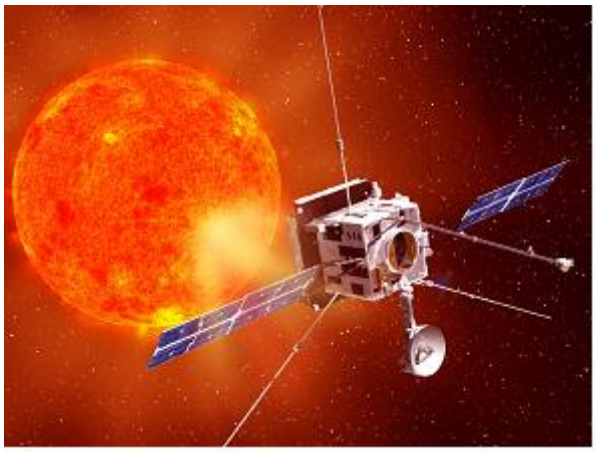

SOLAR ORBITER ENERGETIC PARTICLE DETECTOR

EPD Failure, Detection, Identification and Recovery

Document ID:	SO-EPD-PO-RP-0011
Issue:	2
Revision:	3
Date:	2016-05-04

Written	Checked	Approved Configuration Control	Approved QA	Approved Experiment Manager	Approved Principal Investigator
2016.05.04 12:58:21 +02'00'	NOMBRE CARRASCO GALLARDO ALBERTO - NIF 76255586Y 2016.05.04 13:09:29 +02'00'	2016.05.04 15:43:00 +02'00'	Angel Martinez 2016.05.07 10:32:43 +02'00'	Manuel Prieto Mateo 2016.05.11 09:47:54 +02'00'	Javier Rodríguez-Pacheco 2016.05.11 09:48:14 +02'00'
Héctor García Date and Signature	**Alberto Carrasco Date and Signature**	**Cecilia Gordillo Date and Signature**	**Ángel Martínez Date and Signature**	**MANUEL PRIETO Date and Signature**	**JAVIER R.-PACHECO Date and Signature**

DISTRIBUTION LIST

The following lists indicate the individuals and agencies in receipt of review copies of the present document:

Agency / Organization	Name & Title	Contact information
ESA	Filippo Marliani, Payload System Manager, Payload System Manager	Filippo.Marliani@esa.int
ESA	Kristin Wirth, Instrument System Engineer	Kristin.Wirth@esa.int
ESA	Salma Fahmy, Instrument System Engineer	Salma.Fahmy@esa.int
ESA	Daniel Mueller, Project Scientist	Daniel.Mueller@esa.int
ESA	Philippe Kletzkine, Project Manager	Philippe.Kletzkine@esa.int
ESA	Pierre Olivier, Product Assurance Manager	Pierre.Olivier@esa.int
SRG-UAH	Javier Rodríguez-Pacheco, EPD - Principal Investigator	javier.pacheco@uah.es
SRG-UAH	Manuel Prieto, EPD Project Manager	manuel.prieto@uah.es
SENER	Angel Martínez, EPD Product Assurance Manager	angel.martínez@sener.es
SRG-UAH	Cecilia Gordillo, EPD Configuration Control Manager	cecilia.gordillo@uah.es
SRG-UAH	Andrés Russu, EPD AIVT Manager	andres.russu@edu.uah.es
CAU	EPD-Solar Orbiter Kiel Team	solo_kiel@physik.uni-kiel.de
APL/JHU	Glenn Mason, EPD-SIS Lead Co-I	glenn.mason@jhuapl.edu
APL/JHU	Helmut Seifert, EPD-SIS Project Manager	Helmut.Seifert@jhuapl.edu
APL/JHU	Kush Tyagi, EPD-SIS System Engineer	Kush.Tyagi@jhuapl.edu
SRG-UAH	Sebastián Sánchez, EPD-ICU Lead Co-I	sebastian.sanchez@uah.es
SRG-UAH	Óscar Gutiérrez. ICU Project Manager	o.gutierrez@uah.es
CRISA	Tirso Velasco. ICU PO	Tirso.Velasco@astrium.eads.net
CRISA	Antonio Peña. ICU System Engineer	antonio.pena@astrium.eads.net

