDMS unavailability, the spacecraft shall be put in a safe attitude by the ACMS.

[7] AIR : ACMS in Reconfiguration

*

Reference **GED-006-C**

The ACMS shall be informed about CDMS unavailability via reliable and hardware links. Two links called SIR[8] and CIR[9] shall be implemented.

*

Reference **ACD-002-C**

Deleted.

*

Reference **CDD-003-C**

Depending on the unavailability reason (i.e. alarm level), two different status are sent to the ACMS :

- The SIR status signal in case of CDMS reconfiguration triggered by a level 4 alarm (power alarm : Battery DOD), to request ACMS to reach a status and put the spacecraft in an attitude, safe w.r.t. power generation, (ACMS Sun Acquisition mode). The S/C shall transition to S/C Survival Mode
- The CIR status signal in case of CDMS reconfiguration triggered by a level 3 alarm (computer level anomaly), to request ACMS to put the spacecraft in an Earth pointing attitude permitting to get back the optimum downlink rate. The S/C shall be transitioned to S/C Earth Acquisition Mode

*

In case of CDMS unavailability caused by a level 3 alarm, to reach an Earth pointing attitude will permit to download

data at a high rate and allow a fast failure analysis and recovery by the ground when in visibility.

A special case occurs, however, if the CIR signal is raised while the spacecraft is in Launch Mode and Sun Acquisition Mode :

Reference **ACD-003-C**

If the CIR signal is raised while the S/C is Launch Mode and in Sun Acquisition Mode, no action shall be performed by the ACMS.

*

[8] SIR : Satellite in Reconfiguration

[9] CIR : CDMS in Reconfiguration

3.4.1.2.3 Communication link unavailability

Some information (e.g. synchronization words) have to be transmitted periodically from the CDMU to the ACC over the communication link. The implemented communication link is a 1553 data bus (composed of a nominal bus – *BUS A* and a redundant bus – *BUS B*) where CDMU is the bus controller and ACC a remote terminal.

In the same way, some information (e.g. housekeeping data) have to be transmitted periodically from the ACC to the CDMU.

Reference **CDD-001-C**

Deleted.

*

Reference **ACD-001-C**

[P:SCI-PT-RS-07360#3.14-FTS-2.

If the ACC doesn't receive the regular information expected from the CDMU (e.g. time synchronization messages), a time-out alarm inside the ACC shall be triggered to initiate an Earth Acquisition.

*

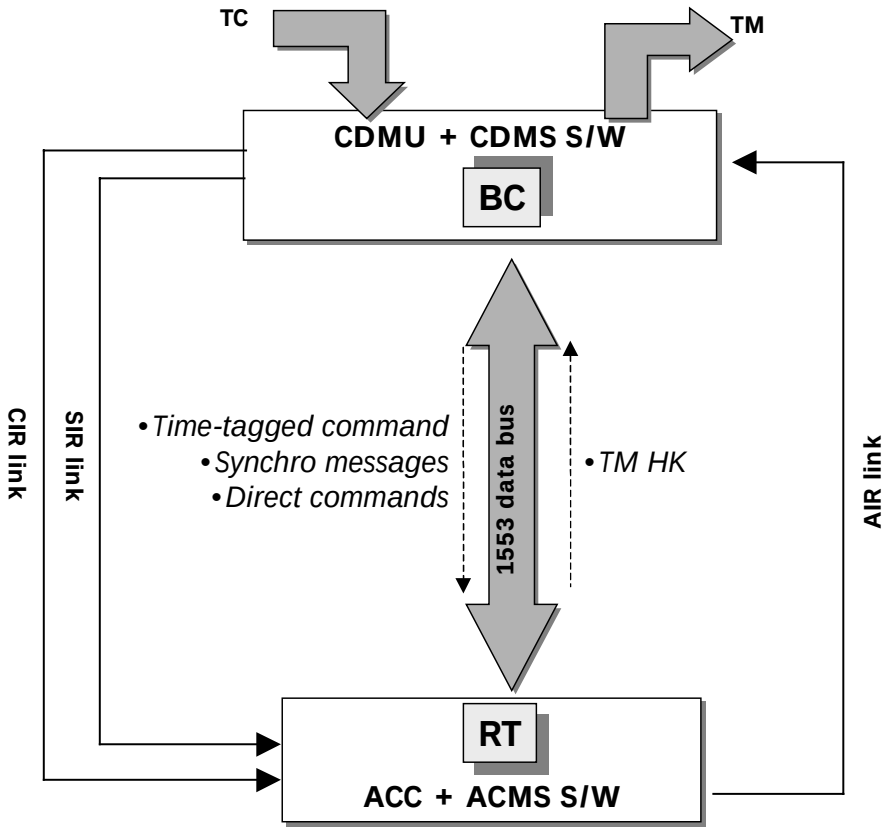

Figure 3.4.2 : CDMS/ACMS Communication

3.4.1.3 MTL Management associated to FDIR actions

One of the main features of the operational concept is the Mission TimeLine which execution is centralized at the level of the CDMS. The MTL is stored in the CDMU, in a non volatile memory area. The MTL represents the mission plan, and one of the drivers of the FDIR strategy is, as far as possible, to help to pursue this plan.

Reference **GEF-080-C**

[P:SCI-PT-RS-05991 - Ch.4#4.3.4-MOOM-195 H/P

Time-tagged commands shall be stored in protected memory (e.g. SSMM for size reason) to ensure a safe backup when resuming operation.

*

However, as a consequence of failures, reconfigurations are performed, depending on the failure type and the spacecraft mode (which drives the FDIR mode, AFS or AFO, see table 3.3.5); these reconfigurations may

interfere with the MTL execution, and present section addresses the way the interface between the MTL and the failure cases are managed such that the MTL can be continued.

3.4.1.3.1 Failure at CDMS level

As long as the CDMU processor module states are not involved in the detected failures nor in the reconfiguration sequences, i.e. for levels 0 to 2 CDMS failures, the MTL can and will be continued with no significant impact.

Reference **GEF-121-C**

For levels 0 to 2 CDMS failures, the MTL shall be nominally continued.

*

Reference **GEF-169-C**

In the case (unpredictable) where a MTL commands would get overdue,

- an event shall be raised
- if the overdue command belongs to a transient subschedule, the subschedule shall be disabled
- if the overdue command belongs to a permanent subschedule, it shall be sent at the earliest possible time, and the MTL commands order shall still be maintained.

*

If the CDMU processor modules are involved in the reconfiguration processes, two distinct conditions are considered :

3.4.1.3.1.1 The reconfiguration is due to a CDMU level 3 failure

As it has been presented before, the first occurrence is labelled level 3a. In this case, the baseline is to have the MTL execution disabled. The corresponding ACMS configuration is described in section 3.4.1.2.2. “CDMS unavailability” : a Safe, Earth pointed, attitude is adopted. The S/C is in Earth Acquisition Mode.

Reference **GEF-122-C**

On a CDMU level 3a alarm occurrence, CDMU will be reset. The corresponding spacecraft Modes transitions and associated subsystem and functional modes shall be as specified in Fig 2.3.2 and tables 2.3.3 and 2.3.4 : the Mission TimeLine execution shall be disabled and no OBCP shall be started by default. The MTL service execution shall only be re-enabled by TC.

*

The second occurrence is labeled level 3b. In that case, the baseline for a level 3b is again to have the MTL transient subschedules disabled. The failure 3b recovery sequence is then such that :

– the CDMS and related units are in a stable “ safe mode ”

– the ACMS is requested to initiate an Earth Pointing as for level 3a failure

– the instruments are put in a defined Standby Mode

Reference **GEF-123-C**

[P:SCI-PT-RS-05991 - Ch.4#4.3.3-MOOM-175 H/P

Following a CDMU level 3b alarm occurrence, the spacecraft Modes transitions and associated subsystem and functional modes shall be as specified in Fig 2.3.2 and tables 2.3.3 and 2.3.4 : the Mission TimeLine service execution shall be disabled and no OBCP shall be started by default. The MTL service execution shall only be re- enabled by TC .

