▼
ALC▲TEL
SPACE

HERSCHEL / PLANCK

Operational concept
H-P-1-ASPI-TD-0263

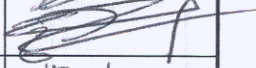#### Product Code : 00000

	HERSCHEL / PLANCK TEAM	Date	Signature
Rédigé par/Written by	F. CHATTE	27.06.02	
Vérifié par/Verified by	P. COUZIN	28/6/02	
Vérifié par/Verified by	P. RIDEAU	29/06/02	
Vérifié par/Verified by	C. MASSE	28/06/02	
Approbation/Approved	J.J. JUILLET	29/06/02	

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

▼
ALC▲TEL
SPACE

SPIRE-ALC-DOC-002355

HERSCHEL / PLANCK

System Database Specification

Operational concept

H-P-1-ASPI-TD-0263

Product Code : 00000

	HERSCHEL / PLANCK TEAM	Date	Signature
Rédigé par/Written by	F. CHATTE		
Vérifié par/Verified by	P. COUZIN		
Vérifié par/Verified by	P. RIDEAU		
Vérifié par/Verified by	C. MASSE		
Approbation/Approved	J.J. JUILLET		

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

ENREGISTREMENT DES EVOLUTIONS / CHANGE RECORDS

ISSUE	DATE	§ : DESCRIPTION DES EVOLUTIONS § : CHANGE RECORD	REDACTEUR AUTHOR
01/00	15/06/02	Issue 01 revision 00	F. CHATTE

TABLE OF CONTENTS

List of figures

List of tables

Note introductory

This document is based on an internal ASPI guide to elaborate operational concept.

The ASPI guide provides a check list of points to address in order to build the contents of the operational concept. Each item of the Check List is referenced in this document as (CL#xx).

Due to Herschel / Planck program customization, mainly in what concern the ground equipment and operation which are not of contractor responsibility, some items of the check list are not covered or as been grouped. The list and object of the non covered items is the following :

CL#13	Operations cost constraints	Not contractor responsibility
CL#14	Operational organization	Not contractor responsibility
CL#16	Philosophy of operation sharing	Not contractor responsibility
CL#17	Backup strategy for MOC	Not contractor responsibility
CL#18	Resource allocation	Not contractor responsibility
CL#19	Centralization or not of operations	Not contractor responsibility
CL#23	Impacts of orbit maintenance activity	grouped in CL#22
CL#26	Delay and means to anomaly diagnosis	grouped in CL#25
CL#27	Reconfiguration delay	grouped in CL#25
CL#27b	safe mode	grouped in CL#25
CL#31	MOC Man Machine interface	Not contractor responsibility
CL#32	MOC design	Not contractor responsibility
CL#33	MOC layout	Not contractor responsibility
CL#34	MOC administration	Not contractor responsibility
CL#35	MOC dimension	Not contractor responsibility

1. SCOPE (CL#1)

1.1 General presentation

The scope of this document is to insure that all the operational constraints imposed externally to the Herschel and Planck spacecraft's have been taken into account in the spacecraft's design in order to cover the spacecraft's operations requirements from launch preparation up to end of live, no "desorbitation" being foreseen.

The operational external constraints are mainly expressed in the applicable documents (ADx) and concern :

- on the spacecraft side
  - the launcher,
  - the environment (including orbit),
- On the ground side,
  - the ground station,
  - the MOC,
  - the instruments ground equipment
- On the operation side,
  - The way the spacecraft shall be operated,
  - The way the autonomy and FDIR shall be implemented.

The operational external constraints do not include the AIT ones as far as they are considered as internal ones, except for constraints associated with SVT tests.

However the AIT is requested to used as far as possible the same observability / commandability capacities of the spacecraft in order to insure to the maximum extend the commonality between operations and AIT, this is achieved by using the same system database, even if some records can be dedicated to operation or AIT, and by running test procedure as closed as possible from the operation procedures during IST.

The life duration of Herschel is specified to be nominally 3,5 years (requirement for helium capacity with a margin of 10%) extended up to 6 years.

The life duration of Planck is 21 months and is limited by the helium for 0.1K dilution cooler.

1.2 Applicability (CL#2)

On one hand, this document is used as an input for the specification relevant to the observability / commandability at spacecraft level, subsystem level and equipment level.

On the other hand, this document shall be consistent with the constraints imposed by the MOC (ESOC), the HSC and ICCs (Herschel) and DPCs (Planck).

This document covers the whole space segment (spacecraft / ground station / MOC) from the launch up to the end of live of the spacecraft.

Except if specifically mentioned, this document applies both to Herschel and Planck.

1.3 Status (CL#3)

The current issue 01 reflects the design at PDR.

Early in phase C/D the detail of the interfaces shall be completed mainly at protocol level and the mission scenario shall be completed.

During phase C/D, some specific chapters can be detailed, mainly in what concern the impact of the observability / commandability as implemented on the ground segment.

2. APPLICABLE AND REFERENCE DOCUMENTS (CL#4)

2.1 Applicable documents

The applicable documents are the ones in which are specified the constraints which applied to Herschel and Planck spacecraft's as specifications or as ICD's.

AD1	SCI-PT-RS-05991	Herschel / Planck - System requirements specification [SRS]
AD2	SCI-PT-RS-07430	First / Planck - System AIV requirements specification
AD3	SCI-PT-RS-07360	Herschel / Planck - Operations interface requirements document [OIRD}
AD4	SCI-PT-ICD-07418	Herschel / Planck - Space / ground interface control document [SGICD]
AD5	SCI-PT-ICD-7527	Herschel / Planck - Packet structure interface control document [PSICD]
AD6 (1)	S2K-MCS-ICD-0001-TOS-GCI	SCOS-2000 - Database import ICD
AD7	SCI-PT-IIDA-04624	First / Planck - Instrument interface document [IID-A]
AD9	SCI-PT-IIDB/HIFI-2125	IID part B - HIFI
AD10	SCI-PT-IIDB/PACS-2126	IID part B - PACS
AD11	SCI-PT-IIDB/SPIRE-2124	IID part B - SPIRE
AD12	SCI-PT-IIDB/HFI-4141	IID part B - HFI
AD13	SCI-PT-IIDB/LFI-2142	IID part B - LFI
AD14	H-P-1-ASPI-IS-0121	EGSE interface requirement specification

(1) For Herschel / Planck applicable issue is 5.1

2.2 Reference documents

Reference documents are the one in which the observability / commandability requirements shall be included.

RD1	SCI-PT/12759	Reference mission scenario
RD2	PT-MOC-SYS-TN-0101-TOS-OGH	Technical note – Autonomy
RD3	FP-MA-RP-0010-TOS/GMA	First/Planck Carrier Consolidated Report on Mission Analysis (CREMA)
RD4	H-P-1-ASPI-SP-0209	System operation & FDIR requirements
RD5	ESA PSS-04-106	Packet telemetry standard
RD6	ESA PSS-04-107	Packet telecommand standard

2.3 Acronyms

ACC   Attitude Control Computer

ACMS   Attitude Control and Measurement Subsystem

AD	Applicable Document	
AFO	Autonomous Fail Operational	(FDIR mode)
AFS	Autonomous fail Safe	(FDIR mode)
AIR	ACMS In Reconfiguration	
AIT	Assembly, Integration and Test	
AM	Acquisition Mode	
ASPI	Alcatel Space	
AIV	Assembly, Integration and Verification	
AUT	Science Mode - Autonomy	
AVM	AVionic Model	
BUV	Bus Under Voltage	
CCU	Cryostat Central Unit	
CDMS	Command and Data Management Subsystem	
CDMU	Central Data Management Unit	
CIR	Computer In Reconfiguration	
CL	Check List	
CLTU	Command Link Transmission Unit	
CREMA	Consolodated Report on Mission Analysis	
DOD	Depth Of Discharge	
DPC	Data Processing Centre (Planck)	
DTCP	Daily TeleCommunication Period	
EDAC	Error Detection And Correction	
EGSE	Electrical Ground Support Equipment	
EQM	Engineering Qualification Model	
ESA	European Space Agency	
ESOC	European Space Operations Centre	

ES-V	An Ariane 5 launcher version
FDIR	Failure Detection, Isolation and Recovery
GMSK	Gaussian Minimum Shift Keying
HSC	Herschel Science Centre
HFI	High Frequency Intrument (Planck)
HIFI	Heterodyne Instrument (Herschel)
HK	Housekeeping
HPC	High Priority Command
HPSDB	Herschel / Planck System Data Base
H/W	Hardware
ICC	Instrument Control Centre
ICD	Interface Control Document
IDSN	Integrated Service Digital Network
IID	Instrument Interface Document
IOCR	In Orbit Commissioning Review
IST	Integrated System Test
LEOP	Launch and Early Orbit Phase
LFI	Low Frequency Instrument (Planck)
LGA	Low Gain Antenna
MGA	Medium Gain Antenna
MOC	Mission Operations Center
MTL	Mission Time Line
NDIU	Network Data Interface Unit
NRZ-L	Non Return to Zero Level
OBCP	On-Board Control Procedure
OBSW	On Board SoftWare

OCM	Orbit Correction Mode
OD	Operational Day
OIRD	Operations Interface Control Document
OOL	Out Of Limit
PACS	Photoconductor Array Camera Spectrometer (Herschel)
PCDU	Power Control and Distribution Unit
PCM	Pulse Code Modulation
PDR	Preliminary Design Review
P/L	Payload
PM	Phase modulated
PSICD	Packet Structure Interface Control Document
PSK	Phase Shift Keying
QRS	Quartz Rate Sensor
RA	Rate Anomaly
RAM	Random Access Memory
RCS	Reaction Control Subsystem
RD	Reference Document
RF	Radio Frequency
RFW	Request For Waiver
RM	Reconfiguration Module
SAS	Sun Acquisition Sensor
SBM	Stand By Mode
S/C	Science
S/C	SpaceCraft
SCM	SCience Mode
SCOE	Specific Check Out Equipment

SCOS	Spacecraft Control and Operations System
SGICD	Space / Ground Interface Control Document
SGM	SaveGuard Memory
SIR	Satellite In Reconfiguration
SM	Survival Mode
SP	Sun Pointing
SPIRE	Spectral photometer imaging receiver (Herschel)
SP-L	Split Phase Level
SRS	System Requirement Specification
SSCE	Sun/SpaceCraft/Earth
SSMM	Solid State Mass Memory
STR	Star Tracker
SUM	Satellite Users Manual
SVF	Software Validation Facility
SVM	SerVice Module
SVT	System Validation Test
S/W	Software
TC	TeleCommand
TBC	To Be Confirmed
TBD	To Be defined
TBW	To Be Write
TM	TeleMetry
TOT	Thruster On Time
TTC	Tracking Telemetry and Command
TWTA	Traveling Wave Tube Amplifier
VC	Virtual Channel

3. SYSTEM AND MISSION (CL#5)

ESA has planned two important missions (merged in one system) for performing astronomical investigations in the infrared and submillimetre wavelength range:

- **Herschel** is an observatory type mission, and is the fourth cornerstone mission (CS4) of the "Horizon 2000" programme. Herschel will carry three instruments (HIFI, SPIRE, and PACS) for high and medium resolution spectroscopy, imaging and photometry over the sub-millimetre and far-infrared range. A 3.5 m telescope will focus the incoming radiation on the Focal Plane Units of these instruments.
- **Planck** is a survey type mission, and is the third Medium mission (M3) of the "Horizon 2000" programme. Planck will provide a definitive high-angular resolution map of the cosmic microwave background anisotropies over at least 95% of the sky and over a wide frequency range. A 1.5 m telescope will focus the incoming radiation on the focal plane shared by the two instruments (LFI and HFI).

Herschel and Planck will be launched by Ariane 5 in the first quarter of 2007. They will operationally travel Lissajous orbits around Lagrange point L2 of the Sun-Earth system.

Herschel and Planck payloads will be supported by Service Modules for maintaining the conditions proper to ensure spacecraft life, scientific observation and communication with ground. The two service modules will have large similarities.

4. MAIN PARTS OF SYSTEMS (CL#6)

4.1 Parts

The complete system is composed of two spacecraft Herschel and Planck and associated ground segments. Each spacecraft executes a specific mission.

The two missions share :

- The same launcher,
- The same kind of orbit (Lissajous orbit around L2),
- The same ground stations.

The launcher is an Ariane 5 ES/V with an upper stage delayed ignition. Herschel is separated first in 3 axis mode, then Planck is separated in spin mode. During launch period, Ariane can potentially change the Herschel configuration by sending commands to cryostat.

The orbits of Herschel and Planck differ only by the amplitude. Herschel is on a large Lissajous orbit which main characteristics are : up to 800000 Km in Y direction (in the ecliptic plan and orthogonal to the sun earth direction) and up to 500000 Km amplitude out of ecliptic plan (Z direction). In order to prevent the Earth and the moon to enter the Planck field of view and generate unacceptable straylight, the Sun / Planck / earth angle is limited to 15 degrees which imposes insertion manœuvre at the arrival at L2 to reduce the amplitude. The Planck orbit around L2 will has the following characteristics : up to 300000 in Y direction and 250000 in Z direction. Those different orbits have minor impacts on the visibility period of the two spacecraft. In a first approximation the visibility period from a ground station, is the same for both Herschel and Planck, however due to different orbit amplitudes, the beginning and the end of the period can differ a little bit between the two spacecraft.

The two spacecraft use the same ground stations. As far as, for a ground station, the visibility period is the same, they have to share the visibility period. the following ground stations are planned to be used depending of the mission phase :

MISSION PHASE	GROUND STATION	
Initial orbit phase	ESA Network (Kourou / New Norcia / Villafranca)	
Commissioning phase	New Norcia / Kourou (routine)	Villafranca (emergency)
Performance verification phase	New Norcia / Kourou (routine)	Villafranca (emergency)
Routine operations phase	New Norcia 35 m (Prime station)	Villafranca / Kourou (emergency)

table 1 : Ground stations and mission phase

For telemetry, depending of antenna and ground station, the following bit rates and telemetry contents are supported.

	Antenna	Ground Station	HERSCHEL	Planck	TM/TC mode
TM Hi-rate	MGA	New Norcia	1.5 Mbps	1.5 Mbps	Real time HK + mem. dump. Real time HK + real time science + mem. dump.
TM medium-rate	MGA	New Norcia / Kourou	150 kbps	150 kbps	Real time science + real time HK.
TM low-rate	LGA	New Norcia	5 kbps	5 kbps	Real time HK (S/C + P/L)
		Kourou	500 bps	500 bps	Real time HK with Kourou 15 m.

table 2 : TM rate / antenna / ground station

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 4kbs is also possible. The various TC mode are summarised in the following table; they are identical for Herschel and Planck.

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

table 3 : TC rate / antenna / ground station

The two missions use also identical :
- MOC (SCOS2000, Database, …).

Even if there is one Mission Operation Center per spacecraft, they will be identical and use the same SCOS2000 version and the same database environment.