CHANGES RECORD

Issue	Revision	Date	Modified by	Section / Paragraph modified	Change implemented
1	0	2012-02-01		All	First issue
2	0	2012-06-27	J. Duatis	6.1, 6.2, 6.3, 6.4, 6.5	PDR-RID-15: Added ICU and sensor over temperature FDIR requirement.
				6.1	PDR-RID-17: Added FDIR-ICU-170.
				6.1, 6.2, 6.3, 6.4, 6.5	PDR-RID-79, PDR-RID-80, PDR-RID-84: Recovery level defined for each FDIR action.
				5.1.3.3	PDR-RID-81: Deactivation of recovery actions is implemented by service 19 in EPD.
				5.1.1 & 5.1.3	PDR-RID-82 & PDR-RID-83: Time reaction and FDIR implementation level redefined.
				6.1	PDR-RID-85: Failures to be handled by the OBC are indicated in section 6.1 with Recovery Level: 2.
				5	PDR-RID-216: Section 5 rewritten.
2	1	2013-07-04	J. Duatis	All	Removed LET
				All	STEIN changed to STEP
				5	Updated section 5 as per RID-PDR-82
				2	Updated applicable and referenced documents tables.
				6.1	Updated according to CDR FMEA update.
2	2	2014-05-06	J. Duatis	6.1	FDIR-ICU-160 and FDIR-ICU-170 modified as per CDR-48
				6.1	Recovery level 2=OBC removed. No OBC reaction expected for any event as per RID-141. Only FDIR-ICU-170 loss of S20 remains.
				2.1, 2.3	Updated AD and RD document versions as per CDR-171
				6,1	Packet retransmission in case of SpW link error removed as per CDR-58
				5.1.3.2	Updated as per CDR-57, No OBCPs required.
2	3	2016-05-02	H. García	5	Updated recovery actions
				5.1.3.3	Added sensor disable parameters
				5.1.3.5	Added autonomous actions for EPD Sensors.
				6.1	FDIR-ICU-090 no event is generated

Issue	Revision	Date	Modified by	Section / Paragraph modified	Change implemented
					FDIR-ICU-100 this anomaly forces an ICU reset
					FDIR-ICU-200 updated RID number.
					FDIR-ICU-220 no event TLM generated.
					FDIR-ICU-250 added SW Trap anomaly
				6.2	FDIR-HE-020, FDIR-HE-030, FDIR-HE-040 added event generation as a result of the onboard monitoring procedure
					FDIR-HE-060 recovery action included
					FDIR-HE-080 added EEPROM read-out error
				6.3	FDIR-STEP-020, FDIR-STEP-030, FDIR-STEP-040 added event generation as a result of the onboard monitoring procedure. Recovering action are sensor power off
					FDIR-STEP-080 added EEPROM read-out error
				6.4	FDIR-SIS-020, FDIR-SIS-030 removed in behalf of the autonomous actions as described in 5.1.3.5
					FDIR-SIS-050 recovering level updated
					FDIR-SIS-070 monitoring condition defined
					FDIR-SIS-080, FDIR-SIS-090 recovery actions updated

TABLE OF CONTENTS

LIST OF TABLES

1 SCOPE OF THE DOCUMENT

This document contains the Fault Detection, Isolation and Recovery (FDIR) Implementation Report of the Energetic Particle Detector (EPD). It provides the design approach of the FDIR strategy to be implemented through all instrument subsystems, according to the EID-A requirements. Specifications defined affecting the EPD subsystems (ICU and EPD sensors) implementation become EPD requirements at system level at all effects.

2 APPLICABLE AND REFERENCE DOCUMENTS

2.1 Applicable Documents (ADs)

The following documents, listed in order of precedence, contain requirements applicable to the activity:

ID	Code	Title	Issue	Revision
[AD 01]	SOL-EST-RCD-0050	EID-A. Solar Orbiter Experiment Interface Document – Part A	4	0
[AD 02]	SO-EPD-PO-IF-0001	EID-B. Solar Orbiter Energetic Particle Detector EPD	3	3
[AD 03]	SO-ESC-RS-05001	Solar Orbiter Operations Requirements Document	1	8