*

3.4.1.3.1.2 The reconfiguration is due to a CDMS level 4 failure

It leads to a complete CDMS level reconfiguration with a switch over to the redundant units, including the processor module. Level 4 failures are system level " critical " failures and a restart of the MTL in these conditions is consequently not baselined.

Reference **GEF-124-C**

[P:SCI-PT-RS-05991 - Ch.4#4.3.3-MOOM-175 H/P

In case of CDMS Level 4 failures, the spacecraft Modes transitions and associated subsystem and functional modes shall be as specified in Fig 2.3.2 and tables 2.3.3 and 2.3.4 : the Mission TimeLine shall be disabled and no OBCP shall be started by default. MTL shall only be re-enabled by TC.

*

The ACMS configuration is described in section 6.5.4.3 "CDMS unavailability" : a Safe w.r.t. power, Sun Pointing Mode is triggered : Spacecraft is in S/C Survival Mode

The configuration of the other satellite units, including the instruments is established by the reconfiguration sequence. Basically, only the essential loads are kept ON, and the instruments are turned OFF via CDM_RM HLC.

3.4.1.3.2 Failure at ACMS level

The general consequences of any reconfiguration are that :

– The expected performance (pointing, orbit correction) may not be ensured during the time of reconfiguration : the instruments will be mis-pointed with respect to ground planning via the MTL. This is definitely not considered as a critical issue, just a mission degradation :

- It may happen only in case of specific manoeuvre / reconfiguration.
- It will be reported in the down-linked telemetry data and be signified to the involved instrument (s).

– The reconfiguration sequence may not be achieved when the next MTL command occurs. In that case, the ACMS may not be ready to execute the received command (still under reconfiguration)

Two cases must be considered :

(1) The recovery is fast enough to maintain the control error within acceptable limits which depend on the controller implementation.

This is the nominal case in the sense that by design, no anticipated single failure should prevent the satellites to catch up with their pointing target in Spacecraft Nominal Mode. The Reaction Wheels unloading activity , for Herschel, will be programmed via the MTL to prevent any wheel saturation in normal operation.

In order that the ACMS can propagate the targeted attitude, regardless of the failure (levels 0 to 2 failures), the relevant MTL commands sending to the ACC will never be interrupted.

Reference **GEF-114-C**

Deleted

*

The MTL functionalities shall allow the ground to select an implementation such that the ACMS commanding is not interrupted in any level 0 to 2 failure case. This will permit the pointing to be calculated without interruption.

(2) The recovery is such that the requested control error cannot be kept within the acceptable limits.

As mentioned above the ACMS is designed not to face this situation in case of single failure at ACMS level. Nevertheless a failure at CDMS level followed by a reconfiguration, or an erroneous MTL TC, may indirectly induce an interruption, momentarily or permanently of the MTL commands issuing, which could eventually result in having, in the case of Herschel, an autonomous reaction wheels unloading sequence to be started, or a non optimum pointing attitude to be kept. This case actually corresponds to the one addressed in section 6.5.4.3 “CDMS unavailability” : it leads a “safe attitude” to be adopted (Sun or Earth pointing depending on the failure). When in one of these modes, routine MTL telecommands will be ignored.

3.4.1.3.3 Failure at instrument level

It is anticipated that the instruments will not be in a position to receive and process the MTL commands at the same time than the recovery activities or commands (OBCP’s) possibly triggered by the reception of the “event TM” signaling an anomaly to the CDMS.

Consequently, upon instrument failure notification, the MTL commands related to this instrument within the running subschedule belonging to the failed instrument will be disabled.

Reference **GEF-115-C**

[P:SCI-PT-RS-07360#3.9-MTL-6.

The MTL implementation selected by the ground entity will be such that the MTL commands for a given instrument can be filtered out in case of instrument failure notification.

*

Because the number and type of commands which would be missed by the instrument while it is recovered is not predictable, the MTL commands for this instrument will typically be re-enabled only if (AND) :

– the instrument has notified its return to a nominal operating mode,

– a new subschedule involving the instrument is enabled.

Reference **GEF-116-C**

The MTL implementation will be such that the restart of the failed instrument operation is made possible, after successful recovery of the instrument, at an adequate point in time (eg. at the next subchedule where the failed instrument is involved).

*

3.4.1.4 Failure Recovery Strategy

The two following tables illustrate the CDMS and ACMS failure recovery strategy for the FDIR levels 1 and 2.

Depending on the failure level and the active FDIR mode, a recovery sequence is defined.

FAILURE LEVEL		DETECTION PROCEDURE	FAILURE RECOVERY	
			AFS Mode	AFO Mode
1a	Equipment failure	OBSW acquisition of unit health check status	Detect failure only. Isolation and recovery will be performed if levels 3 or 4 are triggered On a case by case basis, deviations could be accepted to authorize the isolation and recovery of well identified level 1a failures in AFS	Stop boost if boost and depending on the failed ACMS equipment unit Save failure context Switch over to the redundant unit using SGM configuration Resume operations
1b	Communication I/F failure	Monitoring of communication protocol and bus couplers	Detect failure only. Isolation and recovery will be performed if levels 3 or 4 are triggered. Requirements for 1553 data bus failure detection are specified in Annex 1. On a case by case basis, deviations could be accepted to authorize the isolation and recovery of well identified level 1b failures in AFS	Stop boost if boost and depending on the failed equipment unit (TBC) Save failure context Switch over to the redundant bus coupler or direct interface using SGM configuration. Requirements for 1553 data bus failure detection isolation and recovery are specified in Annex 1. Resume operations
2	Main function failure	OBSW performance check	Detect failure only. Isolation and recovery will be performed if levels 3 or 4 are triggered On a case by case basis, deviations could be accepted to authorize the isolation and recovery of well identified level 2 failures in AFS	Stop boost if boost Save failure context Identify the failed unit by a consistency cross check or possibly switch over to the redundant functional chain using SGM configuration. Resume operations

Figure 3.4.3 : Levels 1 and 2 failure recovery strategy

The two next tables illustrate the FDIR Level 3 failure recovery strategy. Each computer is treated on its own. First is presented the ACC Level 3 failure recovery strategy, then the CDMU one. Again, depending on the failure level and the active FDIR mode, a recovery sequence is defined.

FAILURE LEVEL		DETECTION PROCEDURE	FAILURE RECOVERY	
			AFS Mode	AFO Mode
3a	**ACC** internal failure – first occurrence	Nominal processor module HW alarm or SW watch dog	Stop boost if boost In case of ACC internal alarm: Set the AIR signal, to inform the ACMS about the ACC reconfiguration Save Failure context Reset the nominal processor module. Re-Load SGM context Transition the S/C into the Mode specified in Fig 2.3.2 : S/C is switched to Sun Acquisition Mode. if it runs from S/C Nominal Mode or Earth Acq Mode	
3b	**ACC** internal failure – second occurrence	Nominal processor module HW alarm or SW watch dog	Stop boost if boost In case of ACC internal alarm: Set the AIR signal, to inform the CDMS about the ACC reconfiguration Save failure context Switch over to the redundant processor module Load context from Survival Context memory Transition the S/C into the Mode specified in Fig 2.3.2 : S/C is switched to Sun Acquisition Mode if it runs from S/C Nominal Mode or Earth Acq Mode	

Figure 3.4.4 : ACC Level 3 failure recovery strategy

FAILURE LEVEL		DETECTION PROCEDURE	FAILURE RECOVERY	
			AFS Mode	AFO Mode
3a	**CDMU** internal failure – first occurrence	Nominal processor module HW alarm or SW watch dog	In case of CDMU internal alarm : Set a CIR signal to be acquired by the ACMS, Save failure context Reset the nominal processor module. Re Load SGM context Disable MTL service execution and wait for TC to re-start full MTL execution Transition the S/C into the Mode specified in Fig 2.3.2 : S/C is switched to Earth Acquisition Mode. if it runs from S/C Nominal Mode	
3b	**CDMU** internal failure – second occurrence	Nominal processor module HW alarm or SW watch dog	In case of CDMU internal alarm : Set a CIR signal to be acquired by the ACMS, Save failure context Switch over to the redundant processor module	Re Load SGM context Disable MTL service execution and wait for TC to re-start full MTL execution Transition the S/C into the Mode specified in Fig 2.3.2 : S/C is switched to Earth Acquisition Mode. if it runs from S/C Nominal Mode

Figure 3.4.5 : CDMU Level 3 failure recovery strategy

The last table illustrate the FDIR Level 4 failure recovery strategy.