In addition the spacecraft design is such that a maximum of commonality between Herschel and Planck service modules (SVM) is achieved. The RF subsystem differs only by the fact that Planck has three LGA, Herschel has two. the power subsystem is the same. The CDMS is the same, except the software which is compiled with different parameters. The AOCMS is different however they have some common equipment : ACC, STR.

The main specificity's are :
- The instruments,
- The cryostat for Herschel,
- The Sorption cooler for Planck,
- The AOCS behavior (Herschel is 3 axes stabilized, Planck is low spinner),
- The mission centers (HSC and ICC's for Herschel, DPCs for Planck),

4.2 Internal interfaces
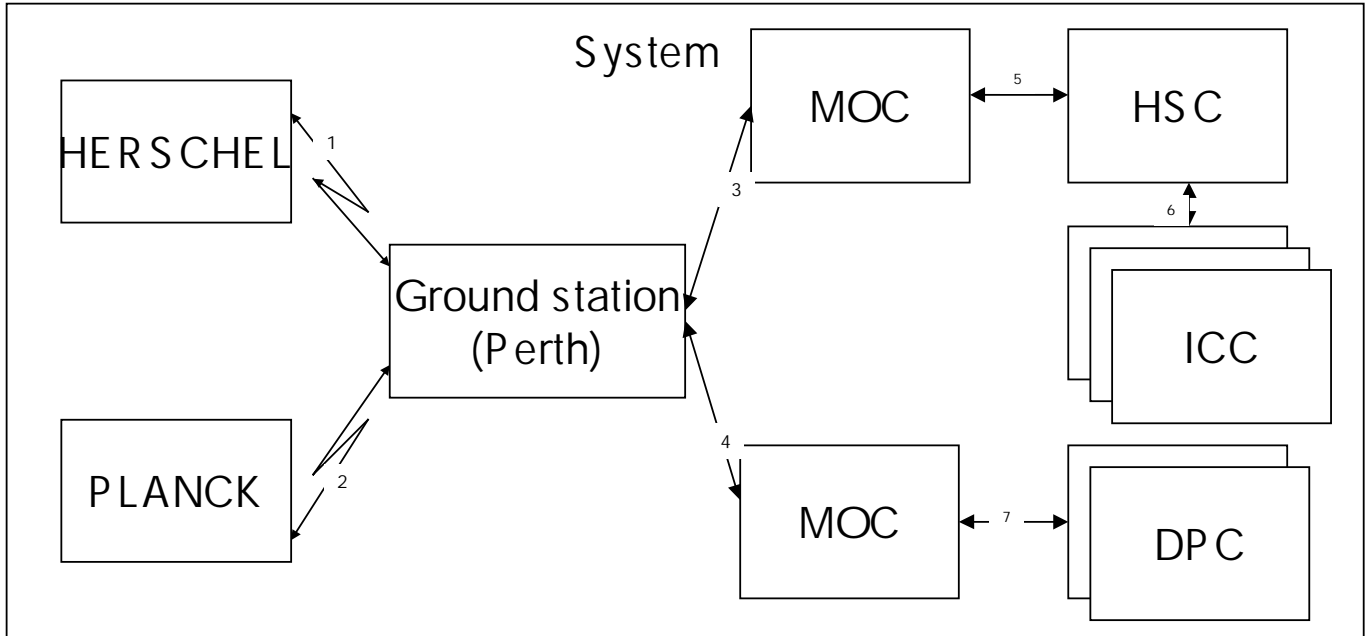
Figure 1 - Internal interfaces

4.2.1 Interface 1 : TM/TC Herschel

Depending of mission phases the ground station can be only New Norcia or both New Norcia and Kourou. Kourou ground station will be used in parallel with New Norcia ground station during the first phases of Herschel Mission : LEOP, transfer to L2, commissioning and performance validation. In case of emergency the Villafrancha ground station can be used.

During normal operation this link will be used during 3 hours per day. However this duration can be reduced or extended depending of Herschel needs , the seasons and the position on the orbit. The coverage of the New Norcia ground station being between 7 hours in (local) summer and 13 hours in (local) winter.

4.2.1.1 TM Herschel interface characteristics

- Herschel TM RF frequency   8468.5 MHz (TBC)   Emission bandwidth : 7MHz

- Herschel TM sub-carrier frequency in function of the bit rate
  - Low bit rate (500bps)   45884.000Hz (sine)
  - Low bit rate (5kbps)   45884.000Hz (sine)
  - Medium bit rate (150kbps)   Not applicable
  - High bit rate (1.5Mbps)   Not applicable

- Herschel TM modulation in function of the bit rate
  - Low bit rate (500bps) PCM(NRZ-L)/PSK/PM
  - Low bit rate (5kbps) PCM(NRZ-L)/PSK/PM
  - Medium bit rate (150kbps) PCM(SP-L)/PM
  - High bit rate (1.5Mbps) GMSK

- Herschel TM encoding. It is the same for the four bit rates and is the standard concatenated one : convolutional 1/2 plus Reed-Solomon (223,255). as consequence the information rate (fb) and the transmitted symbol rate (fs') are the following in function of the bit rate :
  - Low bit rate (500bps) fb = 500.0065 fs' = 1147.1000
  - Low bit rate (5kbps) fb = 5000.0645 fs' = 11471.0000
  - Medium bit rate (150kbps) fb = 150001.9351 fs' = 34413.0000
  - High bit rate (1.5Mbps) fb = 1500019.3511 fs' = 344130.0000

- Transfer frame. Transfer frame protocol is compliant with RD5. The spacecraft identifier is still TBD. The allocation of the virtual channel is the following :
  - VC0 Real time HK telemetry Priority : 1
  - VC1 Real time science telemetry Priority : 4
  - VC2 Dump spacecraft and science HK telemetry Priority : 3
  - VC3 Dump science telemetry Priority : 5
  - VC4 Real time HK telemetry Priority : 2
  - VC7 Idle frames Priority : 6

- Segmentation. No segmentation (except for type (21,x) TM packets : those packets are not processed at MOC level but only at mission center level)
  TM packet source. Compliant with RD5.
  Maximum length of a TM packet source is 1024 octets.

- TM packet source data field header and data field layout. Compliant with AD5.

4.2.1.2 TC Herschel interface characteristics

- Herschel TC RF frequency 7207.8483 MHz (TBC) Emission bandwidth : 3MHz

- Herschel TC subcarrier frequency 16kHz idependently of the bite rate

- Herschel TC modulation PCM(NRZ-L)/PSK/PM independently of bit rate

- CLTU. Compliant with RD6.

- Transfer frame. Transfer frame protocol is compliant with ARD6. The spacecraft identifier is still TBD. The allocation of the virtual channel is the following (TBC) :
  - VC0 Nominal decoder
  - VC1 Redundant decoder
  The 2 MSB of frame length are always zero as far as the maximum frame length is 256 octets.

- Segmentation. No segmentation. The Map Id allocations are TBD. The aggregation is supported (several packet telecommand inserted a TC segment data field.

- TC packet. Compliant with RD6. The sequence counter is such that the three most significant bits are used to identify the source, the eleven less significant bit are used as the counter for the corresponding source. The source allocation is the following :
  - "000" = ground
  - "001" = MTL
  - "010" = CDMS (except MTL)
  - "011" = ACMS
  The maximum length of a TC packet is 248 octets.

- TC packet data field header and data field layout. Compliant with AD5.

4.2.2 Interface 2 : TM / TC Planck

as Herschel

4.2.2.1 TM Planck interface characteristics

- Planck TM RF frequency   8455.0 MHz (TBC)   Emission   bandwidth   : 7MHz

- Planck TM sub-carrier frequency in function of the bit rate
  As Herschel

- Planck TM modulation in function of the bit rate
  As Herschel

- Planck TM encoding
  As Herschel

- Transfer frames
  As Herschel. Spacecraft identifier is TBD.

- Segmentation. As Herschel

- TM packet source. As Herschel

- TM packet source data field header and data field layout. As Herschel

4.2.2.2 TC Planck interface characteristics

- Planck TC RF frequency   7196.3580 MHz (TBC)   Emission   bandwidth   : 3MHz

- Planck TC subcarrier frequency
  As Herschel

- Planck TC modulation.
  As Herschel

- CLTU.
  As Herschel

- Transfer frame.
  - As Herschel. The spacecraft identifier is still TBD.

- Segmentation.
  As Herschel

- TC packet.
  As Herschel

- TC packet data field header and data field layout.
  As Herschel

4.2.3 Interface 3 : Ground station / Herschel MOC

This interface is used to control the ground station and to exchange TM and TC under TBD format. There is one dedicated interface for Herschel supporting 256 kbits. As consequence some, the high bit rate TM shall be buffered at ground station level.

TBW

4.2.4 Interface 4 : Ground station / Planck MOC

Dedicated Planck interface. As Herschel.

TBW

4.2.5 Interface 5 : Herschel MOC / HSC

This interface is used with the following functional protocol during the ground preparation activities relevant for the next (update) and next+1 (new) OD : the MOC sends to the HSC the spacecraft constraints (for instance : the period of unavailability for scientific operations), the HSC sends back the observation plan.

The downloaded science data during DTCP will be transferred to HSC via this interface.

In addition this link will also support the transfer from MOC to HSC of relevant TC packets and TM packets (Instrument housekeeping, instrument memory dump, …) .

Open point : Is this link used also to transfer data base file ?

4.2.5.1 From MOC to HSC

TBW

4.2.5.2 From HSC to MOC

TBW

4.2.6 Interface 6 : Planck MOC / DPC's

There will be two identical interfaces from Planck MOC to each DPC (One DPC per instrument).
This interface is not known currently.
TBW

4.3 External interfaces
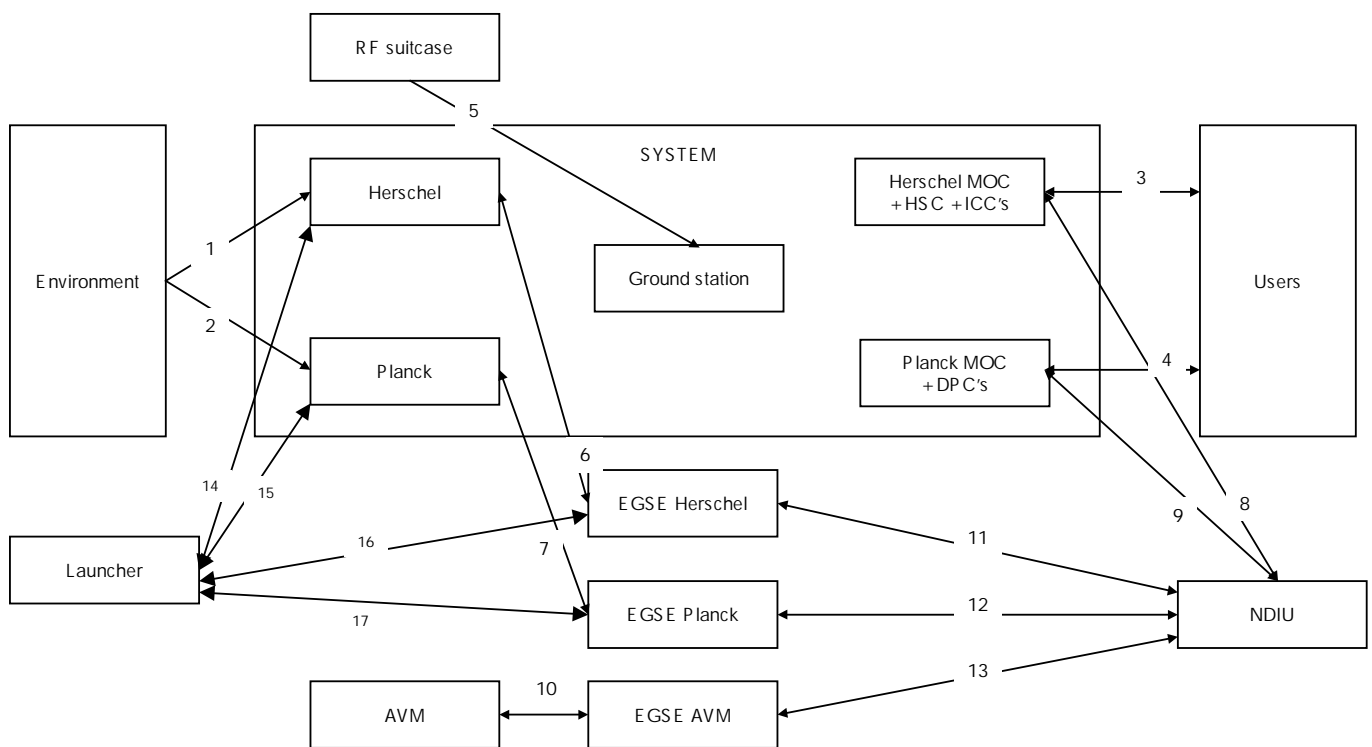
Figure 2 - external interface

4.3.1 Interface 1 : Herschel spacecraft / environment

HERSCHEL is a three-axis stabilised, observatory type satellite. Its typical scientific mission consists in pointing successively at various targets in the sky according to a predefined schedule.

At any time in the mission, the whole sky is not accessible. This is due to the fact that the cold payload has to be protected from the Sun to remain operational. Any rotation around the Sun direction is allowed as it does not change the lighting conditions. Rotations around the perpendicular to the Sun direction are constrained in order to limit the size of the shield protecting the payload. The constraints are shown in Figure 4.4-1.

- 90 ± 30 deg from X_s axis around Pitch axis (Y_s axis)
- 1 deg around Roll axis (X_s axis is the telescope line of sight).

The sunshield protecting the payload has thus to be designed such that no part of the cryostat or telescope are hit by the Sun light for any Sun direction within the allowed ones.

These constraints have top be met during the whole mission, from launcher separation. During launch, the launcher constraints leads to violation of the Sun aspect Angle requirements. Since the SRR, the allowed Sun direction in roll has been reduced from 5 deg down to 1 deg.
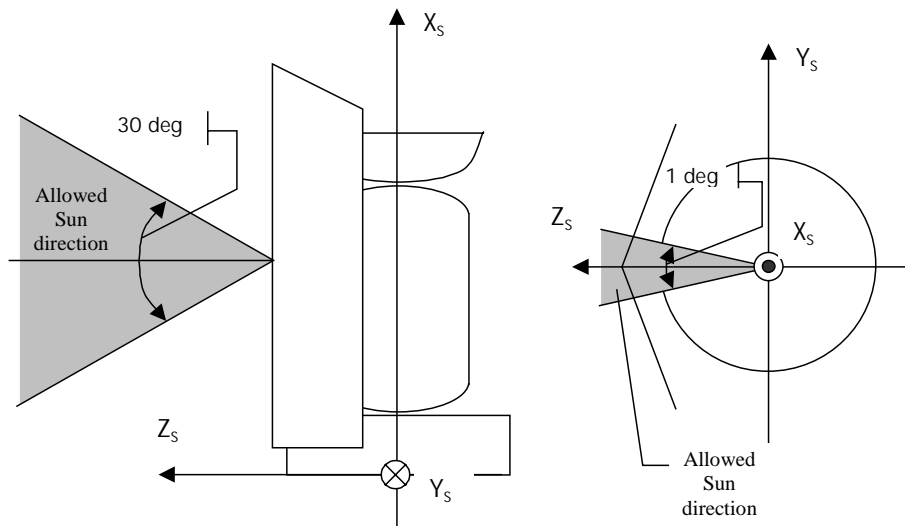
Figure 3 : HERSCHEL ATTITUDE CONSTRAINTS

A $\pm$ 30 deg rotation is allowed in Pitch (Y_s)

while $\pm$ 1 deg is allowed in Roll (X_s).