Table 2-1. Applicable documents list

2.2 Applicable Standards and Regulations (SDs)

ID	Code	Title	Issue	Revision
[SD 01]	ECSS-Q-ST-60C	Space Product Assurance: EEE	C	1

Table 2-2. Applicable standards and regulations list

2.3 Reference Documents (RDs)

The following documents can be consulted:

ID	Code	Title	Issue	Revision
[RD 01]	SO-EPD-EP-00001	Engineering Plan – Solar Orbiter EPD (Energetic Particle Detector)	2	0
[RD 02]	SO-EPD-PA-00001	Product Assurance Plan – Solar Orbiter EPD (Energetic Particle Detector)	2	0
[RD 03]	SO-EPD-PO-RP-0008	EPD FMEA	2	1
[RD 04]	SOL.S.ASTR.TN.00088	Instrument Data Management Overview for PIs	4	0
[RD 05]	SO-EPD-PO-IF-0003	EPD TM/TC Interface Control Document (ICD)	2	9
[RD 06]	SO-EPD-ICU-AN-0004	SO EPD ICU FMEA	4	0
[RD 07]	SO-EPD-KIE-AN-0040	SO EPD FMEA for EPT-HET	2	0
[RD 08]	SO-EPD-KIE-AN-0041	SO EPD FMEA for STEP	2	1
[RD 09]	SO-EPD-SIS-RP-0010	SIS Preliminary FMEA	1	2

Table 2-3. Reference Documents list

3 ACRONYMS AND ABBREVIATED TERMS

Acronym	Description
AD	Applicable Document
AIV	Assembly, Integration and Validation
AU	Astronomical Unit
CDPU	Common Data Processing Unit
Co-I	Co-Investigator
DC	Direct Current
EGSE	Electrical Ground Support Equipment
EID	Experiment Interface Document
EM	Engineering Model
EMC	ElectroMagnetic Compatibility
EPD	Energetic Particle Detector
EPT	Electron Proton Telescope
EQM	Engineering Qualification Model
ESA	European Space Agency
FM	Flight Model
FS	Flight Spare
HET	High Energy Telescope
HW	Hardware
ICU	Interface Control Unit
LCL	Latching Current Limiter
LET	Low Energy Telescope
LVPS	Low Voltage Power Supply
MAG	Magnetometer
MGSE	Mechanical Ground Support Equipment
MLI	Multi-Layered Insulator
PI	Principal Investigator
RD	Reference Document
S/C	Spacecraft
SEL	Single Event Latchup
SEU	Single Event Upset
SIS	Suprathermal Ion Spectrograph
STEP	SupraThermal Electrons & Protons
STM	Structural and Thermal Model
SW	Software
TBC	To Be Confirmed
TBD	To Be Defined
TBW	To Be Written
TC	Telecommand
TCP/IP	Transmission Control Protocol/Internet Protocol
TM	Telemetry
URP	Unit Reference Point

Table 3-1. Acronyms and abbreviated terms list

4 INTRODUCTION

The Energetic Particle Detector (EPD) suite consists of four sensors measuring electrons, protons, and ions from helium to iron, and operating at partly overlapping energy ranges from 2 keV up to 200 MeV/n. The EPD sensors are:

- SupraThermal Electrons & Protons (STEP)
- Suprathermal Ion Spectrograph (SIS)
- Electron Proton Telescope (EPT)
- High Energy Telescope (HET)

The EPD sensors share the Instrument Control Unit (ICU) that is composed by the Common Data Processing Unit and the Low Voltage Power Supply (CDPU/LVPS), which is the sole power and data interface of EPD to the spacecraft.

STEP consists of a single unit having two view cones in opposite directions. SIS consists of two sensor heads with roughly opposite (160°) view directions sharing a common electronics box. EPT-HET has multiple view cones sharing a common electronics box. There are two identical EPT-HET units.

The overall energy coverage achieved with the EPD sensors is 0.002 MeV to 20 MeV for electrons, 0.003 MeV to 100 MeV for protons, 0.008 MeV/n to 200 MeV/n for heavy ions (species-dependent). This energy and species coverage well satisfies and for a large part exceeds the requirements defined for EPD in the Solar Orbiter Payload Definition Document and in the report of the Joint Science and Technology Definition Team (JSTDT) for the Solar Orbiter/Sentinels mission.