There is a common strategy for both FDIR modes (i.e. AFS and AFO), but the recovery sequence is sensitively different depending on the alarmed computer (i.e. ACMS level 4 failures or CDMS level 4 failures).

FAILURE LEVEL		DETECTION PROCEDURE	FAILURE RECOVERY	
			AFS Mode	AFO Mode
4	Global satellite malfunction	System Alarm : DOD (CDMS), RA & SP (ACMS)	Stop boost if boost Disconnect non essential loads In case of CDMS Level 4 alarm : Set SIR signal to be acquired by ACMS In case of ACMS Level 4 alarm : Set AIR signal to be acquired by CDMS, to inform about ACMS reconfiguration Save failure context Switch over to the redundant processor module and re-start from Survival Context memory In case of CDMS level 4 alarm, see Fig 2.3.2 : spacecraft is switched to Survival Mode (exception is from Launch Mode) In case of ACMS level 4 alarm, see Fig 2.3.2: spacecraft is switched to Sun Acq Mode with ACMS in SM (exception is Launch Mode) Disable MTL Service and wait for TC to re-engage full MTL service execution	

Figure 3.4.6 : Level 4 failure recovery strategy

3.4.2 Instruments

Instruments function is obviously fundamentally different from the platform units one : the instruments perform the scientific mission while the SVM provides the operational means to support these instruments.

However, as far as FDIR is concerned, the baseline principle is to manage the instruments as ordinary units through the hardware connecting them to the CDMS. Instruments failures shall therefore be treated as level 1a failures, with the following noticeable differences though :

– the instruments failures detection and recovery is nominally ensured :

- by the instruments themselves, spacecraft actions being possibly requested via the emission of event TM packets.

Reference **INF-006-C**

The failures requesting the intervention of the spacecraft and the associated reconfiguration sequences shall be defined by the instruments via the IIDBs (AD5 to 9).

*

- by the CDMS SW via a monitoring of the amount of science data delivered by the instruments (number of TM packets) : if the data generated is not the expected one, it is assumed that this reflects an instrument anomaly (e.g. the instrument software has got stuck), and will basically lead to a switch over to the redundant instrument electronics (TBC by instruments).

Reference **INF-007-C**

The CDMS SW shall monitor the amount of science data delivered by the instruments and, in case of anomaly CDMS shall start an action to be defined by instruments.

*

– an instrument anomaly detected by or reported to the CDMS implies, as detailed in previous chapters, that the running MTL subschedule “belonging” to the failed instrument is temporarily disabled, and the software Functions and OBCP’s possibly started by this subschedule shall be terminated

3.5 FDIR Requirements on ACMS subsystem

According to the SVM architecture, the FDIR management is divided into the spacecraft monitoring and control function and the spacecraft positioning function. Each computer, respectively the CDMU and the ACC, is in charge of a part of the FDIR treatment.

General system FDIR is mainly managed and executed by the CDMU. But both computer shall have a coherent FDIR strategy. For this reason, some FDIR design requirements have to be defined for the ACMS.

Reference **GEF-110-C**

Deleted.

*

The ACMS shall define a FDIR according to the following design constraints:

3.5.1 ACMS FDIR Modes

The CDMU commands a FDIR mode. The ACMS FDIR strategy follows this mode, which can be AFS (Autonomous Fail Safe) or AFO (Autonomous Fail Operational).

Reference **GEF-111-C**

The ACMS shall not modify the FDIR autonomy mode.

*

The two FDIR modes are the one defined previously:

– Autonomous Fail Safe (AFS)

In this mode, the ACMS shall limit the recovery attempts, in order not to put the spacecraft in a safe attitude.

– Autonomous Fail Operational (AFO)

This autonomy mode aims at maintaining the continuity of the mission and performance as long as healthy alternative redundant functional path exits. It essentially applies for both Herschel and Planck, to the scientific observation phases.

3.5.2 ACMS FDIR Failure Levels

Reference **ACF-004-C**

The ACMS shall report the FDIR events and actions according to the five levels (0 to 4) in which all failures are classified.

*

As an answer to system FDIR events (i.e. Level 4 failures), ACMS typical alarms could be :

– Sun Pointing outside allowed zone (SP)

– Rate Anomaly Detection (RA)

END OF DOCUMENT

APPENDIX 1 : 1553 BUS FDIR

1.INTRODUCTION

This annex describes the implementation of the overall Herschel/Planck communication Bus data exchange FDIR. This communication Bus links the data handling system (CDMU)

- to the science instruments Data Processing Units, the Attitude Control Computer (ACC), considered as " intelligent users ",
- to the Power Conditioning and Distribution Unit (PCDU), the RF Transponders (TRSP) and the Herschel Cryostat Control Unit (CCU), considered as " non intelligent " units.

Two main Bus protocol layers are considered, the Data Link Layer, and the Transfer Layer. Both are specified in the Annex 9 of AD01. For each of them, mechanisms are proposed which, all together allow a simple but exhaustive enough failure identification, and a straightforward recovery strategy.

This annex states the main requirements related to Data Link Layer and Transfer Layer FDIR, and shall be used as reference to complete the relevant AD01 requirements.

All over the document, the "RT" wording will be used. It must be understood, unless specified, as the Remote Terminal 1553 interface + the connected user. Similarly, the " BC " wording relates to the 1553 Bus Controller interface + the connected computer (CDMU).

2.APPLICABLE & REFERENCE DOCUMENTS

2.1Applicable documents

AD01: Packet Structure ICD
Doc. SCI-PT-ICD-07527

AD02: MIL STD 1553B

2.2 Reference documents

RD01: Hardware/Software Sizing Cases
H-P-1-ASPI-TN-0398

3.BUS DATA EXCHANGE FDIR

3.1 General

The exchange of information using the 1553 data bus as support medium happens at different levels and must comply to different levels of protocol, typically :

- the physical level : it defines the bus electrical characteristics which have to be taken into account by the Remote Terminals and Bus Controller (BC) design.
- the data link layer (DLL) : this is the low level bus protocol, as specified in the MIL STD 1553B handbook (AD02). It defines the elementary receive and transmit 1553 messages, and assigns the RT sub-addresses.
- the transfer layer (TFL) : it defines, on top of the DLL, the protocol to be established between the BC and the different RT's to ensure the best usage of the Bus bandwidth and robust transfer mechanisms. The TFL organizes the DLL messages into frame and sub frames in accordance with the specific mission constraints, and the proper handshake between the BC and the intelligent RT's.

In addition to these 1553 level layers, one shall mention the packet layer used by the intelligent RT's on top of the TFL.

Each layer has its own requirements, its own failure modes and its own level of recovery. It is to be noticed that the physical layer failure modes are handled by the design of the 1553 Bus itself (redundant Bus, bus couplers, long stub, ...) and identified at DLL level. In order to satisfy the hierarchical FDIR approach baselined on Herschel/Planck, it is strongly desirable to define clear and unambiguous FDIR strategies for the 2 main communication bus layers, the DLL and the TFL. This is the purpose of the following chapters.

3.2 Data link layer FDIR

The bus level, DLL, FDIR is addressed in AD01 section 3.5.2.

All the intelligent and non intelligent RT's are involved.

3.2.1 Failure identification

Ways to identify failures at 1553 messages level are specified :

Reference **HP-SOFDIR-1553-REQ-0010**

- **from BC 1553 I/F**, the following status are required to be monitored at each message transaction:
  - 1. RT transmission error bit : this identifies a RT or physical link failure. It is set by the BC upon detection of an error in the message received from the RT, ie :
    - if a word of the message has not passed the validity test defined in AD02 §4.4.1.1 :
      - The word sync field must be valid,
      - The word code must be valid (Manchester II)
      - The information field must contain 16bits + parity,
      - The word parity must be odd.