The spacecraft is free to rotate around Z_s

4.3.2 Interface 2 : Planck spacecraft / environment

The PLANCK attitude profile is very different from the one from HERSCHEL. PLANCK is a spinner which systematically scans the celestial sphere to produce a sky map. As shown in Figure 4.4-2, the PLANCK spin axis is normally opposite to the Sun, with the telescope line of sight at 85 deg from the spin axis. During one rotation, the instruments scan a sector of the celestial sphere with an angular diameter of 85 deg.

In order to view the celestial poles, it is thus mandatory to be able to depoint the spin axis by from the Sun direction. A scanning law which depoints the spin axis at 10 deg maximum from the Sun will be defined, in order to achieve scientific objectives. This means that the spacecraft has to be compatible with a maximum angle of 10 deg between the spin axis and the Sun. This is shown in Figure 4.4-3.

Due to the fact that PLANCK is in orbit around L_2, it makes one rotation around the Sun per year. The spin axis has also to rotate at the same rate to remain Sun pointed. This is achieved by making regular precession manoeuvres which also includes out of plane motion to achieve the PLANCK scanning law. This scanning law is constrained by the fact that the angle between the spin negative axis (-X_S) and the direction from satellite to Earth has to remain below 15 deg.
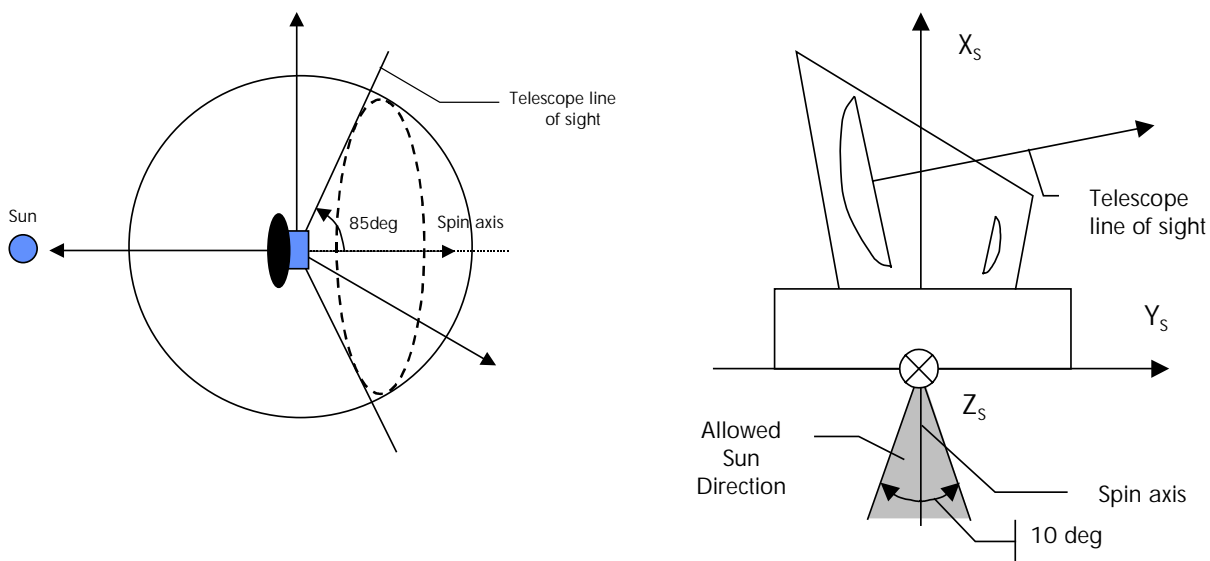
Figure 4 : Planck observation strategy and Planck attitude constraints

4.3.3 Interface 3 : Herschel ground equipment / user

TBW

4.3.4 Interface 4 : Planck ground equipment / user

TBW

4.3.5 Interface 5 : Herschel - Planck / RF suitcase

The RF suitcase provide a TM interface with the ground station. this interface is the same as the Herschel TM interface (refer to §4.2.1.1) or the Planck TM interface (refer to §4.2.2.1) depending of RF suitcase configuration.

The RF suitcase provides a TC interface with the ground station. This interface is the same as the Herschel TC interface (refer to §4.2.2.1) or the Planck TC interface (refer to §4.2.2.2).

Due to RF frequency change complexity, the RF suitcase configuration will be changed only once. It will be first configured as Planck because the AVM EQM transponder will be integrated inside RF suitcase after RF AVM tests, then it will be configured in Herschel. The AVM use the Planck EQM transponder because it is the most critical for test purpose.

4.3.6 Interface 6 : Herschel spacecraft / Herschel EGSE

This interface is limited to the EGSE interface on launch pad. So the interface is done via the umbillical. This interface is used to configure the spacecraft before launch, and to monitor it up to launch.

This interface includes :
- TM interface - RF level via RF fairing window or NRZ-L via umbilical
- TC interface - NRZ-L via umbilical
- Power interface - 28V Bus alimentation via umbilical

4.3.7 Interface 7 : Planck spacecraft / Planck EGSE

As Herschel (refer §4.3.6).

4.3.8 Interface 8 : Herschel ground equipment / NDIU

TBW (IDSN line)

4.3.9 Interface 9 : Planck ground equipment / NDIU

As Herschel (Refer §4.3.8)

4.3.10 Interface 10 : AVM / AVM EGSE

TBW

4.3.11 Interface 11 : NDIU / Herschel EGSE

The NDIU is used to route TC from MOC to the spacecraft and to route TM from spacecraft to MOC during SVT tests and listen-in tests. This interface is different depending of NDIU configuration.

In case of "Normal NDIU" the TM interface is NRZ-L.

In case of "NDIU lite" the TM interface is done at TM transfer frame level and the TC interface at TC CLTU level both over a TCPIP interface.

Question : is the NDIU (lite) used for launch configuration to provide ESOC with spacecraft configuration at launch time ?

4.3.12 Interface 12 : NDIU / Planck EGSE

As Herschel (refer §4.3.11)

4.3.13 Interface 13 : NDIU / AVM EGSE

As Herschel (refer §4.3.11)

4.3.14 Interface 14 : Herschel spacecraft / launcher

TBW

4.3.15 Interface 15 : Planck spacecraft / launcher

TBW

5. SPACE SEGMENT (CL#7)

5.1 Parts and responsibility

To operate nominally the two spacecraft's, the prime is in charge to deliver :
- Herschel spacecraft,
- Planck spacecraft,
- The Herschel / Planck common system data base and Flight Dynamics Data (HPSDB)
- The Herschel SUM (including normal and recovery procedures),
- The Planck SUM (including normal and recovery procedures)

In addition to support software evolution, procedure validation, investigations, … the prime is in charge to deliver :
- All on-board software sources (including OBCP's),
- SVF,
- AVM test bench and associated EGSE and ground software

The ground station, the MOC and the procedures executed on the MOC are customer responsibility.

5.2 Space segment internal interfaces

The internal interfaces are the same than the ones described at system levels. The interfaces between the MOC and HPSDB is done via bridge files, the interface between the SUM and the MOC is TBD (most probably manually).
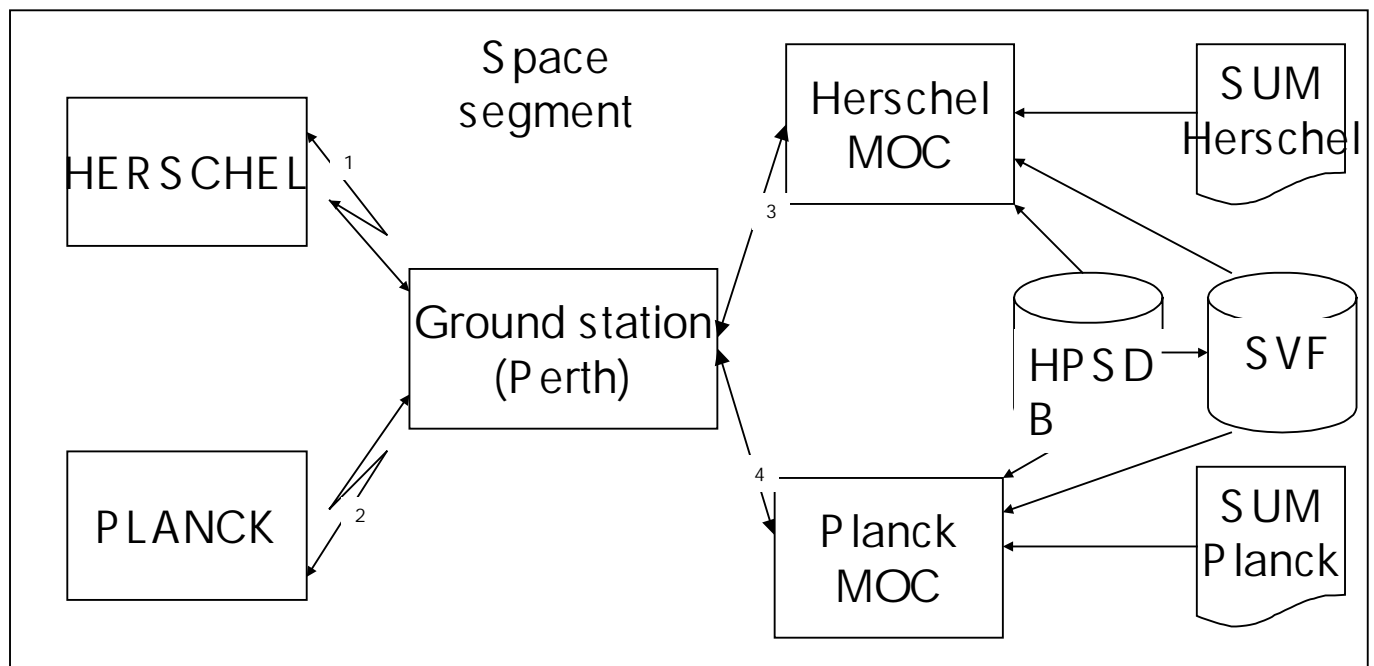
Figure 5 : space segment - internal interfaces

5.2.1 Interface 1 : Herschel spacecraft / environment

As for system internal interface (refer §4.2.1).

5.2.2 Interface 2 : Planck spacecraft / environment

As for system internal interface (refer §4.2.2).

5.2.3 Interface 3 : Ground station / Herschel MOC

As for system internal interface (refer§4.2.3).

5.2.4 Interface 4 : Ground station / Planck MOC

As for system internal interface (refer§4.2.4).

5.2.5 Other interfaces

The other interfaces between :
- HPSDB to Herschel MOC (refer to RD4),
- HPSDB to Planck MOC (refer to RD4),
- HPSDB to SVF

Are off line interfaces and are supported via bridge files.

The other interfaces between :
- Herschel SUM to Herschel MOC,
- Planck SUM to Planck MOC

for nominal and contingency procedures transfer are not yet defined.

6. EXTERNAL INTERFACES OF SPACE SEGMENT (CL#8)
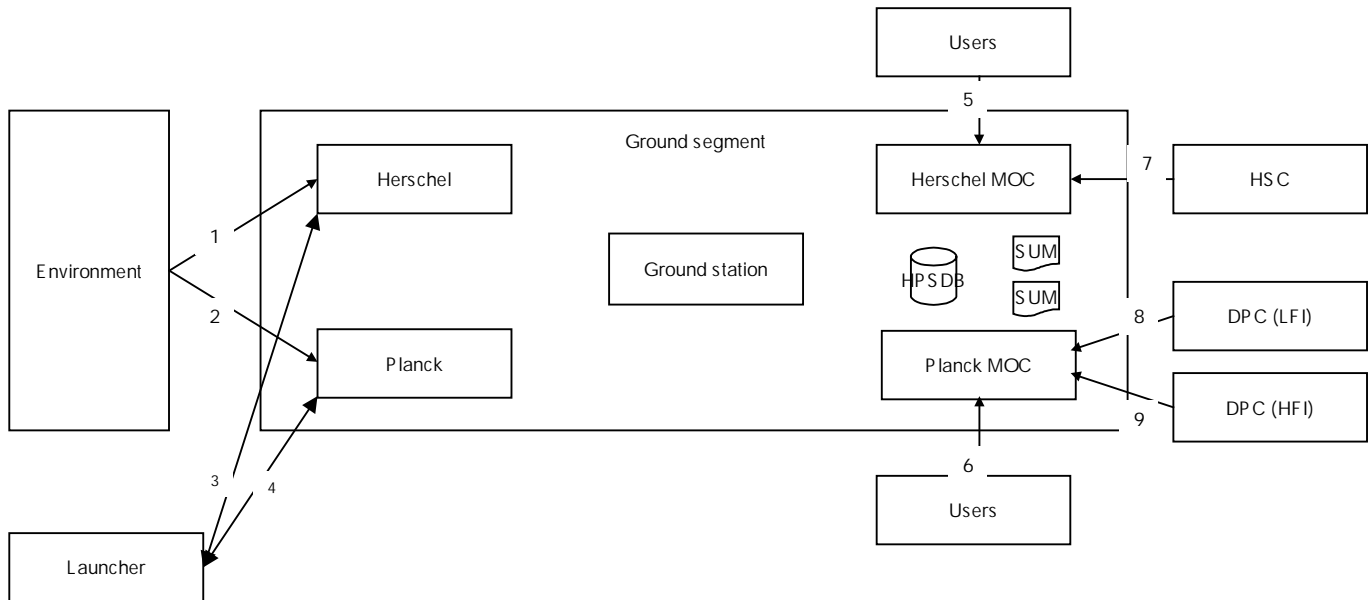
Figure 6 : Ground segment external interface

6.1.1 Interface 1 : Environment / Herschel spacecraft

As Interface 1 of system external interface (refer §4.3.1)

6.1.2 Interface 2 : Environment / Planck spacecraft

As Interface 2 of system external interface (refer §4.3.2)

6.1.3 Interface 3 : Launcher / Herschel spacecraft

As Interface 14 of system external interface (refer §4.3.14)

6.1.4 Interface 4 : Launcher / Planck spacecraft

As Interface 15 of system external interface (refer §4.3.15)

6.1.5 Interface 5 : user / Herschel MOC

As Interface 3 of system external interface (refer §4.3.3) limited to MOC interface.

6.1.6 Interface 6 : user / Planck MOC

As Interface 4 of system external interface (refer §4.3.4) limited to MOC interface.