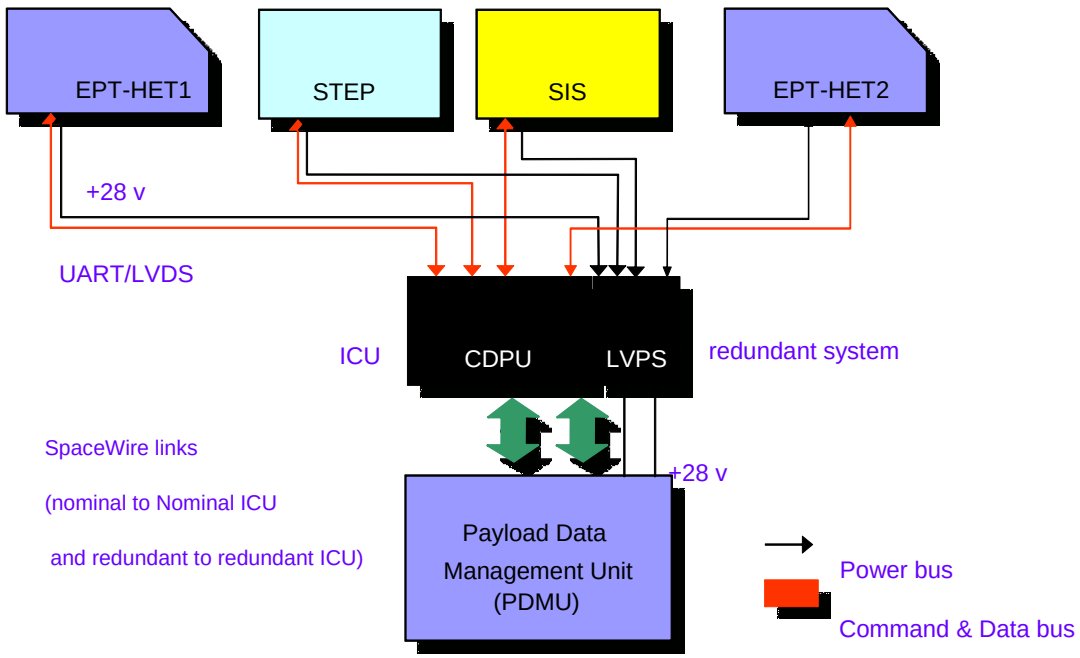

Figure 1. EPD Block Diagram

5 APPROACH AND GENERAL FDIR CONCEPT

The EPD implements a classical FDIR concept, with 5 **Recovery Levels** for failure detection and recovery action implementation:

Recovery Level	Description
Level 1. Ground	Ground processing of telemetry and sending of telecommand. Max reaction time 24 hours in all mission phases (as per CTRL-1 on [AD03]).
Level 2. OBC	On-board Monitoring Process by the On-board Computer, monitoring parameters of its Central Data Pool (provided by EPD by Housekeeping telemetry) or reacting to an EPD event (Service 5). On out-of-margins detection or on event reception, OBC implements a recovery action with a maximum reaction time 10 seconds. This level is limited by the amount of parameters that can be monitored at OBC level and the number of recovery actions that can be programmed in the OBC.
Level 3. ICU	On-board monitoring process of ICU monitoring parameters of its own Data Pool, including sensor units housekeeping data. On out-of-margins detection, ICU implements a recovery action with a maximum reaction time of 2 seconds (1 second for sensor telemetry + 1 second for On board monitoring function). The number of parameters to be monitored by the ICU will be also limited.
Level 4. ICU Errors	Errors requiring an immediate ICU reaction (reboot, EDAC, hardware reaction) which are detected at ICU level. These errors will be handled internally by the ICU and the recovery action will be implemented immediately on detection.
Level 5. Sensors	Errors which can be detected at sensor level and can be also mitigated at sensor level.

Table 5-1. Recovery Levels

This FDIR has indeed three stages: the Detection, the Isolation, and the Recovery.

Detection

The Detection feature is meant to monitor the variables which are considered important and which can uncover malfunctions or risks to EPD. It basically implements some kind of check in the variable, which will tell if it reads as expected or something is going wrong. The Detection will conclude that everything is OK or that something is not behaving properly.