- ➢ if the message is not contiguous (AD02 §4.4.1.2)
- ➢ if the BC fail safe hardware has timed out (AD02 §4.4.1.3)

- 2. RT no response time out bit : this identifies a RT or physical link failure. It is set if the RT response has not arrived within 14µs after the last mode command has been sent by the BC.
- 3. BC loop back test fail flag : this identifies a BC 1553 I/F failure. It is set if the BC self test fails. The self test typically involves a wraparound test of the BC encoder/decoder and transceiver sections. Note that its detailed implementation depends on the BC design.

*

Reference **HP-SOFDIR-1553-REQ-0020**

– **from the RT's Status Word**, for each 1553 message transaction, the following bits shall be monitored :

- 4. RT message error bit, set by the RT upon detection of an error in the message (any message word received by the RT has not passed the validity test defined in AD02 §4.4.1.1, criteria in AD02 §4.4.1.2 are not met) or an illegal message identification (if the RT selects the option to monitor the illegal commands). If this bit is set this means none of the data received within the complete message is used by the RT. This is a MANDATORY bit, however processing of illegal commands, or not, shall be stated by the RT.
- 5. RT busy bits, provided as a feedback to the BC that the RT is " being moving " data between the RT 1553 I/F electronics and the host subsystem in response to a command or more generally that the RT 1553 I/F or the host subsystem is " busy " such that the communication on the Bus can be affected. Note that this is an " historical bit " which use is discouraged by Notice 2 of the AD02. If used, the Notice requires it to be set only after as a result of a particular command received from the BC, and NOT due to routine operation.
- 6. RT subsystem flag bit, used to provide " health " data regarding the subsystem (instrument, unit.) the RT 1553 I/F is connected to. It serves as a failure indicator (" watchdog ") without providing information on the nature of the failure which must be provided via a given SA ; AD01 proposes SA1T to contain RT status message.
- 7. RT terminal flag bit informs the BC about a fault/failure within the RT 1553 I/F (not the connected subsystem) circuitry. Further information on the nature of the failure shall be reported via a defined SA. SA1T is proposed in AD01. Note that this bit is requested to reflect the status of the whole RT, ie the channels A & B.

*

As illustrated in Fig 3.2-1 below, the Data Bus failure detection applies only on the BC reported status, ie the status labeled 1, 2 & 3 above. RT's message error, subsystem flag, terminal flag and busy bits are used as criteria to evaluate, at BC level, TM packet acquisition, and return, or not, the Telemetry Packet Transfer Confirmation message (see §3.3.3).

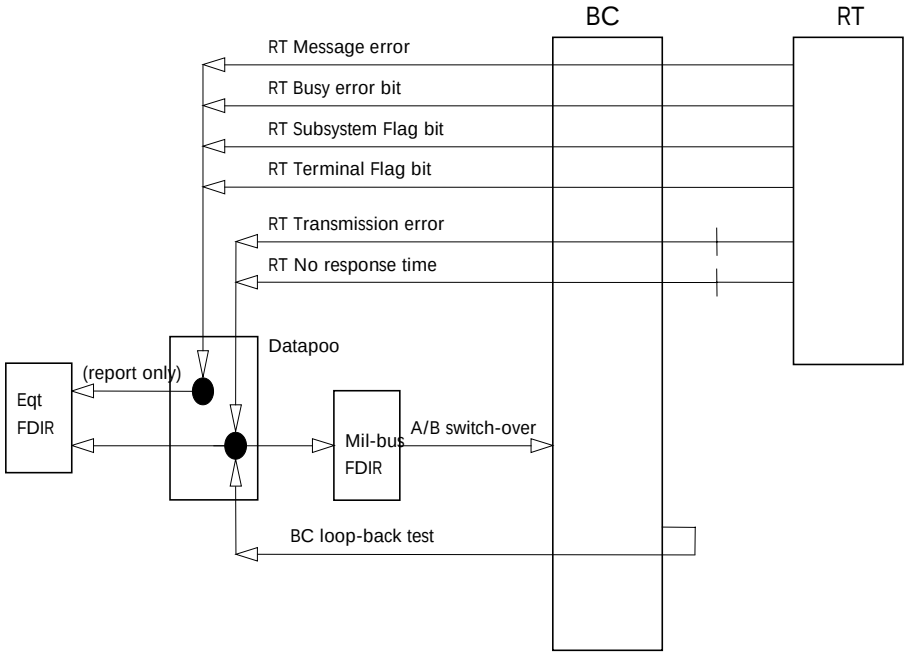

Figure 3.2-1 DLL failure detection principles

3.2.2 Recovery mechanisms

NOTA : In the present section, nominal, active bus is assumed to be the Bus A. Should the traffic happen on Bus B, the same requirements would apply, just inverting Bus A- Bus B.

In order to support the DLL FDIR process, and also the TFL FDIR process (see later) there is a need to create several status flags, associated to each RT address. These status shall be maintained by the BC in SafeGuard memory.

Reference **HP-SOFDIR-1553-REQ-0150**

A RT configuration matrix shall be maintained by the BC; It shall be composed at a minimum of :

- the RT *ON/OFF* status
- the RT *Dead/Alive* status, to permit to identify RT's which are definitely failed, and cannot be turned OFF (eg. because a standard LCL has failed, or because the unit is powered via FCL). The dead/alive status is managed by the ground,
- RT *Well_TC/Sick_TC* status, to permit to mark a failed RT during a TFL TC FDIR sequence (see §3.3),
- RT *Well_TM/Sick_TM* status, to permit to mark a failed RT during a TFL TM FDIR sequence (see §3.3),
- RT *valid/invalid* status to mark non available RT's during a DLL recovery FDIR sequence. A RT will typically be labelled invalid when it is recognised to be reconfiguring
- RT *Vital/Non Vital* status in order to be able to allocate specific recovery actions to selected RT's. Currently, only the ACC is identified as a Vital RT ; confirmed communication failure with a Vital RT (on both A & B 1553 Buses) leads to a CDMU level 3 reconfiguration. Vital/Non Vital status is maintained by the ground.

*

Reference **HP-SOFDIR-1553-REQ-0151**

The RT configuration matrix shall be saved in CDMU SGM as part of the CDMS context.

*

Reference **HP-SOFDIR-1553-REQ-0152**

The RT *Invalid* to RT *Valid* transition shall only be performed upon dedicated TC.

The only exception is : the ACC Active RT shall be declared *Valid* at the occurrence of AIR signal Set to AIR Reset transition.

*

Reference **HP-SOFDIR-1553-REQ-0154**

DLL level failure Isolation and Recovery actions for a RT declared *Invalid* shall be immediately disabled

*

Reference **HP-SOFDIR-1553-REQ-0156**

TFL level failure Isolation and recovery actions for a RT declared *invalid* shall be immediately disabled.

*

The Bus DLL FDIR is considered as essential to the spacecraft safety. As a consequence, it shall remain active in FDIR AFS mode.

Reference **HP-SOFDIR-1553-REQ-0025**

DLL FDIR shall remain enabled by default in FDIR AFS Mode.

*

Reference **HP-SOFDIR-1553-REQ-0030**

Bus shall be declared " unhealthy " if any one of the failed bits at BC interface level (labels 1, 2 or 3 in §3.2.1) is set , and if the failure happens with a "valid" RT.

*

Reference **HP-SOFDIR-1553-REQ-0035**

Bus recovery sequence shall be started if alternate Bus is "healthy ". If current Bus if declared unhealthy while alternate Bus is found unhealthy, level 3 CDMU alarm shall be triggered

*

When the conditions for Bus recovery are met :

Reference **HP-SOFDIR-1553-REQ-0040**

When the current communication Bus is declared " Unhealthy ", an event TM(5,2) as defined in AD01 §5.5, shall be raised by the CDMU SW.