6.1.7 Interface 7 : Herschel MOC / HSC

As Interface 5 of system internal interface (refer §4.2.5).

6.1.8 Interface 8 : PLANCK MOC / LFI DPC

As Interface 7 of system internal interface (refer §4.2.7).

6.1.9 Interface 9 : PLANCK MOC / HFI DPC

As Interface 7 of system internal interface (refer §4.2.7).

7. ACTORS OF SPACE SEGMENTS (#CL9)

The following phases are defined :
- Launch and early orbit phase (LEOP),
- Commissioning phase,
- Performance verification phase
- Routine operations phase

Phase	begin / end	Responsible	Support	Comments
LEOP	Launch / Lauch + 12 days	ESOC	ASPI (Phase E1)	. ground station : New Norcia , Kourou and Villafrancha
Commissioning phase Concluded by IOCR	4 to 5 weeks for Herschel 4 months for Planck (TBC)	ESOC	ASPI (Phase E1) Instruments	. ground station : New Norcia and Kourou
Performance verification phase	TBD	ESOC	ASPI (Phase E2) Instruments	. ground station : New Norcia and Kourou
Routine operations phase		ESOC	Instruments (if requested)	. ground station : New Norcia

table 4 : Phase / responsibility / support / activities

ASPI is in charge to provide the spacecraft's system and flight Dynamics data bases (HPSDB) and user manuals.

ASPI is also in charge to deliver the SVF, the AVM and associated EGSE which can be used respectively for on-board software maintenance and for procedure validation or investigation.

ESOC is in charge to provide MOC and ground stations.

Instruments are in charge to provide :
- HSC and the ICC's (probably one per instrument + spare ?)
- DPC's (probably one per instrument + spare ?)

During nominal operation, one team per spacecraft (TBC) on a one shift basis per day, seven days per week.

The priority, in case of conflict, between Herschel and Planck, mainly because they share the same ground stations is TBD.

The priority, in case of conflict, between Herschel / Planck and other spacecraft (Rosetta, Mars express, …), mainly because they share the ground stations is TBD.

8. OPERATIONAL SCENARIO (CL#10)

Refer to RD1for a more detailed scenario.

8.1 Preparation

The interfaces between spacecraft and ground stations are validated before launch using a RF "suitcase". The suitcase is representative of spacecraft in what concern the RF interface but also the frame interface and packet interface. The suitcase includes all facilities to analyse received TC and to send representative TM packets.

The MOC functionality and procedures, including the common AIT and operations system database (HPSDB: Herschel/Planck System Data base), are validated first against spacecraft simulator, using representative telemetry generated during spacecraft AIT activities, then against spacecraft itself during System Validation Test (SVT). Three SVT tests are foreseen. During SVT, the spacecraft is controlled from the MOC, however it is still monitored in parallel from the CCS which can take over the spacecraft control in case of anomaly. Additionally, during specific AIT phases, it is possible to perform listen-in tests, during which the spacecraft is fully controlled by the CCS, but the MOC receives in parallel telemetry from spacecraft.

8.2 Non routine scenario

The non routine scenario includes all the operations which shall be performed between the launch and the normal operations of the spacecraft (routine scenario). Even if some operational activities could differ between Herschel and Planck, the major part of the activities are common and, unless otherwise specified, the description of the non routine scenario is common for both Herschel and Planck. This scenario is composed of the following phases:
- Launch and early orbit phase (LEOP)
- Commissioning phase
- Performance and verification phase

prior to start the launch phase, the initial spacecraft configuration shall be determined.

Initial configuration

The initial configuration is set via the CCS. The power is provided by the batteries. The SVM subsystems are powered as defined in §6.5.2.1, the instruments are not except power applied to launch lock devices. Some CDMS and ACMS functions are inhibited up to the separation detection.

Launch and early Orbit Phase (LEOP)

This phase start at launch time (T0) and ends after the second trajectory correction which is planned at T0 + 12 days

During launch phase ARIANE provides "dry loop" relay commands to Herschel CCU to allow opening of cryostat valves. The telemetry emission is inhibited.

After separation detection, the CDMS and ACMS switche autonomously to HK1 mode in order to reach a stable sun-pointed attitude safe for payload, power and communications. 20 seconds after separation the spacecraft is able to transmit HK TM via the LGA and the ACMS is fully operational. Once sun acquisition is achieved transition to HK2 is performed by ground command.

All the operations during this phase are conducted from ground. New Norcia,Kourou and Villafranca ground stations provide a ground coverage of approximately 22 hours per day. During the non visibility period the HK data are stored inside the Solid State Mass Memory (SSMM).

Three manoeuvres are performed during this phase. The first manoeuvre is aim to correct the speed variation at perigee and takes place as soon as possible during the first day. The second manoeuvre is intended to remove the launcher dispersions and takes place at T0 plus 2 days. The third manoeuvre is aimed to remove the previous manoeuvre execution error and takes place at T0 + 12 days and marks the end of the LEOP phase.

The operations will be centred on the checkout of the spacecraft subsystems and the correct transfer trajectory to L2. The following operations are carried out during this phase:
- Establish the correct spacecraft configuration (RF, Thermal control, power, data handling, ACMS, etc .)
- Establish basic spacecraft properties (centre of gravity, moments of inertia)
- Determine spacecraft attitude (and spin rate for Planck)
- Correct attitude (spin rate) if necessary)
- Carry out orbit determination
- Determine optimal attitude and magnetude of the trajectory correction manoeuvre
- Slew to correct firing attitude
- Thruster calibration (TBC)
- Refine magnitude and timing of the burn
- Execute trajectory correction #1
- Determine the orbit
- Repeat for trajectory correction #2
- Slew to optimal attitude for transfer
- (for Planck) Adjust spin rate if necessary
- begin of telescope decontamination heating.

Timeline summary :

Time	Event	Description
T0	Lift-off (H0)	
T0+144.9 sec	Acceleration threshold detection (H1)	
T0+145.7 sec	Booster jettisoning (H1 + 0.78 sec)	
T0 + 196.3 sec	Fairing jettisoning (FJ)	Herschel sun solar aspect constraint applies
T0 + 539.2 sec	End of EOC thrust phase (H2)	

T0 + 545.2 sec	Lower composite jettisoning (H2 + 6 sec)	
T0 + 116 mn	End of coast arc Upper stage ignition (K2.1)	
T0 + 133.2 mn	Spacecraft separation (H3)	Herschel is separated in three axis mode, Planck is separated in spin mode
D1	Manoeuvre	Perigee velocity correction
D2	Manoeuvre	Removal LV dispersion
D12	Manoeuvre	Remove previous manoeuvre correction

Commissioning phase

The commissioning phase starts after the second trajectory correction which is planned at T0 + 12 days and ends at the beginning of performance verification phase.

During this phase, the New Norcia and Kourou ground stations are used, insuring a 10 hours per days of coverage to be shared by Herschel and Planck.

Some operations are performed from the ground, some others are performed autonomously from the MTL.

The mains operations performed are:
- Complete check out of spacecraft functions and verification of all subsystems performances
- Verification of the spacecraft-instrument interfaces
- Instrument switch on and functional check out
- End of telescope decontamination heating
- For Herschel: telescope cool-down and cryo-cover opening
- For Planck: passive cool down to 50 K. Switch-on 20 K cooler and cool down to 20 K. Switch-on 4 K cooler and cool down to 4 K. Switch-on 0.1 K cooler and cool down to 0.1 K.

The commissioning phase duration is expected to be 4 to 5 weeks for Herschel and 4 months for Planck.

For Planck, three manoeuvres are foreseen during this phase. The first manoeuvre is aim to removed accumulated error during cruise and fine targeting and takes place 20 days before injection. The second manoeuvre is intended to inject Planck on its final orbit (15°). The third manoeuvre is aimed to remove injection manoeuvre execution error and takes place at injection + 2 days. No other manoeuvres, other than the ones for orbit maintenance at L2, are foreseen for Planck.

For Planck, during the transfer to L2, the sun spacecraft earth angle which is limited to 15 deg. will be violated during 72 days from day 36 up to day 108 after separation and during 43 days from day 54 to

day 97 after separation this angle will be greater than 25 deg. In this last case, in order to keep the sun direction in the allowed range (10 deg. from spin axis), Planck will be re-oriented and the telecommunication via MGA will no more be possible, LGA has to be used.

Timeline summary :

Time	Event	Description
Day 36	SSCE becomes > 15 deg	Planck : angle spin axis / sun direction lower than 10 deg applies. MGA usage is limited
Day 54	SSCE becomes > 25 deg.	Planck : angle spin axis / sun direction lower than 10 deg applies. MGA no more available
Day 97	SSCE becomes < 25 deg.	Planck : angle spin axis / sun direction lower than 10 deg applies. MGA available but usage limited
Day 108	SSCE becomes < 15 deg.	Planck : no more limitation on MGA usage
Injection - 20 days	Planck manoeuvre	remove accumulated error during cruise
Injection	Planck manoeuvre	Planck injection
Injection + 2 days	Planck manoeuvre	remove injection manoeuvre execution

Performance verification phase

The performance verification phase starts after the commissioning phases.

During this phase, the New Norcia and Kourou ground stations are used, insuring a 10 hours per days of coverage to be shared by Herschel and Planck.

Some operations are performed from the ground, some others are performed autonomously from the MTL.

The mains operations performed are:
- performance verification of CDMS and ACMS
- ACMS sensors calibration
- Instruments performance determination and calibration
- Verification/optimisation of instrument operations.

At the end of PV phase the spacecraft and instrument nominal configurations have been established and all tunable spacecraft and instrument parameters have been set to their optimal operating value.

For Herschel, this phase shall end during the transfer to L2 and routine operations can be started.
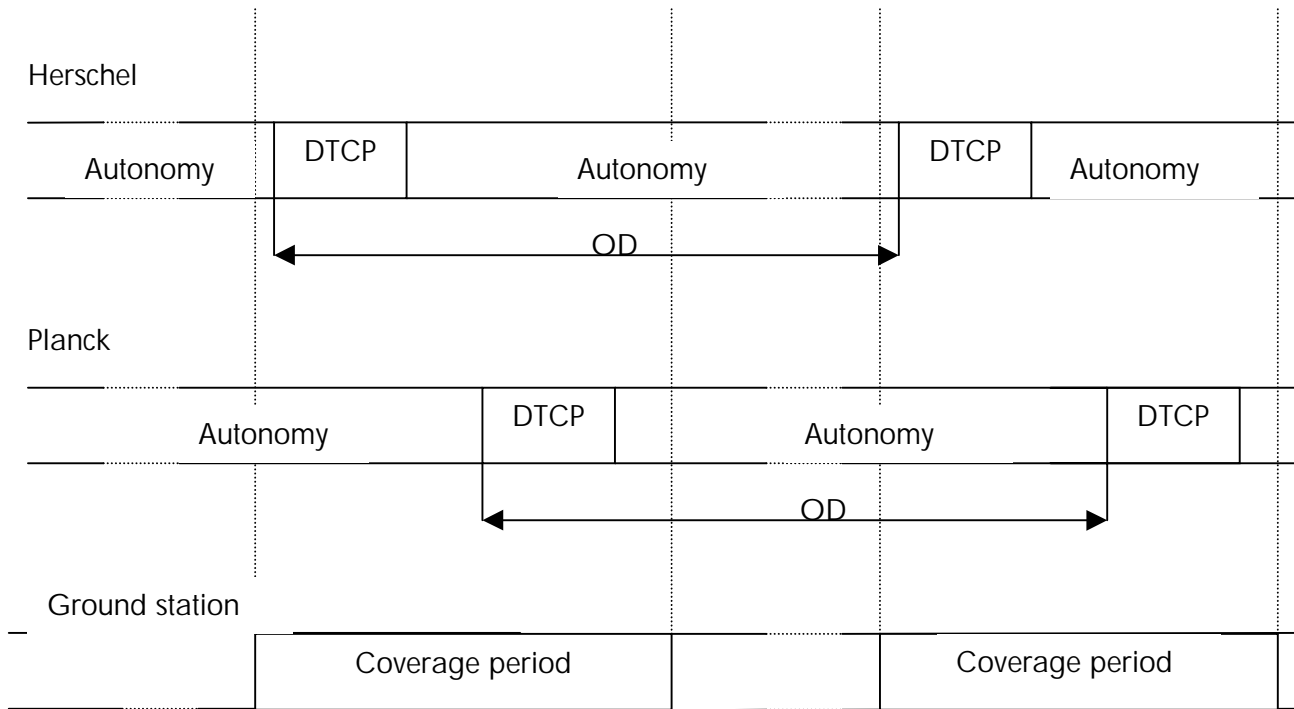
For Planck this phase cannot be completed during the transfer to L2.

From launcher separation until completion of this performance verification phase, the operations are planned to be run in FDIR Autonomous Fail Safe (AFS) mode (see later FDIR and mode description).

8.3 Routine scenario

During normal routine operations in L2, Herschel and Planck share the same ground station: New Norcia. This ground station assures a variable daily coverage for both spacecraft depending of spacecraft position on its orbit and of season. The minimum daily coverage period is 7 hours. The daily coverage is shared by Herschel and Planck. As a consequence, for each spacecraft, each 24 -hour operational day (OD) is divided in two periods:
- 1. The DTCP (Daily Tele-Communication) Period during which the spacecraft is in visibility of the ground station and communicating with the ground (duration between 2 and 3 hours).
- 2. The "autonomy" period during which no communication with the ground takes place and the satellite are operating without ground support (autonomous operations - Duration between 21 and 22 hours).

During this phase orbit maintenance is carried out on the basis of once per month.

DTCP

By convention the DTCP will be at start of the OD. The Herschel and Planck DTCP are run consecutively, the order in which they are run will depends of operational or spacecraft constraints.

When the DTCP period starts the spacecraft should have the following configuration:
- TM is medium rate via MGA (that means that the spacecraft is pointed to earth)
- TC is nominal rate via LGA1/Transponder1 and LGA2 / Transponder2 (which insures that the TC can be sent to the spacecraft even if the earth pointing is not met).

During DTCP period the following activities shall be performed by ground (unless disabled, the autonomous activities from MTL continue to be carried out):
- 1   Initial activities
  - Signal acquisition at medium rate
  - perform ranging for some minutes (TBD) (TM can be received and TC can be send in parallel)
  - Switch to high rate
- 2   Spacecraft assessment
  - Assess spacecraft and instrument health
  - Assess the status of the operations which happened during the 'autonomy' period
- 3   Housekeeping activities
  - Carry out specific spacecraft operations e.g. reaction wheel unloading, star tracker calibration, etc …
  - Carry out specific instrument housekeeping activities e.g. cooler recycling for PACS and SPIRE
  - Uplink a new schedule for up-coming operations
  - Implement any diagnostic procedure planned during the DTCP e.g. dump of specific parameters or memory areas (spacecraft and/or instruments)
  - Implement any corrective action required
  - Re-plan for failure cases
- 4   Science data recovering (this activity is run in parallel with the other as far as a dedicated low priority virtual channel is allocated)
  - Recover the stored scientific data
- 5   Completion activities
  - Switch to medium rate
  - perform ranging for some minutes (TBD) (TM can be received and TC can be send in parallel)
  - stop TM transmission.