Isolation

If the Detection triggers some error, the Isolation comes into play. Broadly speaking, the Isolation is meant to identify and remove the failing signal from the control chain avoiding cascade error handling, and to either stop operations or to provide an alternative which allows resuming them autonomously and safely in the short term.

In the case of autonomous isolation by EPD, the instrument shall indicate in a TM the error identification (event or HK value).

Recovery

Finally, the last stage is implemented by the Recovery process. It deals with the analysis of the failure at and the implementation of the recovery action. The list of ICU autonomous recovery actions is the following;

- Recovery Action 1: Send an indexed sequence of messages to a sensor
- Recovery Action 2: Sensor power-off/power-on sequence
- Recovery Action 3: Sensor disable and power-off
- Recovery Action 4: ICU Reset
- Recovery Action 5: Sensor power-off/power on and send an indexed sequence of messages to the sensor (combination of action1 and 2),

Each action has a specific code indicating the target sensor, and in the case of sending a message block, the corresponding table and index to that table.

Note that upon Recovery Action 3 the affected sensor will not be powered-on again until a ground action is implemented to re-enable the sensor.

5.1 FDIR procedures approach

As defined in [AD 01], FDIR procedures initiated by onboard automatisms or by ground (automatism or manual procedures) shall be compatible with the maximum allowed reaction time. Indeed, the most critical failures in terms of time reaction are implemented by hardware in the EPD.

5.1.1 FDIR time reaction

After identification of the failure, the maximum reaction time before permanent damage has to be determined. Once the reaction time is defined, the level in which has to be implemented can be selected according to the following table and taking into account that the failure has to be handled at the lowest possible level.

Time reaction	FDIR implementation	Recovery Level				
		1	2	3	4	5
< 2 seconds	FDIR function shall be implemented at Instrument Subsystem level.				X	X
< 10 seconds	FDIR function shall be implemented at Instrument level.			X	X	X
10 seconds < time reaction < 24 hours	FDIR function shall be implemented at System (OBC) level or higher.		X	X	X	X
> 24 hours	The FDIR function can be implemented by ground processing at GSOC.	X	X	X	X	X

Table 5-2. Recovery level vs. time reaction

5.1.2 Failure criticality

Each FDIR procedure has been categorized according to the failure criticality:

Severity Level	Description
1	Failure Propagation to S/C.
2	Loss of EPD mission.
3	Major EPD mission degradation.
4	Minor EPD mission degradation or any other effect.

Table 5-3. Severity Levels

5.1.3 FDIR implementation

5.1.3.1 Level 1. Ground

FDIR on ground will be implemented through the monitoring capabilities at the GSOC. Data will be analyzed from telemetry. Nominal values will be defined and checked against received telemetry. In case that an anomaly is detected, procedures will be defined to react.

Actions to be implemented at Ground level are indicated in section 6 where the Recovery level is indicated as **1**.

5.1.3.2 Level 2. On-board computer

FDIR on the on-board computer will be based on the capabilities of the OBC to monitor EPD housekeeping parameters and the definition of monitoring configurations through service 12.

As defined in [RD 04], the OBC will be able to detect that a parameter goes out of the nominal value and trigger an event which activates an on-board procedure. Through these procedures it will be possible to implement recovery actions.

All autonomous actions at OBC level can be deactivated by deactivating the associated monitoring function through OBC Service 12.

Following parameters will be transmitted to the OBC to be stored in the Central Data Pool:

– EPD Status Word

– Unit Temperature (EPT-HET-1, EPT-HET-2, STEP, SIS)

– Unit Voltage (EPT-HET-1, EPT-HET-2, STEP, SIS)

– Unit Last event (ICU, EPT-HET-1, EPT-HET-2, STEP, SIS)

See [RD 05] for housekeeping structure definition details.

Actions to be implemented at OBC level are indicated in section 6 where the Recovery level is indicated as **2**.

Currently there is not a need for OBCP in the OBC as the only action traced in section 6 is regarding stop sending Service 20 TC packet due to S/C is moving to Safe mode.