*

Simultaneously, at detection of a " unhealthy " status, the Isolation and recovery actions shall be :

Reference **HP-SOFDIR-1553-REQ-0050**

– the active bus profile shall be " muted ", ie :
  - no TC (messages or packets) from the Bus profile shall be output
  - Bus profile TC's (messages and packets) shall be buffered during the "muted" period
  - TM acquisition (messages or packets) from the Bus profile shall not be performed
  - Sync broadcast messages shall be nominally distributed
– the Transfer Layer Isolation and Recovery actions shall be momentarily disabled (see later)

*

Reference **HP-SOFDIR-1553-REQ-0060**

– the healthiness of Bus B/Bus A communications shall be confirmed by data wrap around test with each RT at SA30R/SA30T on bus B then Bus A

*

Reference **HP-SOFDIR-1553-REQ-0065**

– The data wrap around test shall be implemented depending on the RT by (OR) :
  – writing a fixed data set to RT SA30R during 1553 Bus slot N (see AD1 appendix 9) and reading back RT SA30T in slot N+1
  – writing a fixed data set to RT SA30R during 1553 Bus slot N (see AD1 appendix 9) and reading back RT SA30T in slot N+I, where I shall be specified by the RT.

*

Reference **HP-SOFDIR-1553-REQ-0070**

– Bus switch over shall happen only if communications on Bus B are found healthy, while there are not on bus A - see figure below.

*

Reference **HP-SOFDIR-1553-REQ-0080**

– overall recovery sequence shall be less than 250ms. This means that the Bus users must be able to buffer > 250ms of TM data to avoid TM data loss. This short recovery time has been selected to ensure that :
  - a minimum amount of TM is to be buffered by the Bus users,
  - a maximum of 1 subframe dedicated to the sending of TC packets, among 4, is missed,
  - a maximum of 16x3=48 command/acquisition slots are missed.

*

This leaves the capability to transmit 9 TC packets and perform up to 144 commands/acquisitions in the frame where the Bus anomaly has occurred. As specified in RD01, this remains sufficient to support the high priority, time critical messages (ie originated from the FDIR processes, and the MTL). Therefore, a DLL failure recovery does not impair the command priority scheme described in RD01, and allows for a nominal mission continuation in case of successful recovery.

After the recovery sequence successful completion :

Reference **HP-SOFDIR-1553-REQ-0090**

– The bus profile shall be " unmuted ". This shall take place at the next subframe following the completion of the bus checks and DLL failure recovery.

*

Reference **HP-SOFDIR-1553-REQ-0100**

– the Transfer Layer Isolation and Recovery actions shall be enabled

*

Reference **HP-SOFDIR-1553-REQ-0110**

– Any last TC message sent shall be repeated

*

Reference **HP-SOFDIR-1553-REQ-0120**

– Any last TC packet sent shall be repeated, which means that the Bus intelligent user's shall be robust to the repetition of the same telecommand. An agreed deviation is if the BC has acknowledged the correct reception of the TC packet (ie. correct PTC has been returned by RT).

In order to ease the handling of a repeated TC packet, the BC shall ensure that the TC Packet Transfer Descriptor packet count field (8 bits) of the repeated TC is identical to the TC PTD count field of the 1st TC sent before the bus failure.

*

Reference **HP-SOFDIR-1553-REQ-0130**

The overall DLL FDIR algorithm is illustrated in Fig. 3.2-2 hereafter and shall be applied.

*

Reference **HP-SOFDIR-1553-REQ-0140**

As shown, if the switch over to Bus B is not successful, 2 cases are considered :

– If the Bus communication anomaly is with one RT only, ie the wraparound test fails with only one RT : in this configuration, the failure is considered to be within the subsystem connected to the 1553 I/F RT, and the relevant subsystem FDIR shall be activated,

– If the Bus communication anomaly is with several RT's, ie the wrap around test fails with more than one RT, or if the Bus communication anomaly is with one Vital RT (see definition below), ie the wrap around test fails with a vital RT : the BC shall be considered failed and the DLL FDIR shall raise a level 3 alarm to trigger a CDMU reset and thus put the spacecraft in Earth Pointing Mode.

*

Reference **HP-SOFDIR-1553-REQ-0141**

The current healthy/unhealthy Bus (A / B) status shall be periodically stored in CDMU_SGM as part of the CDMS status.

*

Reference **HP-SOFDIR-1553-REQ-00145**

It shall be possible to independently set the status of Bus A & B to healthy or unhealthy by dedicated TC's.

*

Reference **HP-SOFDIR-1553-REQ-00142**

The Bus side (A or B) to use in S/C Survival Mode (ie. after CDMS level 4 alarm) shall be stored in the write protected Survival Context memory.

*

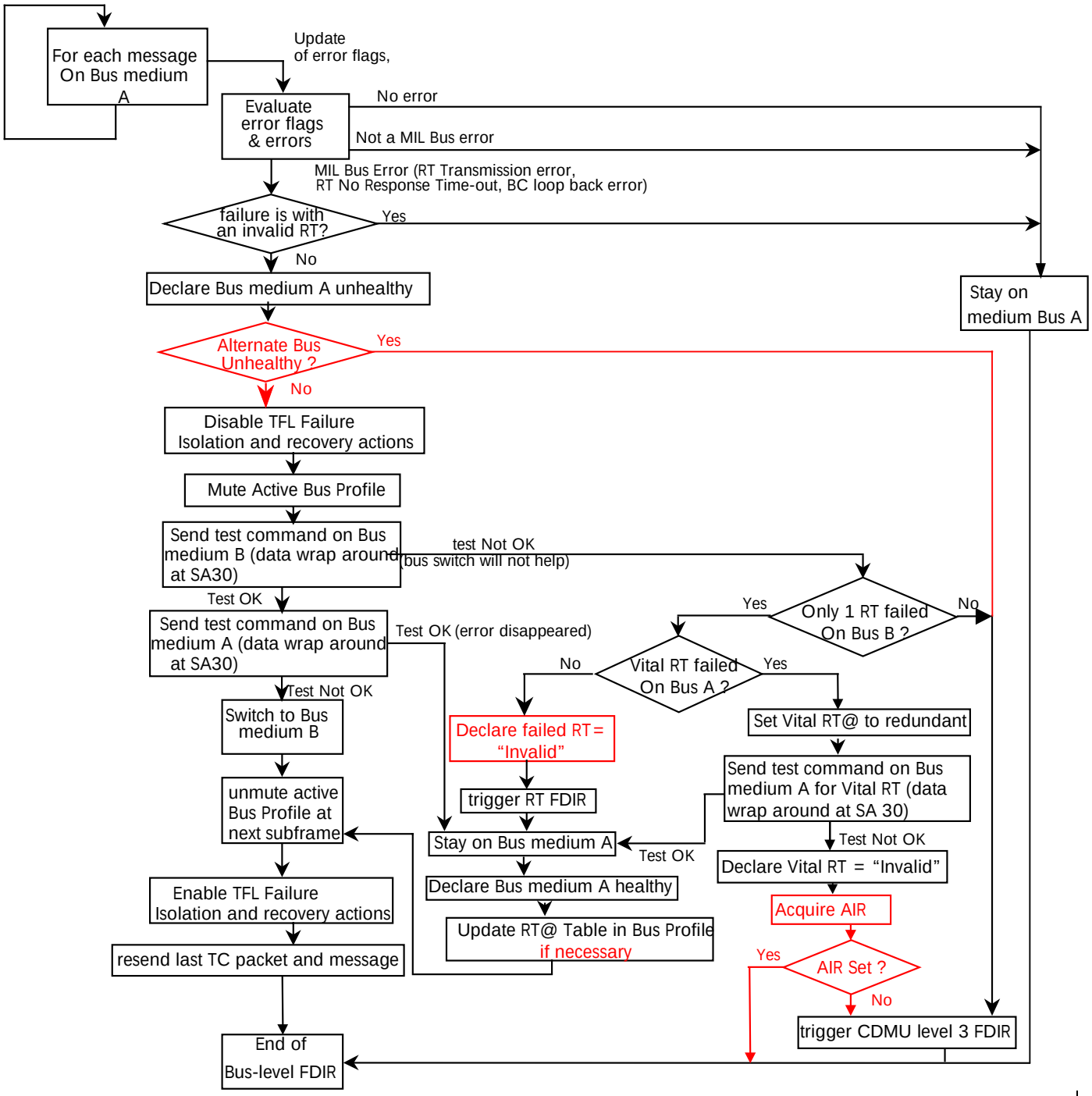

Figure 3.2-2 DLL failure isolation and recovery

The flags 4, 5, 6, 7 in §3.2.1 deal with the RT status. As such they are not treated as a " bus " failure by the BC, but as anomaly in the addressed RT and will be reported to the higher TFL FDIR level described in next chapter.