During DTCP, for Planck, the scientific operations continue autonomously from MTL, for Herschel they can continue autonomously from MTL according to constraints of the spacecraft pointing to earth, to constraints associated to cooler recycling for PACS / SPIRE and to constraints associated to incompatibility of HIFI with X-band TM. In both cases the scientific data are recorded in the SSMM and simultaneously dumped to ground.

Autonomy

During autonomy period, the spacecraft normal activities are driven from the MTL. The MTL is such that it covers all the activities to be performed during the next 48 hours in case the next DTCP is missed. In case of failure detection, to the maximum extend the scientific mission will be carried out. Depending of failure gravity, either the normal MTL will continue, or the current sub-schedules impacted by the failure will be stopped but the other running sub-schedules and the future ones are executed nominally.

An Herschel, oversimplified autonomous sequence operation can be:
- ACMS calibration (10 minutes)

- Instrument initialisation: transition from stand-by to prime, warm up, stabilisation, selection of instrument mode (30 minutes)
- Slew to target # 1 (10 minutes)
- End of slew: On Target Flag (OTF) set high in spacecraft TM
- Pointing on target #1, data collection, HK and science TM to CDMS (duration 60 minutes)
- Slew to target #2: OTF set low in spacecraft TM
- (Optionally) mode change (a few seconds up to a few minutes)
- End of slew: OTF set high in spacecraft TM
- Pointing on target #2, data collection …
- time slot blocked for spacecraft activities (duration 15 minutes)
- …
- …
- Pointing on target #n (last target)
- Instrument from prime to stand-by.

A Planck oversimplified autonomous sequence operation can be (Planck is a survey type mission and as the instruments operate in parallel autonomous sequence of operations are simpler than the Herschel ones):

- ACMS calibration (10 minutes)
- Every 45 minutes (in average) precession manoeuvre to follow the scanning law,
- Spacecraft activities (if needed, in parallel to science observation),
- Scanning law execution (including regular precession manoeuvres).

During autonomy period the ground prepares the activities which will be carried out during the DTCP and the MTL which shall cover the next 48 hours.

9. DATA FLOW (CL#11)

TBW (to be derived from the internal and external interfaces of the space segment and from RD1, this chapter shall described the functional exchange and their dependencies).

10. HIGH LEVEL REQUIREMENTS (CL#12)

After separation, each spacecraft autonomously detects the separation, and reorients itself to achieve sun-pointing of the solar arrays.

> This supported via on-board ACMS software. For Herschel the following AOCMS sensors : SAS and GYRO and the following actuators : RCS are used. For Planck the following AOCMS sensors : QRS and SAS and the following actuator : thruster 10N are used.

20 seconds after separation the spacecraft is able to transmit telemetry via LGA.

> This is supported by the fact the EPC of the TWTA is switched ON in pre-heating mode at launch.

Each spacecraft can operate 48 hours without ground contact and without interrupting the mission.

> This requirement is mainly supported via the SSMM size and MTL size which are compliant for 48 hours of continuous science operation. The SSMM size is 25 Gbits end of life. The MTL is stored inside the SSMM and 35Mbits are allocated. The SSMM is supposed to support :
> * Spacecraft HK : 844 Mbits (5 kbits/s)
> * Instrument data (Science + HK) : 23 Gbits (140 kbits/s)
> * MTL : 35 Mbits (100 sub-schedules per day of 100 max length TC : 100 * 100 * 2 days * 226 bytes)
> * OBCP : negligible
> * Video camera : 180 Mbits

To the maximum extend, in case of failure detection, spacecraft shall continue normal operations.

> This requirement is mainly supported via FDIR in AFO mode and MTL. The FDIR detects the error and depending of its level and of equipment failure, some sub-schedules of the MTL are stopped (they were active at failure occurrence time) , and, during the recovery phase, some are not triggered, however some sub-schedules, not concerned by the failure, continue their normal execution (they were active at failure occurrence time) or, during recovery phase, are triggered nominally. When a sub-schedule is stopped all the running OBCP, and their children if any, triggered by this sub-schedule are also stopped. The switching to autonomy mode is done only on FDIR level 4 error detection or on ground command.

The switching to safe mode shall be trigger on major failure or from ground

> This requirement is implemented via software and hardware in case a failure level 4 is detected and via dedicated telecommand.

The spacecraft shall survive in a safe mode for 7 days.

> This requirement is mainly supported via software to keep the attitude constraints.

11. SITE LOCATIONS (CL#15)

The ground stations are used in function of the mission phase (refer to §4.1), however they are driven from Darmstadt.

Ground station	Longitude East (deg)	Latitude North (deg)
Kourou 15m, French Guyana	-52.80	5.25
New Norcia 35m	116.21	-30.97
Villafranca	-3.95	40.45

table 5 : Ground station location

Each spacecraft MOC will be located in ESOC (Darmstadt - Germany) and supported by a redundant (cold or hot ?) SCOS-2000 system. This has the advantage that in normal operation mode via the New Norcia ground station, the DTCP will take place during normal working day period.

The HSC, ICC's, and DPC's are located in Villafranca (Spain).

12. CONSTRAINTS AND PERFORMANCES OF SPACECRAFT ACCESS (CL#20)

During their full life Herschel and Planck share the same ground station. Mainly during normal operation they share the New Norcia ground station.

During normal routine operations in L2, Herschel and Planck shared the same ground station: New Norcia. This ground station assures a variable daily coverage for both spacecraft depending of spacecraft position on its orbit and of season. The minimum daily coverage period is 7 hours. The daily coverage is shared by Herschel and Planck. As a consequence, for each spacecraft, each 24 -hour operational day (OD) is divided in two periods:

- The DTCP (Daily Tele-Communication Period) during which the spacecraft is in visibility of the ground station and communicating with the ground (duration between 2 and 3 hours).
- The "autonomy" period during which no communication with the ground takes place and the satellite are operating without ground support (autonomous operations - Duration between 21 and 22 hours).

Refer to chapter 8 for main activities performed during DTCP and "autonomy" phases.

On a basis of 100 sub-schedules of 100 TC of 226 bytes, it will take approximately one hour and a half to load a 24 hours MTL.

On a basis of TM generation at 150 kbits/s on board, it will take approximately 2 hours and a half to download the data generated during the last 24 hours.

The spacecraft design can accommodate for 1 missed pass, having a TM storage capacity sized for 2 full days. Nevertheless the dump of those data shall then be optimized during the "third day" visibility period.

In addition, the ground station can also be used by some other missions (Rosetta, Mars express) which can lead to some potential conflicts.

13. STRATEGY FOR ORBIT ACQUISITION (CL#21)

The orbit correction manoeuvres have been computed with the assumptions described hereafter. Few manoeuvres have been scheduled as presented in Table 4.4-6.

Each manoeuvre has been determined using a guidance scheme which targets to remove the velocity component along the escape direction. A modified approach with a Monte-Carlo simulation with re-optimisation of the transfer Delta-V helps to reduce the required Delta-V. The main hypothesis of the computation are:

- Launcher performances as given in previous section (including a 20% margin)
- Orbit Determination accuracy (typical data)
- Manoeuvre execution error less than 1% in size and 1 deg in pointing at 1 sigma
- Solar radiation bias error of 10%.

All the orbit manoeuvres are considered inertial for HERSCHEL and PLANCK.

date	Delta-V (m/sec)	Purpose	Solar Aspect Angle
T_0 first day	5	Launcher interface	[0-180] deg
T_0 + 2 days	52	Remove launcher dispersions	[0-180] deg
T_0 + 12 days	4	Remove first manoeuvre execution error	[0-180] deg
$T_{injection}$ – 20 days	3	Remove accumulated error during cruise and fine targeting	[0-180] deg
$T_{injection}$ (PLANCK only)	187.5	Lissajous orbit manoeuvre (specification for 6 months launch window)	125 deg
$T_{injection}$ + 2 days (PLANCK only)	5	Remove injection manoeuvre execution error	28.4 or 208.4 deg

Figure 7 : HERSCHEL AND PLANCK ORBIT CORRECTION MANOEUVRES (T0: LIFT-OFF) (A5-ESV, 15 DEG ORBIT)

14. STRATEGY FOR ORBIT MAINTENANCE (CL#22, CL#23)

The objective of the orbit maintenance strategy is to correct the deviations observed on the satellites. Due to the instability of the Lagrangian point, it is necessary to correct these orbit deviations without too much time delay and with a good accuracy.

The Lissajous orbits are not stable orbits: if one solves the linear equation for arbitrary initial conditions, exponential terms with positive exponent appear in the solution for the X and Y components. The initial conditions have to be carefully chosen to get a non-escape orbit with periodic terms and decreasing exponential terms only in the solution.

It can also be proven that any Delta-V performed along a specific direction in the [X, Y] plane, called the non-escape direction, produces a transfer from a non-escape orbit to another non-escape orbit with a different amplitude. This non-escape direction lies in the [X, Y] plane at an angle 61.6 deg from the X axis (see Figure 4.4-17).

On the other hand, Delta-V performed along the escape direction, perpendicular to the non-escape direction, produce a transfer from a non-escape orbit to an escape orbit or vice versa.

The escape direction, with an angle of 28.4 deg to the X axis, is the one used for orbit maintenance: it allows to cancel any unstable terms appearing in the orbit due to external disturbances.
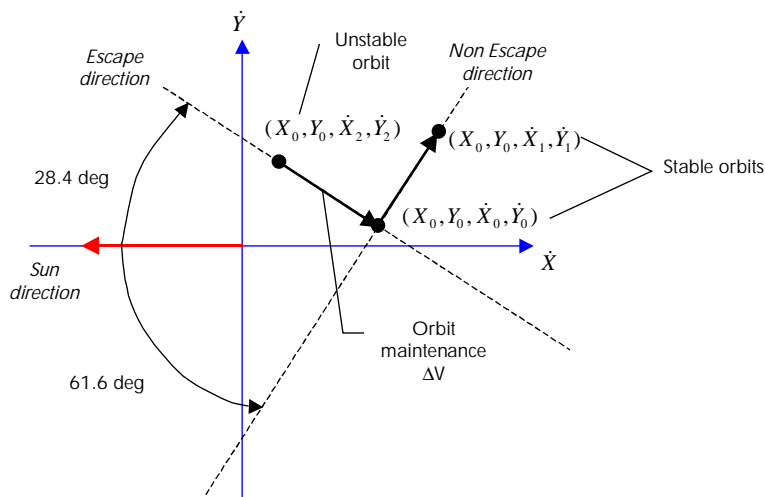
Figure 8 : ESCAPE AND NON-ESCAPE DIRECTIONS IN THE XYZ EARTH ROTATING FRAME

One major factor is the eclipse avoidance which is ensured by the orbit maintenance strategy. This is performed by eclipse avoidance manoeuvre which can be performed, for instance, along the non-escape direction.

Several methods have been applied to compute the orbit correction strategy for both spacecraft. The results give an orbit maintenance cycle including one manoeuvre per month. The amplitudes of the correction may vary but averaged values of 6 m/sec for HERSCHEL, and 2.5 m/sec for PLANCK have been selected for all their mission duration.

15. MISSIONS PERFORMANCES (CL#24)

Due to limited ground contact period (3 hours per day) and to autonomy requirements (48 hours of normal mission operation without ground contact) during each DTCP the following mission plan activities will be performed :
- Update of the next 24 hours if needed,
- Load of the last 24 hours of the next 48 hours.

It will not be possible to react to a mission plan modification in less than 24 hours, and in case of a DTCP is missed this delay will be 48 hours.

In case of an instrument anomaly detection on-board, the reconfiguration will depend of the gravity of the anomaly, to the maximum extend the mission shall be continued normally.

During the DTCP time slots shall be reserved for spacecraft maintenance activities, and the mission timeline shall allow also to insert some dedicated spacecraft activities.

Planck is a spinner which systematically scans the celestial sphere to produce a sky map. Spin axis is normally opposite to the sun, with the telescope line of sight at 85 deg from the spin axis. During one rotation, the instruments scan a sector of the celestial sphere with an angular diameter of 85 deg. In order to view the celestial poles, it is thus mandatory to be able to depoint the spin axis from the the sun direction. A scanning law which depoints the spin axis at 10 deg maximum from the sun is defined in order to achieve the scientific objectives which are "95% of the sky shall be scan over two full sky surveys".

16. ANOMALY DETECTION (CL#25, CL#26, CL#27)

The on-board anomaly will be detected autonomously and in function of the anomaly severity, the spacecraft mode and the FDIR mode autonomous recovery actions will be performed. The MOC shall not be required to send telecommands with response time of less than 3 (TBC) minutes. In addition the situations in which the MOC is required to react in a short time (< 30 minutes) shall be well identified and agreed by ESA. In this last case the telemetry shall allow to unambiguously recognize the situation in which this could happen.

The following chapters group the spacecraft requirements relevant to FDIR per failure detection, failure isolation and failure recovery. During phase C those different chapters will be completed with the ground equipment (ground station, MOC, network, …) requirement relevant for FDIR.

16.1 FD - Failure detection

MOOM-135   The survival mode shall be activated automatically by the spacecraft after a major on-board failure or a violation of the attitude constraints.

MOFM-005   The design shall prevent the lost of the satellite. Any hazardous situation , which will not cause immediate loss but may develop into a loss of the satellite, shall be prevented by design or shall be protected.

MOFM-010   Single failures, which pose a threat to mission objectives, mission life or spacecraft safety shall be eliminated. Where this cannot be achieved, a justification for retention shall be proposed for ESA assessment and approval by a Request For Waiver (RFW).

MOFM-035   Autonomous failure detection and recovery shall not be base on a single sensor readout.

MOFM-055   The spacecraft shall suppress uncontrolled recycling of error reaction functions.

MOFM-060   It shall be possible to enable, disable or reverse any on-board autonomous function or action by ground segment. Exceptions (e.g. power distribution, DC/DC converterqs over-voltage protections, …) shall be identified and agreed.

MOFM-065   The design of fault management systems shall be intrinsically fail-safe.

MOFM-070   All relevant anomalies shall be properly detected and unambiguously reported.

MOFM-075   A clear and adequate fault reporting shall be provided in telemetry.

MOFM-080   A clear and adequate fault diagnosis and identification shall be provided on-board.

MOFM-110   Trigger limits shall have adequate and quantified margins.

MOFM-115   It shall be possible to adjust software parameter values for confirmation time and trigger by ground command.

MOFM-120   Control laws and parameters for autonomous functions shall be capable of being

modified by ground command.

MOFM-130   No nominal operation shall require the deactivation of the on-board protection system.