5.1.3.3 Level 3. EPD – ICU

The ICU SW shall implement the following services for FDIR management:

On Board Monitoring Service: On-board monitoring is a task in the ICU Software that performs a periodic checking of a set of ICU Data Pool parameters against configured conditions. These checks can be enabled/disabled and configured by telecommand. Checks can be configured a value checking or out of limits (for details see the services definition in [RD 05]). Data Pool parameters can be internal ICU parameters or parameters acquired from the EPD sensor units through housekeeping.

Even Action Service: Even-action service allows the association of an event with an autonomous recovery action triggered by a TC. Actions will be pre-programmed in the ICU in advance. Actions include:

- ICU warm reset (ICU action).
- ICU cold reset (through event to S/C).
- Switch ICU to redundant (through event to Ground).
- Sensor warm reset (if available).
- Sensor cold reset (through LCL).
- Send a TC to a sensor.

It shall be able to deactivate all autonomous actions at ICU level by deactivating the associated monitoring function through ICU Service 12.

Event Service: The ICU Software shall generate an event telemetry TM(5,x) on failure detection according to the failure severity as per the table below.

Failure Severity	Severity Description	Event	Event Description
1	Severity Level 1. Failure Propagation to SC.	5,4	Error/Anomaly Report -- High Severity
2	Severity Level 2. Loss of EPD mission.	5,4	Error/Anomaly Report -- High Severity
3	Severity Level 3. Major EPD mission degradation.	5,3 or 5,4	Error/Anomaly Report -- Medium Severity
4	Severity Level 4. Minor EPD mission degradation or any other effect.	5,2	Error/Anomaly Report -- Low Severity

Table 5-4. Service 5 Event Telemetries

Actions to be implemented at ICU On-board monitoring level are indicated in section 6 where the Recovery level is indicated as **3**.

Sensor Disable Service: The ICU implements the Data pool parameter for each sensor which indicates if the sensor is enabled (powered-on when in Configuration and Operational modes) or disabled (remains powered-off). The parameters are the following (see the user manual for more information):

STEP_INIT_CONFIGURATION_STRUCT
SIS_INIT_CONFIGURATION_STRUCT
EPT_HET_1_INIT_CONFIGURATION_STRUCT
EPT_HET_2_INIT_CONFIGURATION_STRUCT

5.1.3.4 Level 4. EPD – ICU Errors

EPD ICU shall react autonomously to some errors which are detected and recovered from hardware. These errors include:

- 1-bit memory errors (EDAC correction)
- Processor trap (ICU reset).

Actions to be implemented at ICU hardware level are indicated in section 6 where the Recovery level is indicated as **4**.

5.1.3.5 Level 5. Sensors

Errors detected and corrected at STEP, HET-EPT1 and HET-EPT sensors level are those related to EDAC memories.

SIS take care autonomously of monitoring internal voltages and currents. In case of error implements an autonomous shutdown. Before executing the autonomous shutdown SIS will sent and event to OBC informing about the error.

For the rest of errors related to Sensors the EPC ICU implements monitoring on housekeeping and implement the required actions. Actions to be implemented at EPD Sensor level are indicated in section 6 where the Recovery level is indicated as **3**.

6 EPD FDIR PROCEDURES

Below table describes the columns of FDIR requirements listed in following sections:

Column Title	Description
FDIR Req.	Identifier of the FDIR requirement
FMEA Block or **Circuit/Index**	Identifier of the circuit or component in the FMEA analysis
Function	Function of the component
Failure Mode	Description of the failure
Consequence	Consequence of the failure
Sev.	Severity of the failure as described above
Detection	Symptoms caused by the failure
Remarks	Additional information about the failure
Rec. Level	Level in which the recovery action is implemented as described above
Recovery Action	Description of the recovery action