3.3 Transfer layer FDIR

3.3.1 General

The Transfer Layer addresses the protocol which organizes the data exchange for the different RT's, depending on the type of RT's and in line with the mission constraints (number of RT's, data rates, requested BC support, ...). The TFL is specified in chapter 4 of Annex 9 to AD01. While the DLL layer concerns all the bus users, intelligent and non intelligent, this section addresses the RT's using the Data Bus to transfer and receive data under packets format .

The TFL FDIR purpose is to monitor and detect failures of the TFL implementation. The TFL first organizes the Bus traffic into frames and subframes ; the division of the Bus activities is materialized by the transmission of Synchronization Mode Commands to the users at 64Hz. The TFL then defines the protocol by which the TM packets are polled and collected from the intelligent user's, depending on the user operating mode (i.e. nominal or burst mode, see AD01, annex 9), and the TC packets are transmitted. This is achieved by suitable subframes allocations in the Bus profile, and by request-service-confirm mechanisms between the BC and the intelligent RT's.

The TFL for these packets users is based on the exchange of well identified messages :

- Sync Mode commands from BC to RT
- TM packet Transfer Request from BC to RT
- TM Packets Transfer Confirmation from RT to BC
- TC Packets Transfer Descriptor from BC to RT
- TC Packet Transfer Confirmation from RT to BC

The basic principle of the 1553 data Bus is to have the overall Bus traffic control centralized within the Bus Controller. In the same way, as far as the TFL FDIR is concerned, the target in the mechanisms design will be to have most of the FDIR features supported at Bus Controller level. These features shall essentially be based on the existing protocol, using the messages listed above, and for the 2 cases :

- the TM acquisition protocol and
- the TC sending protocol

The following sections go through these 2 cases and detail the corresponding FDIR approach.

Finally, the TFL FDIR applies at a level higher than the DLL FDIR, and, as mentioned in §3.2 and shown in Fig 3.2-2, the TFL FDIR shall be momentarily disabled when an anomaly is flagged and recovered by the DLL FDIR.

3.3.2 FDIR for TC transmission protocol

The proper TC transmission on the Data Bus is a key to nominal operations of Herschel/Planck spacecraft : mission continuation is considered as unsafe in case of failure of TC packets transmission. It is consequently proposed to implement a " one retry " capability.

The TC FDIR state diagram is presented in Fig. 3.3-1 ; it mainly relies on the analysis by the Bus Controller of the Packet Transfer Confirmation (PTC) message returned by the RT upon successful acquisition of the TC.

Reference **HP-SOFDIR-1553-REQ-0151**

The procedure to apply to detect, isolate and recover from a TC transmission error on the CDMU 1553 Bus (TFL TC FDIR) shall be as described in Fig 3.3-1. It is explained through the following requirements.

*

Reference **HP-SOFDIR-1553-REQ-0160**

The TC PTC shall be checked by the BC not earlier than 3 subframes after the TC Packet Telecommand Descriptor (PTD) message has been put by the BC to SA27R.

*

Reference **HP-SOFDIR-1553-REQ-0170**

The TC PTC shall be declared " invalid " by the Bus Controller if the TC PTC content is different from the corresponding TC PTD.

*

As mentioned, in order to improve the robustness of the TC acquisition process, it is proposed to implement a " one retry " capability.

Reference **HP-SOFDIR-1553-REQ-0180**

A TC packet shall be kept in the " BC queue " until one of the 2 conditions is valid :

- the TC packet acquisition by the RT is Confirmed via the TC PTC,
- the second attempt to send the TC packet is unsuccessful

*

Reference **HP-SOFDIR-1553-REQ-0190**

When, at the first attempt, the TC PTC is found invalid by the Bus Controller, the same TC shall be re-sent at the next available slot in the next subframe allocated to TC's in the active Bus Profile.

*

Reference **HP-SOFDIR-1553-REQ-0191**

If, at the first attempt, the TC PTC for a given RT is found invalid by the Bus then :

- The RT shall be declared "Sick_TC"

Default RT status is "Well_TC".

*

Reference **HP-SOFDIR-1553-REQ-0200**

The packet count field in the TC PTD message word for the second attempt (retry) shall be the same than the packet count field of the TC PTD at the first attempt.

*

Reference **HP-SOFDIR-1553-REQ-0201**

Deleted

*

Reference **HP-SOFDIR-1553-REQ-0210**

When , after the second attempt (retry), the TC PTC is still found invalid, then :

- the BC shall raise a TM(5,1) event to report the occurrence of the anomaly,
- if one single Non Vital RT is declared " Sick_TC " : The commanding associated to the failed RT (RT APID's) shall be disabled and the relevant RT FDIR shall be triggered ; it shall be stressed that the RT FDIR will obviously not make use of the 1553 TFL layer
- The CDMU FDIR level 3 (see AD03) recovery shall be engaged as soon as :
  - more than one RT is declared " Sick_TC " (in that case the failure is assumed located at BC level)
  - One Vital RT is found " Sick_TC "

*

Reference **HP-SOFDIR-1553-REQ-0215**

A RT which has been declared *sick_TC* after the second attempt to send the TC shall be reset «*well_TC* » only by a dedicated TC.

Exception is in case a CDMU level 3 or level 4 alarm is triggered : all the RT status shall then be automatically reset to «*well_TC* ».

*

Reference **HP-SOFDIR-1553-REQ-0220**

As far as the RT side is concerned, and mainly for ground failure analysis purpose,

the RT shall check the validity of the TC PTD. The TC PTD shall be declared " Valid " if the Command Word layout is as expected, and if the Packet Count field is different from the previous Valid TC PTD count.

*

3.3.3FDIR for TM acquisition protocol

The optimum science return relies on the correct operation of the TM acquisition process. A " one retry " capability is specified in AD01 and gives a " second chance " to acquire the TM packets.

The TM FDIR state diagram is presented in Fig. 3.3-2 for the detailed BC activities and in Fig 3.3-3 for the detailed RT activities.

3.3.3.1 TM acquisition FDIR - BC side

Reference **HP-SOFDIR-1553-REQ-0221**

The procedure to apply to detect, isolate and recover from a TM packet transmission error on the CDMU 1553 Bus (TFL TM FDIR) shall be as described in Fig 3.3-2. It is explained through the following requirements.

*

The basic FDIR principle applied to the telemetry packet acquisition process relies on the maintenance by the Bus Controller, of a TM packet counter for each RT's which status is :

- " *ON* "
- " *Alive* "
- " *Valid* "

Reference **HP-SOFDIR-1553-REQ-0230**

The BC shall maintain, for each " *Valid* ", " *ON* ", " *Alive* " RT, a *RTi_TM_Packet_nb* counter of the TM packets successfully acquired.

*

Reference **HP-SOFDIR-1553-REQ-0235**

Deleted

*

Reference **HP-SOFDIR-1553-REQ-0240**

A TM packet transfer shall be considered as failed, if during any of the message transfer related to the TM packet, one of the bits 4, 5, 6, 7 defined in §3.2.1 is set to " one ".

*

Reference **HP-SOFDIR-1553-REQ-0250**

These *RTi_TM_Packet_nb* counters shall be reset (to zero) at each period T_{RT} of TBD seconds.

*

Reference **HP-SOFDIR-1553-REQ-0260**

At each period T_{RT} , before reset, the counters shall be compared to the minimum number of expected packet for a given RT, *Min_RT_TM_nb*.