AUT-3   The spacecraft shall be able to detect failures which are hazardous for the spacecraft or its instruments; if such a condition is detected the spacecraft shall autonomously configure the affected on-board subsystems and instruments into safe lodes of operation. For the following cases (currently TBD) the spacecraft shall be capable of recovering from the failure and continue normal operations.

AUT-7   It shall be possible to enable / disable autonomous entry, and to force manual entry into survival mode by telecommand. Autonomous entry shall be enbled by default.

AUT-8   No nominal operation shall require inhibition of the survival mode nor a forced entry into survival mode.

AUT-9   The management of anomalies within a subsystem or instrument shall be handled in a hierarchical manner such that resolution is sought on the lowest level possible.

AUT-10   All intelligent subsystems and instruments shall perform regular self-checks.

AUT-11   Anomalies and actions taken to recover from them shall be reported in event packets.

AUT-12   It shall be possible to reconstruct from the telemetry the conditions leading to the generation of an event.

AUT-13   The on-board system shall capture sufficient information to enable the ground to analyze failures.

AUT-14   It shall be possible for the ground to enable / disable each individual fault management function.

AUT-15   All parameters used for autonomous fault management (e.g. thresholds for limit checks or thresholds and biases for attitude control), including fault management, orbit and attitude control, etc., shall be updateable by telecommand and available in telemetry.

16.2 FD - Failure isolation

MOFM-015   The spacecraft design shall not include any failure propagation path such that failure from one function / unit causes permanent failure to another function / unit.

MOFM-095   The implementation of any autonomous action shall avois switching back and forth between unhealthy systems.

MOFM-100   An anomaly detection shall be confirmed by using more than one sample of the same measurement.

MOFM-105   The anomaly detection system must ensure that only valid information is used.

16.3 FD - Failure recovery

MOOM-140	The survival mode shall be maintain a safe attitude within the constraints allowing a continuous supply of power and maintaining a thermal environment compatible with the spacecraft and essential loads.
MOOM-145	The survival mode shall insure a two way communication link with the ground station when coverage is available for at least housekeeping telemetry data and commanding (i.e. providing suitable link margins with omni-directional coverage).
MOOM-150	The survival mode shall maintain spacecraft and instruments in safe conditions and broadcast a safe mode flag to the instruments upon entry to the safe mode.
MOOM-155	It shall be possible to enter the survival mode by ground command. Exit from the survival mode shall only be possible by ground command.
MOOM-160	The spacecraft shall be able to maintain the survival mode without any ground contact for at least seven days.
MOOM165	The survival mode shall not rely on any volatile memory (Random Access Memory or other) stored data.
MOOM-170	The exact attitude during the survival mode may not be known, but the attitude constraints shall be satisfied.
MOOM-175	Upon entry in the survival mode, the mission time_line shall be discontinued. the TM format shall be switched to HK mode only.
MOOM-180	If no ground command has been received since more than a ground programmable time and after a minimum time of TBD, the survival mode shall be initiated.
MOOM-185	In case of survival mode is entered because no ground command has been received, an automatic search phase shall be defined in order to re-establish command reception capability.
AUT-2	On-board intelligent units including instruments shall be able to enter their safe mode on receipt of a single TC packet.
AUT-4	The survival mode shall initiate any payload reconfiguration activities necessary to put the payload in a safe and recoverable mode.
AUT-5	When in survival mode the spacecraft shall start generating a minimum set of telemetry packets which allow unambiguous and rapid identification of the survival mode. The reason for the triggering of the survival mode and the history of the defined events occurred before and after the detection of the failure condition shall also be accessible in telemetry either directly or stored in memory areas that can be later dumped and reset by ground.
AUT-6	Essential on-board autonomous functions, including fault management, shall be available in survival mode.

AUT-20	The on-board fault management shall avoid continuous toggling of the configuration of a unit between the prime and the redundant element.
AUT-22	The spacecraft shall have the knowledge of the actual health status of all the hardware units required for any automatic transitions. This information shall be maintained on-board, updateable by telecommand and available in telemetry.
AUT-23	An on-board safety logic shall be available to prevent inadvert commanding of forbidden mode transitions. the table of allowed transitions shall be updateable by telecommand and available in the telemetry.
MOFM-020	redundant units shall have a physical separation between them. If redundancy is implemented in the same box, a metallic separation is required.
MFOM-025	Where redundancy is employed, the design shall allow to operate and verify the redundant item / function independently of nominal use.
MOFM-030	Switch over to redundant units shall be possible without reconfiguration of unrelated units.
MOFM_045	The satellite shall respond to on-board failures by switching, independent from ground control, to redundant functional path. Where this can be accomplished without risk to satellite safety such switching shall enable the continuity of the mission timeline and performance. In the event that alternative redundant paths do not exist or that the failure effect is too complex to allow autonomous recovery, the satellite shall enter survival mode.
MOFM-050	No single failure in the on-board protection system shall cause the spacecraft to go into survival mode.
MOFM-060	It shall be possible to enable, disable or reverse any on-board autonomous function or action by ground segment. Exceptions (e.g. power distribution, DC/DC converters over-voltage protections, …) shall be identified and agreed.
MOFM-085	An expedite and reliable procedure, under ground control, shall be provide to return to nominal operations after a failure.
MOFM-090	Autonomous action shall be implemented at the appropriate level, i.e. at system level if the impact is system wide, at subsystem level if the impact does not reach further than the subsystem and at unit level if the impact is constrained to that unit.
MOFM-120	For any on-board autonomous reconfiguration, telemetry data shall indicated the time and the conditions, at / under which the event occured.

17. FAILURE ANTICIPATION (#CL28)

Some specific procedures shall be provided to allow failure anticipation. Those procedures require for TM to be downloaded, for tools to perform the analysis and for procedures to prevent the failure.

The different failure anticipation and associated procedures, telemetry and tools will be defined during phase C.

Example of such failure anticipation : detection that a temperature is permanently growing on long period and OOL will occur if no corrective actions are performed.

18. IMPACTS OF CONTROL AND COMMAND ON OPERATIONS (#29)

This chapter is provisional and provide the way the control command is intended to be implemented on-board. During phase C, this chapter shall be completed by the impacts of this implementation on the operations.

18.1 Spacecraft system modes

18.1.1 Pre-Launch/Launch Mode

This mode corresponds to a waiting mode of the spacecraft up to the spacecraft separation from ARIANE. It ends by separation detection, which is made by majority voting in the CDMU Reconfiguration module (CDM_RM) on the one hand, and in the ACC Reconfiguration Module (CDM_ACC) on the other hand.

During this mode the following equipment units have to be powered on:
- CDMU Nominal
- ACC Nominal
- CDMS S/W (booted and in a standby mode)
- ACMS S/W (booted and in a standby mode)
- PCDU
- CCU (nominal and redundant) for Herschel
- TTC Receiver (Nominal and Redundant) and EPC in pre-heating mode

During launch mode, power will be provided by the battery. After fairing separation, orientation of the launcher will be such that the Herschel Sun Aspect Angle requirements will be fulfilled (i.e. Herschel Solar Array will be exposed to Sun allowing battery charging). This is however not the case on Planck as its Solar Array will not be exposed to the Sun.

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

When the separation is detected at CDMS level, the Housekeeping mode 1 is engaged.

18.1.2 Housekeeping Modes

The housekeeping modes are the nominal system modes when no scientific operations are performed.

Two housekeeping modes have been defined:
- HK1, which is the initialisation mode at separation
- HK2, which corresponds to the routine mode in absence of routine scientific activity.

18.1.2.1 HK1

The aim of HK1 mode is to reach and maintain a safe sun-pointing attitude. Launcher separation detection initiates the separation sequence program running in the CDMU which commands all activities to perform Sun acquisition and acquire link with Earth.

The separation sequence will power ON the following units :
- RF Transmitter and associated TWTA (the EPC is already in pre-heating mode)
- ACMS sensors and actuators for Sun acquisition mode
- Thruster drivers and cat bed heaters
- RCS latch valve

20 second after separation, the spacecraft is able to transmit telemetry and the ACMS is fully operational. Then, spacecraft can reach and maintain a sun-pointing attitude. Once sufficient sun-pointing is achieved, power generation is automatically switched to Solar Array. Sun-pointing will be observed by the Sun acquisition sensors of ACMS; alternatively it can be detected by monitoring of Solar Array delivered power.

On Planck, the initial spin direction is defined by the launcher and will not change during the mission.

During HK1 mode, communication with Earth on both TM and TC will be performed using omni-directional coverage provided by the LGA. This is imposed by the fact that, at launcher injection and for few tens of minutes, the angle between Earth and Sun seen from the spacecraft is above 90 deg. 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.

In HK1 mode, after separation from the launcher, the TM link budget permits to download at 5 kbps with both New Norcia and Kourou. In this mode, the spacecraft real-time housekeeping rate will be kept low enough such that progressive download of the housekeeping data stored during launch is performed.

In this mode, the payload instruments are "off".

Transition from HK1 mode to HK2 mode will only be performed by ground command.

18.1.2.2 HK2

HK2 mode is the basic housekeeping mode. It is used at the beginning of the mission, during platform commissioning phase. HK2 mode is also used to resume scientific operation after a transition to survival mode.

HK2 mode can be divided into 2 sub-modes:
- When the spacecraft is in ground visibility: HK2/V sub-mode
- When the spacecraft is not in ground visibility: HK2/NV sub-mode

Transition between the two HK2 sub-modes (i.e. HK2/V and HK2/NV) will be performed by ground command but could also be done by timeline service.

HK2/V

In HK2/V mode it is possible to use all modes of the following subsystems:

- ACMS
- CDMS
- TM/TC
- Payload and Instruments
- Power Control Subsystem
- Thermal Control Subsystem

Instruments are individually powered on by ground TC or MTL service and set to a safe mode, following procedures defined by the instruments.

During HK2/V sub-mode, only housekeeping data from the instruments will be collected and transmitted to the ground. The spacecraft receives TC from ground and downloads housekeeping telemetry.

HK2/NV

During HK2/NV sub-mode, Herschel spacecraft will nominally remain in operational pointing mode, 3-axis stabilised with the Z-axis Sun-pointed. Planck will nominally remain in operational pointing mode with the spin axis Sun pointed. Spin axis re-orientation manoeuvres can be commanded in order to maintain the S/C Sun pointed.

Housekeeping data from the instruments (if switched ON) and platform is stored in the mass memory during HK2/NV mode.

18.1.3 Science Modes

Science modes are the spacecraft modes of operation during scientific mission. They can only be entered from HK2 mode and only under ground telecommand or time tagged command from the MTL service.

Science modes can be exited to:
- HK2 mode under ground telecommand or time tagged command
- Survival Modes in case of major failure.

Science modes can be decomposed into 2 modes:
- Scientific autonomy mode (SCI/AUT), which corresponds to the nominal science observation without ground contact
- Telecommunication mode (SCI/TC), which corresponds to phases in ground contact during science activities.

Transition between the two science modes will be triggered by ground command or by time tagged command.

Line of sight calibrations will be conducted in science modes during science commissioning phase. 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 both in the instrument detectors. Science modes will also be used during science commissioning phase to validate proper functioning of the satellite and payload.

During science modes (i.e. both scientific autonomy mode and telecommunication mode), the operations on both Herschel and Planck will follow the commands defined by the on-board mission timeline service.

18.1.3.1 SCI/AUT

On Herschel, the 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:

- 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. There are two other possible operational modes for the payload: SPIRE in Prime mode, PACS in parallel mode performing photometer observations with a degraded sensitivity and spatial resolution. HIFI is in standby mode.

During slew, HIFI and PACS are in standby. 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	COMMENTS
1	Prime	Standby	Standby	
2	Standby	Prime	Standby	
3	Standby	Standby	Prime	
4	Standby	Parallel	Prime	TM rates will be shared between PACS and SPIRE. PACS and SPIRE observe at the same time.
5	Standby	Standby	Specific mode: "Serendipity"	During slew. All TM bandwidth available for SPIRE.

table 6 : Herschel instrument modes

▼ 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

table 7 : Planck instrument modes

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.

During science autonomy mode, the housekeeping data from the platform and instruments, as well as scientific data, are collected and stored in the mass memory for subsequent downloading during a telecommunication period. Instrument data acquisition bandwidth is identical for Herschel and Planck, i.e. 130kbps.

18.1.3.2 SCI/TC

During science telecommunication mode, the spacecraft is 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. Tlecommanding nominally uses the LGA1 (in the Planck -X and Herschel +Z s/C axis) with the MGA kept as back up. This is considered as preferable mainly because it does not required the S/C to be properly Earth pointed which is of particular importance for Herschel which may need a large slew to achieve the MGA pointing towards the earth.

On Planck, the scientific observation will continue nominally in parallel to telecommunication.

On Hershel, the observations will also be carried out in SCI/TC mode provided the antenna earth-pointed constraint is respected. This is ensured by a ± 10 deg field of view MGA, compatible with the maximum Sun/SpaceCraft/Earth (SSCE) angle during mission.

he 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. (Herschel) wheel unloading will be performed during Telecommunication mode (SCI/TC).

For both spacecraft, the payload modes of operations are similar to the ones in science autonomy mode (SCI/AUT). However, on Herschel, some specific payload housekeeping tasks such as coolers recycling will be preferably conducted in science telecommunication mode (SCI/TC).

18.1.4 Survival Modes

When reached in one of survival modes, the spacecraft will be put in **safe conditions** and it shall be able to survive for at least 7 days without ground contact.

Survival modes are only reached in case of major on-board failures (i.e. system failures).

The safe conditions are defined from a spacecraft safe state (i.e. a configuration of each subsystem, which allow the spacecraft to be safe) **and** an instrument state (i.e. safe or OFF).

Communication to ground during survival modes is performed using the LGAs for TM and TC. Omni-directional coverage is provided by the LGAs which allows to receive TC and send TM in any spacecraft attitude.

Transition to survival modes from any other system mode (except HK1 and Launch modes) can be initiated in two ways (TBC) :

- From a ground command (TBC). It happens when, the spacecraft being under ground control, the ground detects an on-board failure.
- After a major on-board failure (e.g. attitude loss). The spacecraft autonomously performs a reconfiguration of the whole system.

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

Survival modes can be decomposed into two modes:

- SM1 for which spacecraft is in a Safe state and the instruments are in a safe mode
- SM2 for which the whole spacecraft is in a Safe state and the instruments are powered off.

The survival mode in which the spacecraft is transitioned (i.e. SM1 or SM2) depends on the kind of failure.

18.1.4.1 SM1

The spacecraft switches to ACMS survival mode[1] and the instruments are transitioned to a safe mode. A safe mode message will be sent to the instrument to initiate proper reconfiguration.

SM1 is entered in case of :

- Loss of proper Sun Pointing (SP) and/or
- Violation of Thruster on Time (TOT) (TBC) and/or
- Rate Anomaly Detection (RA).