T_{RT} shall be expressed in integer number of frame (ie the minimum monitoring period is 1s)

*

Reference **HP-SOFDIR-1553-REQ-0270**

Both T_{RT} and *Min_RT_TM_nb* parameters shall be defined within the Satellite DataBase, for each RT, and, if necessary, for each operating mode of the RT.

*

Reference **HP-SOFDIR-1553-REQ-0280**

At each period T_{RT} if the number of properly acquired TM for a given RT is lower than the expected number,

- If the RT is not already yet "*Sick_TM*", the BC shall raise a TM(5,1) event to signify the anomaly,
- If the failed RT is not yet declared "*Sick_TM*", it shall be declared "*Sick_TM*"
- The relevant RT FDIR shall be triggered if one single " Non Vital" RT is found "*Sick_TM*".
- The CDMS FDIR level 3 recovery shall be engaged if
  - several RT's are declared *Sick_TM* (in that case the failure is assumed located at BC level)
  - one Vital RT is found "*Sick_TM*.

*

Reference **HP-SOFDIR-1553-REQ-0285**

If, at the end of the TFL TM FDIR sequence a RT is declared "Sick_TM", it shall only be set back "Well_TM" upon dedicated TC.

Default RT status is "Well_TM".

*

It must be pointed out that the setting of the *Min_RT_TM_nb* parameters for each RT is based both on the expected amount of packets to be acquired over a given time range, and on the needed monitoring accuracy. It is nevertheless not a critical issue : a very straightforward setting would simply be to have, for all RT's :

Min_RT_TM_nb = 1

This would essentially detect a RT failing into "silent". However, different values, mode dependent, could possibly refine the failure detection.

In addition to the basic principle, the possibility - mainly for ground analysis purpose - to have the BC monitoring, at the time of polling, the validity of the TM Packet Transfer Request put by a RT at SA10T has been analyzed. This intended to precisely time locate the anomaly by which a RT does not have TM to send while it should, by reporting the " invalid " TM PTR together with the corresponding subframe number. However, this mechanism has been eventually discarded considering the overhead it implies on the amount of telemetry generated : a failed RT could lead to up to 20-30 TM events generated in a second before the failure is isolated by the mean of the basic TM FDIR principle described before.

3.3.3.2 TM acquisition FDIR - RT side

It has been mentioned in §3.3.1 that the main FDIR activities would generally be in charge of the BC ; however, for a deeper ground analysis, it is necessary to have the RT monitoring and reporting any identified anomaly in the TM TFL protocol. As illustrated in Fig.3.3-3, this is essentially performed through the analysis of the TM Packet Transfer Confirmation command word put by the BC to RT SA10R in response to a correct TM packet acquisition.

To summarize,

Reference **HP-SOFDIR-1553-REQ-0290**

– When a TM packet transfer attempt for a given RT happens at subframe n (the polled RT being identified in the data word of the Sync message at the beginning of each subframe), the RT shall assess the validity of the TM PTC during the subframe n+1.

*

Reference **HP-SOFDIR-1553-REQ-0300**

– The TM PTC shall be stated as " Invalid " if

- the TM PTC layout is incorrect
- the TM PTC does not report the corresponding TM PTR content ; especially if the TM PTC packet count field is different from the TM PTR one.

*

Reference **HP-SOFDIR-1553-REQ-0310**

– If the TM PTC is declared " Invalid ", The RT shall report the content of the last Invalid TM PTC with the corresponding subframe n number within the RT status word at SA1T. The Invalid TM PTC report shall be cleared every one second.

*

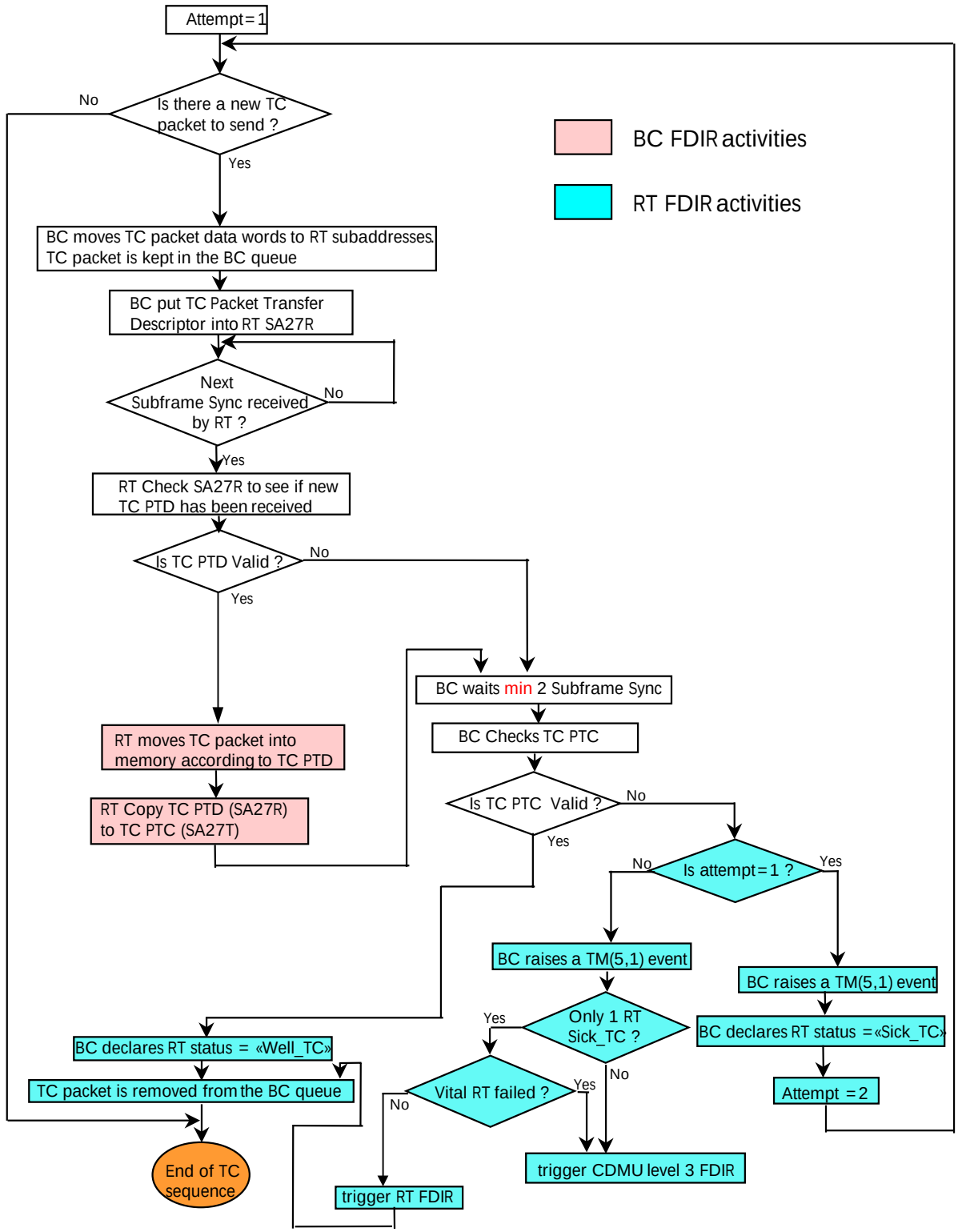

Figure 3.3-1 : TFL TC protocol flow chart & FDIR

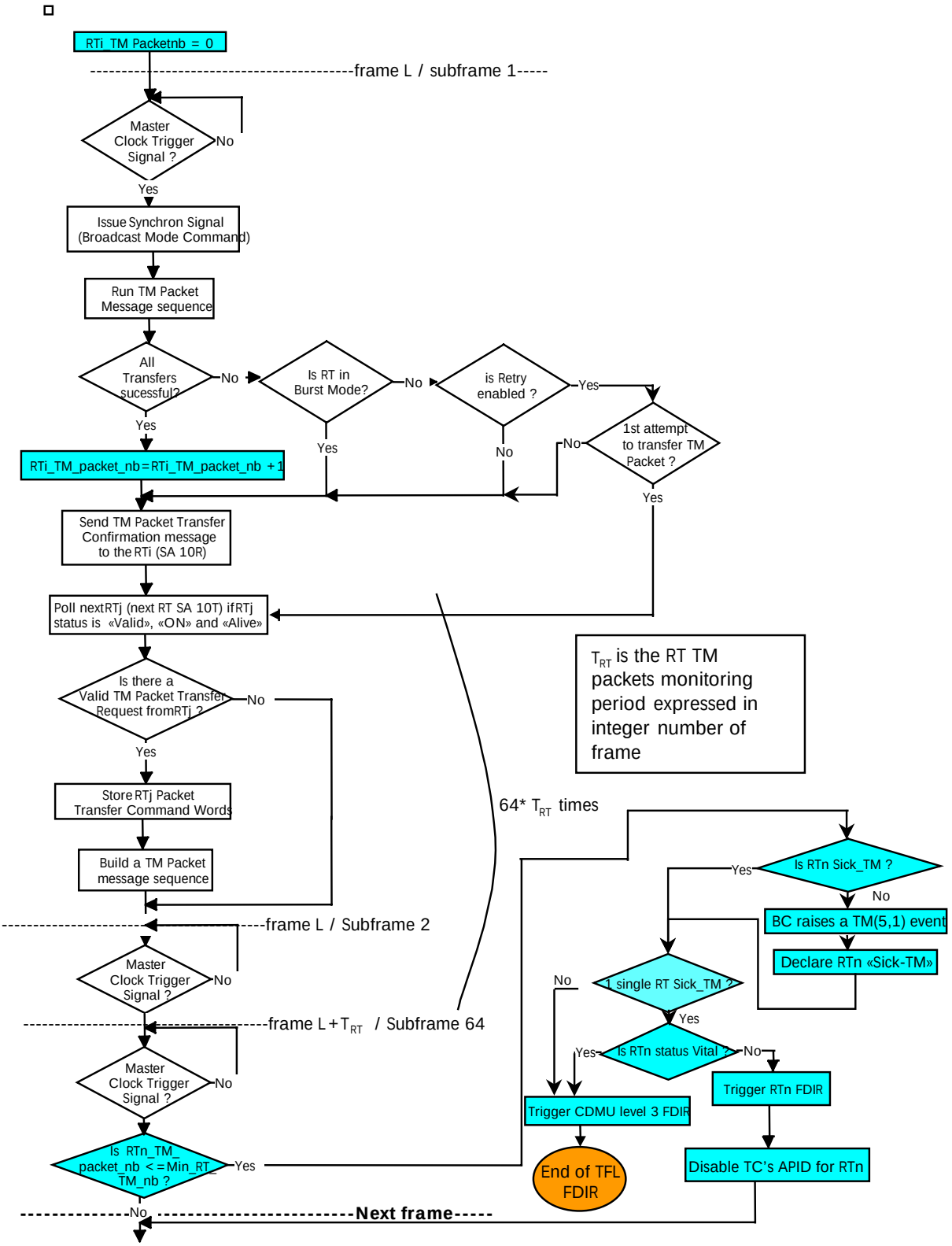

Figure 3.3-2 : TFL TM protocol flow chart & FDIR from the BC

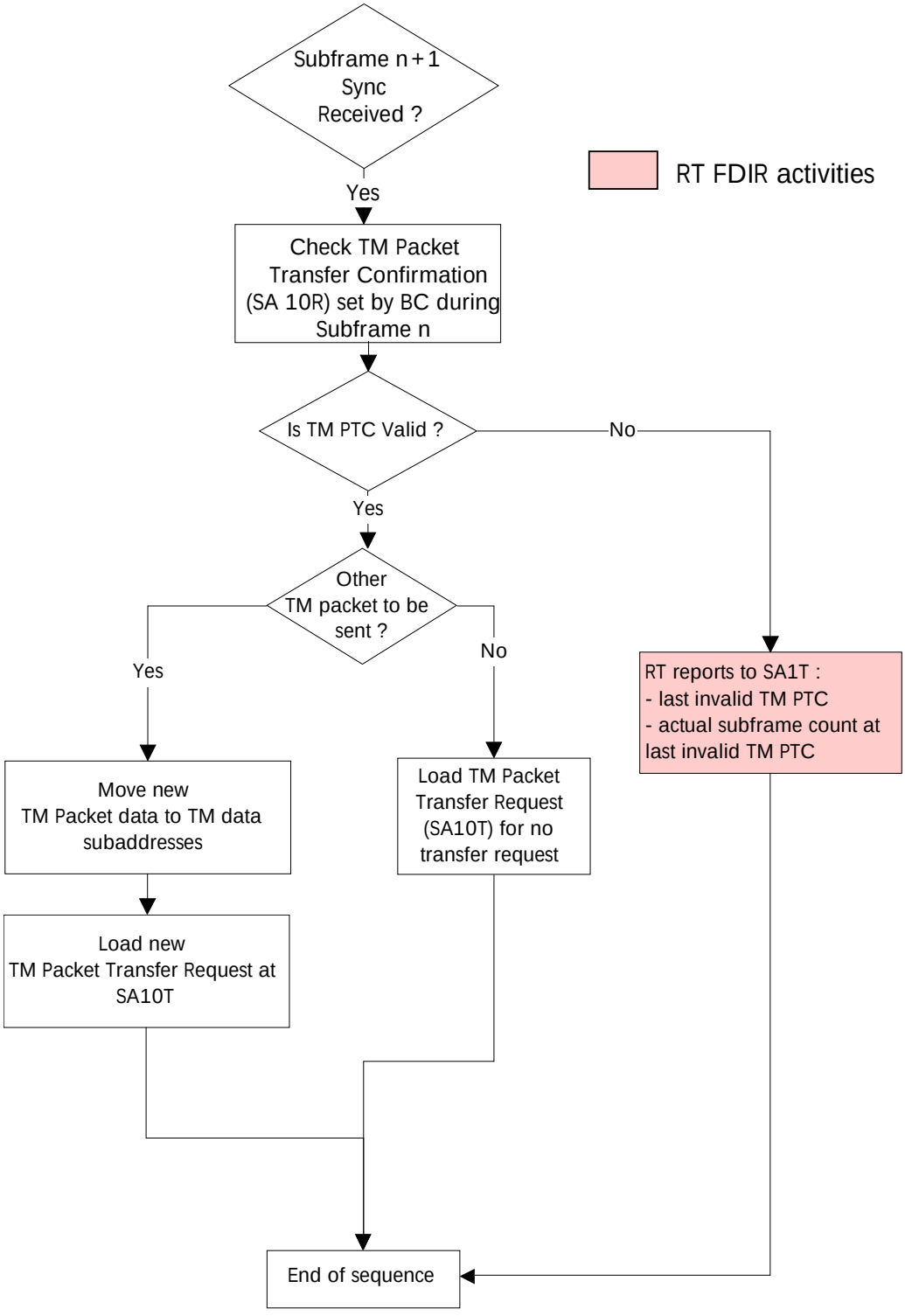

Figure 3.3-3 : TFL TM protocol flow chart & FDIR from the RT

4.CONCLUSION

The present annex has described simple criteria for the checking of the consistency of the data transfers on the 1553 Bus. To summarise :

At Data Link Layer level, derived from AD01 requirements, the FDIR is fully handled at BC level, and is based on the checking, for each 1553 message, of 3 bits reported by the BC hardware. The recovery intends to minimize the outage and is ultimately completed by the bus switch over the B redundancy. The DLL FDIR applies to all RT's.

At Transfer Layer level, for TC transmission the FDIR is performed within the BC and essentially relies on the analysis of the TC PTC message word. It implements a retry capability and graduates the recovery action depending on the identified error source. For TM acquisition the FDIR is based on the monitoring by the BC of the number of acquired TM packets over a given time range. This number is then compared to an expected packet production rate for each RT. A retry capability is also implemented, as stated in AD01, annex 9. The TFL FDIR applies only to the intelligent RT's.

- END OF DOCUMENT -