18.1.4.2 SM2

In case of transition to SM2, the spacecraft will be put in a safe state (i.e. optimum power generation, stable temperature conditions…) and the instruments will be switched off (including the active cooling system on Planck)

As this could result in the loss of a significant mission time, spacecraft will switch to SM2 only in case of :

- Bus Under Voltage (BUV)
- Battery Depth of Discharge (DOD)

18.1.5 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.

---

[1] The complete primary ACMS-branch with all its units becomes deactivated or switched off and the essential units of the redundant branch of the ACMS start operating in safe sun pointing mode.
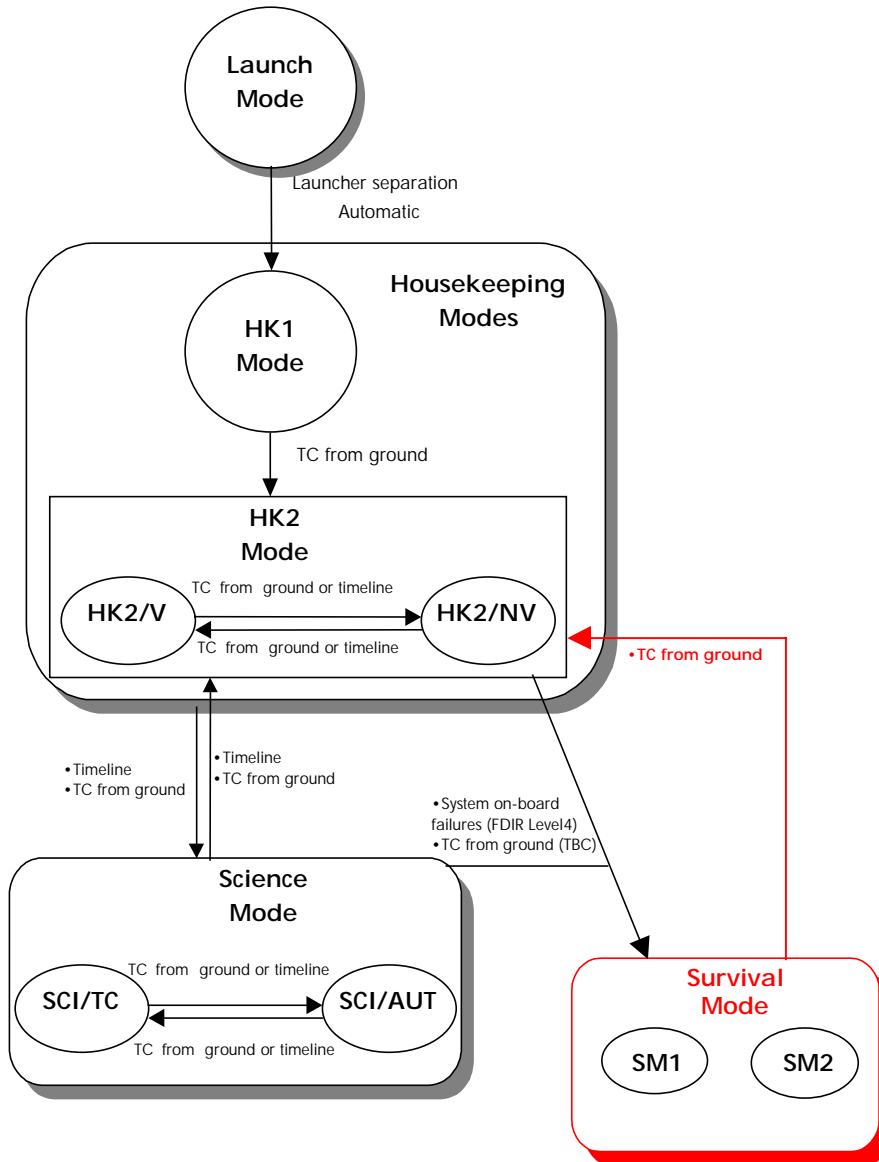
Figure 9 : System Modes transition logic

18.1.6 Modes links and transitions

The following table summarizes the Herschel operational modes. For each of them, the TM/TC mode is driven by the down-link rate and the virtual channels allocation and prioritisation.

SATELLITE MODE	SUB-MODE	TM/TC ANTENNAS	TM DATA RATE	ACMS MODE	PAYLOAD MODES	POWER MODE
Launch		N/A	N/A	SBM	Instruments OFF.	Battery
HK1		TM/TC by LGA + Z/- Z	TM Low-rate	AM	Instruments OFF.	SA
HK2	V	TM/TC by LGA + Z or TM by MGA	TM Medium-rate or High-rate	AM ; SCM; OCM	Instruments OFF or in a safe mode.	SA
	NV	N/A	N/A	SCM; AM		SA
Science (SCI)	Autonomy (AUT)	N/A	N/A	SCM	- 1 instrument Prime; others in a safe mode. - PACS Prime, SPIRE parallel. - SPIRE in serendipity.	SA
	Telecommunication (TC)	TM = MGA TC = LGA + Z	TM Hi-rate / TM Hi-rate / TM Medium-rate	SCM OCM	- 1 instrument Prime; others in a safe mode. - PACS Prime, SPIRE parallel.	SA
Survival	SM1	TM/TC by LGA + Z/-Z	TM Low-rate	SM	Instruments in a safe mode	Battery or SA
	SM2	TM/TC by LGA + Z/-Z	TM Low-rate	SM	Instruments OFF	Battery or SA

table 8 : Herschel operations mode

SATELLITE MODE	SUB-MODE	TM/TC ANTENNAS	TM DATA RATE	ACMS MODE	PAYLOAD MODES	POWER MODE
Science (SCI)	Autonomy (AUT)	N/A	N/A	NOM HCM	- 2 intruments Prime - 1 Prime, 1 in a safe mode	SA
	Telecommunication (TC)	TM = MGA TC = LGA -X	TM Hi-rate / TM Hi-rate / TM Medium-rate	NOM HCM OCM	- 2 instruments Prime - 1 Prime, 1 in a safe mode	SA / SA / SA
HK1		TM/TC by LGA - X	TM Low-rate	SAM/AI	Instruments OFF.	SA

HK2	V	TC = LGA – X TM = LGA – X TM = MGA	TM Medium-rate Or high rate	SAM/AI ; NOM ; HCM ; OCM	Instruments OFF or in a safe mode.	SA
	NV	N/A	N/A	NOM ; HCM		SA
Survival	SM1	TM/TC by LGA + Z/-Z	TM Low-rate	SAM/SM	Instruments in a safe mode.	Battery or SA
	SM2	TM/TC by LGA + Z/-Z	TM Low-rate	SAM/SM	Instruments OFF	Battery or SA
Launch		N/A	N/A	SBM	Instruments OFF.	Battery

table 9 : Planck operations mode

SCM: Science Mode – AM: Acquisition Mode – SM: Survival Mode – SBM: Stand By Mode – OCM: Orbit Correction Mode

18.2 Failure Classification

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 6.5.4.2-1.

Level 4	Level 3	Level 2	Level 1	Level 0
S Y S T E M	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	⋮

table 10 : failure classification

Failure types have been 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).

The different levels are detailed hereafter.

18.2.1 Level 0

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

Level 0 failures are typically:
- <u>EDAC single bit error</u>. 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.
- <u>Arithmetic error in processor module</u>, detected by Software, which raises an internal interruption. A specific recovery procedure is then carried out by software application. This procedure shall contain at least an arithmetic error counter increase and a TM report. The impact on the involved application is negligible and is null on the other applications.

Multiple (number selectable by ground) occurrences of Level 0 failure shall lead to higher level recovery actions (unit/coupler/computer reconfiguration). Then, level 0 failures will be reported to the higher level.

18.2.2 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.

The status of each equipment unit is monitored by the CDMS S/W or the ACMS S/W depending on the unit. This status will be compared to unambiguous thresholds to possibly initiate recovery actions. In case of failure, the ACMS or the CDMS, depending on the failed equipment unit, provides the necessary actions to recover from the detected failure.

Two sub levels are 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.

Failure of these equipment units are detected by related ACC or CDMU software application. Failure detection is based on unit specific health data and operational parameters.

Any ACMS unit reconfiguration action shall be reported to the CDMS, with the past and current unit contexts, and the safeguard memories shall be updated in accordance with the updated spacecraft configuration.

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

Every bus coupler will be checked by the mean of:
- Specific internal health status depending on coupler design,
- 1553 protocol errors including I/O timeouts.

As described in the appendix 9 of the PS-ICD (AD03.3), 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.

18.2.3 Level 2

A **level 2** failure is related to an anomaly of one of the 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.

For each function, depending on the current System mode, observed performances are compared to non ambiguous thresholds and in case of failure a recovery strategy is engaged, possibly leading to the reconfiguration of the whole functional chain. 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.

18.2.4 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.

FDIR Level 3 corresponding errors will 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**.

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

18.2.5 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. Each level 4 failure shall be detected by dedicated independent system alarms and directly hardwired to the relevant reconfiguration module (ACC_RM or CDM_RM).

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

18.3 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 concept for both spacecraft.

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
	Thruster over activation or Thruster failure
	Fuel over consumption (Thruster over activation or Thruster failure)
Thermal monitoring and control function	Satellite over/under heating
Power supply function	Battery overcharge
	Bus undervoltage
	Power loss
Spacecraft monitoring and control function	Transmission with Earth loss

table 11 : system feared failures

From this list of system potential failures, 5 system alarms have been considered. Retained alarms are at a minimum (TBC):
- Loss of proper Sun Pointing **(SP)**
- Violation of Thruster On Time **(TOT)**
- Battery Depth of Discharge **(DOD)**
- Bus Under Voltage **(BUV)**
- Satellite Rate Anomaly **(RA)**.

SP, RA and TOT alarms are handled by the ACC_RM.

DOD and BUV alarms are handled by the CDM_RM.

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

When a level 4 alarm is activated on ACC, it shall be instantaneously taken into account and satellite shall directly go to survival mode 1.

When a level 4 alarm is activated on CDMU, it shall be instantaneously taken into account and satellite shall directly go to survival mode 2.

18.3.1 FDIR Modes

To fit the mission requirements, FDIR concept is organized around two main points:
- The failure classification, which has been exposed in the two previous sections
- The FDIR modes.

FDIR modes are associated to System modes and aims to support the mission observation. In fact this has been set up to define two reconfiguration strategies depending on the mission life phase.

FDIR strategy is 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 doing scientific observations and acquisitions
- autonomous fail safe (AFS), the rest of the time.

Each System mode is associated to one of these FDIR autonomy modes.

18.3.1.1 Autonomous Fail Safe (AFS)

Autonomous Fail Safe (AFS) mode is the first FDIR autonomy mode. It 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 sterategies.

In AFS mode, the flight program, uploaded during ground contact, is autonomously executed. On alarm occurrence, the spacecraft safety is given more importance than to the mission continuation : the related failure is not isolated nor recovered by low level FDIR processes, and the spacecraft safety is eventually based on level 4 recovery.

18.3.1.2 Autonomous Fail Operational (AFO)

Autonomous Fail Operational (AFO) mode is the second autonomy mode and it 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.

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

18.3.1.3 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).

For each satellite mode, the corresponding FDIR modes shall be as described in the table hereafter.

Satellite Modes		Sub-mode	AFS	AFO	N/A
Launch Mode	LM				x
Housekeeping Modes	HK1		x		
	HK2	V	x		
		NV	x		
Survival Modes	SM1				x
	SM2				x
Science Mode - Autonomy	AUT			x	
Science Mode - Telecom	TC			x	

table 12 : Relation between satellite et FDIR modes

For launch mode and both survival modes (i.e. SM1 and SM2), FDIR modes concept is not applicable.

Indeed, for part of the launch mode, Herschel/Planck spacecraft are still inside the launcher. Then it has to be impossible to switch System mode into one of both survival modes.

Similarly the Survival Modes, are not directly concerned by FDIR modes. As explained earlier in the chapter, FDIR modes correspond to a reconfiguration strategy. One of the several actions included in a reconfiguration sequence could lead (after failure detection and Identification) to a switch into survival mode which is the ultimate status.

18.4 General FDIR Implementation

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.

Symetrically, the FDIR function is divided into CDMS FDIR part and ACMS FDIR part, with simple interfaces between them. **Each** FDIR subset (i.e. CDMS FDIR and ACMS FDIR) comprises, for hardware monitoring:

- 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, respectively the CDM_SGM for the CDMS safeguard memory, and the ACC_SGM for the ACMS safeguard memory.

Each hardware reconfiguration module (i.e. ACC_RM and CDM_RM) is independently powered from the rest of the computer (respectively the rest of the ACC and the rest of the CDMU). The context of the satellite is periodically saved in the suitable non-volatile safeguard memory (i.e. ACC_SGM or CDM_SGM depending on the considered set of equipment units). Suitable toggling mechanism protects the critical data (the context) stored in SGM from being corrupted in case of OBSW failure :

The context is saved every T seconds. The SGM is split into two areas A and B; when the context is written in A every 2T, B is write protected and when the context is written in B every $2T+1$, A is write protected. In that way an OBSW failure cannot corrupt both areas, and the valid context to restart from is always, at a given time, the write protected one.

Basically, the CDM_SGM and ACC_SGM memorize all the system and units configuration necessary to ensure autonomous failure recovery, and to save the failure context for later analysis (eg. attitude data). Note that the design of CDMU is such that the Central time reference, distributed to all intelligent users keeps running in case of computer reconfiguration.

The CDMS S/W and the ACC S/W detect low level alarms (i.e. Levels 1 and 2 alarms), while the CDM_RM and the ACC_RM detect high level alarms in input and order any reconfiguration by means CPDU telecommand packets issueing High Priority Commands called HPC_CDM when originated from the CDM_RM, and HPC_ACC when generated from the ACC_RM.

CDMS FDIR and ACMS FDIR communicate via either S/W messages (e.g. events TM packets, TC accepatance report packets) for low level alarms, and H/W signals for high level/system alarms. An important feature is that any failure detection isolation and recovery procedure can be individually enabled or disabled by ground commands.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, CDMS – ACMS communication is not available.

It shall be noticed that ACMS and CDMS are considered as unavailable only in case of levels 3 and level 4 failures (see before). Analysis and recommandations partly driving the present implementation are detailed in RD03.20.

ACMS unavailability

The ACC_RM reports a status signal to the CDMS, via a reliable status link called AIR, to inform of its unavailability. For failure tolerance reason the status link is hardware and independent from the communication link.

CDMS unavailability

During the CDMS unavailability, Herschel and Planck spacecraft have to be maintained in a safe mode, command/control function and Mission Timeline service being temporarily unavailable. The spacecraft shall be put in a safe attitude by the ACMS.

The CDMU_RM sends a status signal to the ACMS, via reliable links. 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 or Bus undervoltage), to request ACMS to reach a status and put the spacecraft in an attitude, safe w.r.t. power generation ; in Sun Pointing 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 in order to be able to download data at a high rate and allow a fast failure analysis and recovery by the ground when in visibility.

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) is transmitted periodically from the ACC to the CDMU.

The basic mechanism is such that if the CDMU doesn't receive the information expected from the ACC Remote Terminal through the nominal bus, the CDMU switches over to the redundant bus. 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 is triggered to initiate a reconfiguration of the ACC remote terminal.
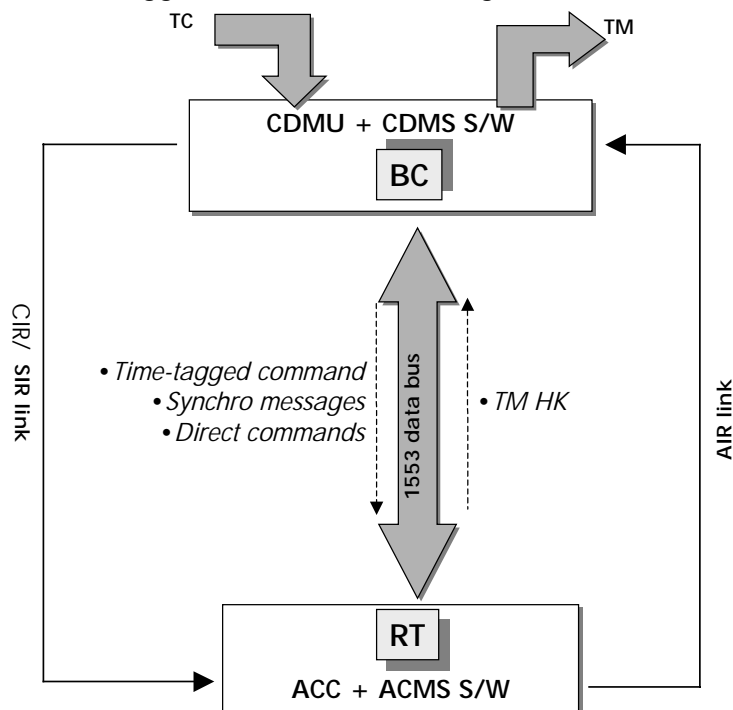

Figure 10 : CDMS/ACMS COMMUNICATION

18.5 FDIR Strategy

The FDIR strategy is defined for both spacecraft : each phase, from an autonomy and FDIR point of view is declared as autonomous fail safe or autonomous fail operational. For each system mode, depending on the operational life phase, the top level requirements (AFO, AFS) are refined at lower levels.

The proposed principles and protocol for the system level FDIR implementation, i.e. the synchronization of the two FDIR subsets, are based on some general rules detailed hereafter.

18.5.1 Platform

The hierarchical failure detection identification and recovery architecture 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 failure processing essentially depends on the current System mode, and the reconfiguration actions, in AFO mainly, is graduated with regards to failure severity. As already explained, each computing subsystem, CDMS and ACMS, applies a similar strategy to recover from a single failure:
- 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.

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

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

18.5.1.1 MTL Management associated to FDIR actions

As expressed is §6.5.1, 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 as mentionned in §6.5.4.1, one of the drivers of the FDIR strategy is, as far as possible, to help to pursue this plan.

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 6.5.4-3); these reconfigurations may interfere with the MTL execution, and the present section addresses the way the interfaces between the MTL and the failure cases are managed such that the MTL can be continued. This issue is detailed in a dedicated Technical Note RD03.20.

Failure at CDMS level

As long as the CDMU processor modules 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.

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

1- the reconfiguration is due to a CDMU level 3 failure

As it has been presented before, the first occurrence is labeled level 3a. In this case, the baseline is to restart the MTL only for the telecommands addressed to the CDMS and to the units directly managed by the CDMS (PCDU, TTC, ...). All the subschedules "belonging" to the instruments are disabled, and the ACMS configuration is described in section 6.5.4.3 "CDMS unavailability" : a Safe, Earth pointed, attitude is adopted.

The second occurrence is labeled level 3b. In that case, the baseline for a level 3b is to not restart the MTL : 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

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 <u>not baselined</u>.

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

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.

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. Note that this is definitely not considered as a critical issue, just a mission degradation:
  - It may happen only in case of specific maneuver / 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 immediately execute the received command (because 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 Science 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.

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 be ignored.

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.

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 be re enabled only if:
- the instrument has notified its return to a nominal operating mode
- **and** the running subschedule belonging to the failed instrument is completed.

After an instrument failure is recovered, its activity is resumed at the next subschedule.

18.5.1.2 Failure recovery strategy

The following tables illustrate the <u>CDMS failure</u> recovery strategy. 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	• Stop boost (if applicable) • 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	• Stop boost (if applicable) • Switch over to the redundant bus coupler or direct

			or 4 are triggered	interface using SGM configuration • Resume operations

table 13 : Level 1 failure recovery strategy

FAILURE LEVEL		DETECTION PROCEDURE	FAILURE RECOVERY	
			AFS Mode	AFO Mode
2	Main function failure	OBSW performance check	• Detect failure only. Isolation and recovery will be performed if levels 3 or 4 are triggered	• Stop boost (if applicable) • Save failure context • Identify the failed unit by a consistency cross check or possibly switch over to the redundant functional chain • Resume operations

table 14 : Level 2 failure recovery strategy

FAILURE LEVEL		DETECTION PROCEDURE	FAILURE RECOVERY	
			AFS Mode	AFO Mode
3a	CDMU or ACC internal failure – first occurrence	Nominal processor module HW alarm or SW watch dog	• Stop boost (if applicable) • In case of CDMU internal alarm: Send a CIR signal to the ACMS, to ask for an Earth pointed attitude • Save failure context • Reset the nominal processor module. • Load SGM context • Wait for Ground TC to re-engage MTL service	• Stop boost (if applicable) • In case of CDMU internal alarm: Send a CIR signal to the ACMS, to ask for an Earth pointed attitude to be adopted • Save failure context • Reset the nominal processor module. • Load SGM context • Disable all instruments sub-schedules • Autonomously re-engage the MTL service for the CDMS controlled units

3b	CDMU or ACC internal failure – second occurrence	Nominal processor module HW alarm or SW watch dog	• Stop boost (if applicable) • In case of CDMU internal alarm: Send a CIR signal to the ACMS, to ask for a Sun pointed attitude to be adopted • Save failure context • Switch over to the redundant processor module from SGM • Load SGM context Wait for Ground TC to re-engage MTL service

table 15 : Level 3 failure recovery strategy

FAILURE LEVEL		DETECTION PROCEDURE	FAILURE RECOVERY
4	Global satellite malfunction	System Alarm	• Stop boost (if applicable) • Disconnect non essential loads • Suspend MTL service • In case of CDMU internal alarm: Send a SIR signal to the ACMS, to trigger a sun pointing mode • Save failure context • Switch over to the redundant processor module from PROM • Switch to satellite survival mode : SM2 • wait for ground TC to re-engage MTL service

table 16 : Level 4 failure recovery strategy

18.5.2 Instrument strategy

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. The failures requesting the intervention of the spacecraft and the associated reconfiguration procedures are defined by the instruments.
    *   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).

Operational concept

REFERENCE :	H-P-1-ASPI-TD-0263
DATE :	15/06/02
ISSUE :	01/00 **Page :** 74/77

- an instrument anomaly detected by or reported to the CDMS implies, as detailed in previous chapters, that the running subschedule belonging to the failed instrument is temporarily disabled.

19. SECURITY CONCEPTS (CL#30)

For TM and TC there is no other protection than the ones required by the TM / TC standard. There is no encrypted authentication of telecommand. (refer to chapter 4.2.1 for TM / TC characteristics)

Some critical telecommand will need to be armed first on ground before sending (SCOS-2000 facility).

Some critical telecommand will need to be loaded on-board first then a second telecommand shall be send to trigger them.

Different users roles and right access are are defined at SCOS-2000 levels and at system data base level.

In order to avoid some errors for repetitive operations several possibilities are offered :
- Implementation of sequences (SCOS-2000 facility), this is a ground facility,
- Implementation of on-board software functions which can be activated via a dedicated PSICD service, this is an on-board facility,
- Implementation of OBCP which can be activated via a dedicated PSICD service, this is both an on-board (because execution takes place on-board) and a ground (because ground generates the OBCPB as it generates procedures) facility.

In order to manage the commonality between Herschel and Planck, as far as possible telemetry, telecommand, procedures, OBCB, functions, displays, … will have common identifiers. The drawback of this implementation is that an operator can send to the wrong spacecraft the command he wants to execute. This drawback is minimized by the fact there is one MOC dedicated per spacecraft.

20. TESTS AND VALIDATIONS

The different elements of the system to be tested are :
* The Spacecraft,
* The ground station,
* The MOC (including system database and nominal and contingency procedures),
* and the ground instrument equipment.

and their interfaces.

For test purposes, the spacecraft validation is shared in :
* Function tests,
* TM / TC interfaces tests.

For test purposes, the MOC validation is shared in :
* Function tests,
* TM / TC interfaces tests.

Function tests

The spacecraft functions are tested during AIT activities using EGSE to simulate environment (AOCS, power, …) , to control the spacecraft (TC) and to monitor it (TM). Those tests will be run in different environments representative of the mission and associated spacecraft configuration (thermal vacuum tests, vibration tests, acoustic tests, …). In parallel the MOC functions are validated using a spacecraft simulator. In order to improve the MOC function validations, the spacecraft simulator is able to issue TM which has been recorded during AIT activities.

test of interface : Spacecraft / ground station

The test of the ground station and its interface with the spacecraft is done using the RF suitcase. The RF suitcase is fully representative of spacecraft for RF subsystem (EQM model) and partially representative of CDMS subsystem (as a minimum TM and TC interface contents is representative). The RF suitcase will be first configured as Planck, as soon as the RF representative equipment (EM) used to build the RF suitcase are taken from the AVM, then it will be refurbished to be configured as Herschel. As far as the RF suitcase is representative of spacecraft up to TM/TC interfaces, this test allows to validate not only the ground station, but also the TM / TC interface.

Test of interface : Spacecraft / MOC (without ground station in the loop)

The SVT (System Verification Tests) are aimed to validated the interface between the spacecraft and the MOC. During SVT tests, the telemetry is permanently received in parallel by the MOC and the CCS, AIT is in charge to switch On the spacecraft and put it in an agreed configuration, then the control of the spacecraft (TC) is transferred to the MOC from which are run the SVT tests, in parallel the EGSE insure the spacecraft "baby setting" and the needed stimulation (Solar array simulation, AOCMS environment simulation, ground station simulation by RF SCOE, …), at the end of one SVT test the control of spacecraft (TC) is recovered by EGSE which will then switch off the spacecraft. 3 SVT are foreseen. SVT-0 will take place at L-18 months for a duration of 5 days per spacecraft. SVT-1 will take place at L-9 months for a

duration of 15 working days per spacecraft. SVT-2 will take place during launch campaign at L-4 months for a duration of maximum 10 days per spacecraft. SVT-0 is a pre-run of SVT-1. SVT-1 is aimed to validate all telemetry, all telecommands, the ground processing of telemetry, the ground processing of telecommands, the database, the behavior of the spacecraft and the operational procedures. SVT-2 is aimed to validate the full integrated ground segment (including instrument) against the flight spacecraft and to validate the functional performances before launch. In addition to those SVT tests, Listen-in tests will be performed mainly during important AIT tests (thermal vacuum, …). During Listen-in tests the MOC will received the telemetry, as during SVT tests but will not send telecommand.

Hereafter a schema showing the different validation stages (note : the AIT validation stages : spacecraft environment and spacecraft function are not shown). The SVT tests and the ground station tests are complementary to validate the full chain TM/TC from spacecraft up to MOC via ground station. The SVT tests and the simulation tests are complementary to validate all the spacecraft and ground functions.
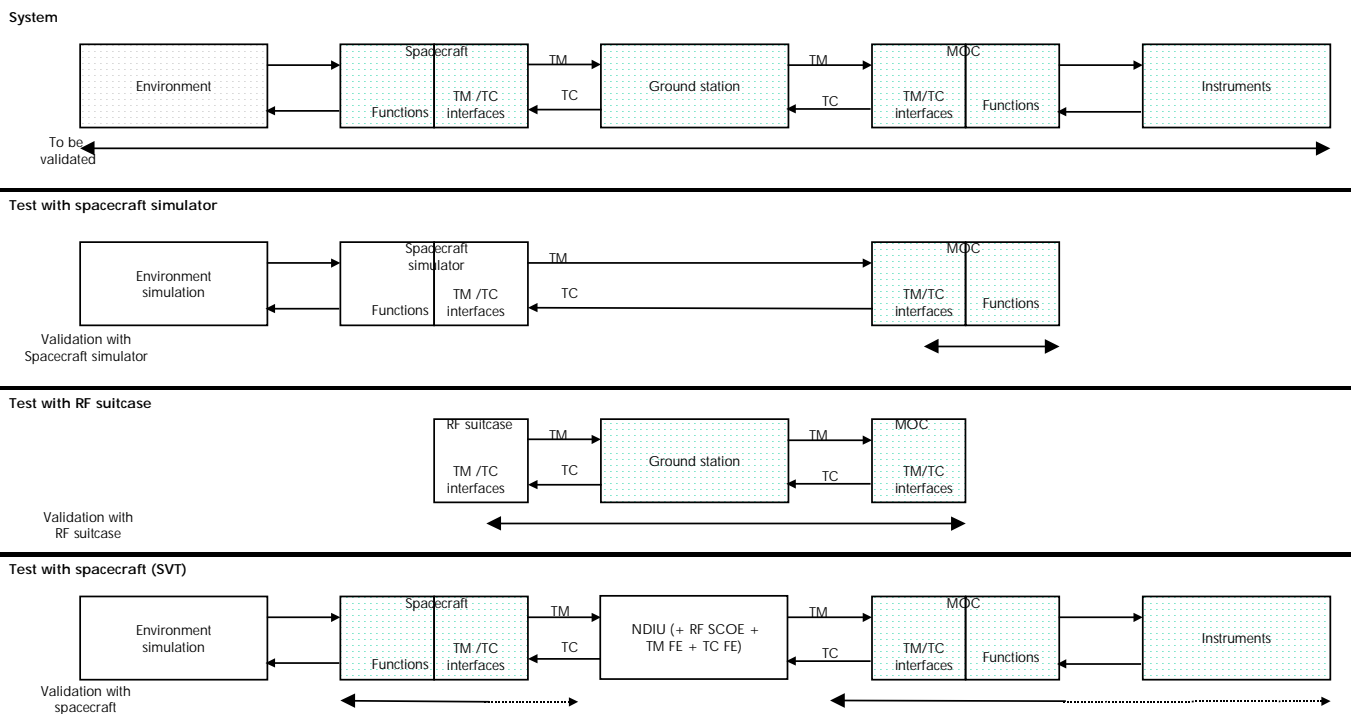

Figure 11 : system validation

Note :

The database is common with AIT and an automatic tool is proposed to trace which TM parameters and telecommands have been or not validated during AIT activities.

The normal and contengency procedures will be tested as far as possible during AIT activities, but due to configuration limitations or too complex simulations some procedures will not be tested in AIT (can be on ESOC simulator).