Table 6-1. FDIR table columns definition

6.1 ICU

ICU									
FDIR	**FMEA Block**	**Function**	**Failure Mode**	**Consequence**	**Sev**	**Detection**	**Remarks**	**Recovery level**	**Recovery action**
FDIR-ICU-010	01-01	Upstream LCL	Open circuit	ICU cannot be switched ON	3	No TLM received at OBC		1	Power cycle, if problem persists Switch ICU to redundant
FDIR-ICU-040	01-02	CPU	CPU not working	Loss of ICU	3	No TLM received at OBC		1	Power cycle, if problem persists Switch ICU to redundant
FDIR-ICU-050	01-02	PROM	PROM not working	ICU cannot boot.	3	No TLM received at OBC		1	Power cycle, if problem persists Switch ICU to redundant
FDIR-ICU-060	01-02	EEPROM	Single/Multiple bit failure	Wrong EEPROM data.	3	Event 0x4004	EEPROM checksum at page level / Contents may be upgraded	1	Patch of the ASW. If the problem persists, switch to redundant
FDIR-ICU-070	01-02	EEPROM	EEPROM not working	Unable to load baseline ASW data to RAM	3	Event 0x4004	EEPROM checksum at page level	1	Patch of the ASW. If the problem persists, switch to redundant
FDIR-ICU-080	01-02	EEPROM	EEPROM not working	Unable to load updatable ASW data to RAM	3	Event 0x4004	EEPROM checksum at page level	1	ICU try to load the Baseline ASW.
FDIR-ICU-090	01-02	RAM	Single bit failure	Wrong RAM data	4		ICU: During memory scrubbing, if a single bit error is detected, the error is corrected (EDAC is able to correct 1 error)	4	EDAC bit correction
FDIR-ICU-100	01-02	RAM	RAM multiple bit failure	Wrong RAM data. Temporary interruption of EPD operation	3	ICU reset and event report 0x4100	ICU: During memory scrubbing, if more than one error are detected, the ICU is reset.	4,1	ICU Reset If problem persists switch to redundant
FDIR-ICU-110	01-02	RAM	RAM not working	Unable to load baseline ASW to RAM.	3	Event 0x4003	ICU: During the boot process, RAM is tested (each bit is written and then read). If the available RAM after this test cannot allow the baseline ASW deployment, then this branch is non operative and the solution would be a switchover.	1	If problem persists switch to redundant

ICU									
FDIR	**FMEA Block**	**Function**	**Failure Mode**	**Consequence**	**Sev**	**Detection**	**Remarks**	**Recovery level**	**Recovery action**
FDIR-ICU-120	01-02	RAM	RAM not working	Unable to load updatable ASW to RAM.	3	Event 0x4003	ICU: During the boot process, RAM is tested (each bit is written and then read). If the available RAM after this test cannot allow the updatable ASW deployment, then this branch is non-operative and the solution would be load the baseline ASW.	4	Load de Baseline ASW
FDIR-ICU-130	01-02	Power lines	Shortcircuit	Loss of DPU	3	No TLM		1	Switch to redundant
FDIR-ICU-140	01-02	SpaceWire	Link error	Loss of TC packet	3	Event: Link error 0x4200	TC transmission of S/C interrupted	1	Event + Increment housekeeping counter. If problem persists switch to redundant.
FDIR-ICU-150	01-02	SpaceWire	Link error	Loss of TM packet	3	Event: Link error 0x4200	TLM transmission to S/C interrupted	1	Event + Increment housekeeping counter. If problem persists switch to redundant.
FDIR-ICU-160	01-02	SpaceWire	Link error not recovered	ICU unable to communicate with S/C	3	No TLM	Transmission interrupted	1	If problem persists switch to redundant.
FDIR-ICU-170	01-02	SpaceWire	Service 20 not received	Service 20 is used as Health & Status indicator.	3	No Service 20 TC	Interruption of service 20 indicates that OBC is not operative.	2	Prepare for EPD switch-off. S/C switches off EPD in 60 seconds.
FDIR-ICU-180	01-02	FPGA	FPGA not working	Loss of ICU	3	No TLM	Transmission interrupted	1	Switch to redundant
FDIR-ICU-190	01-02	Master clock generation (FPGA)	Open or short or not working	Loss of ICU	3	No TLM	Transmission interrupted	1	Switch to redundant
FDIR-ICU-200	01-01	LCL	Failure in sensor LCL activation or failure in feeding sensor	Loss of ICU/sensor	3	Housekeeping, Event 0x4300 Sensor under voltage	Sensor OFF	1	Switch to redundant
FDIR-ICU-210	01-01	LCL	Failure in LCL CMD monitor	Wrong HK value	4	Housekeeping	No consequences, TM from sensor is received	1	
FDIR-ICU-220	01-02	Sensor UART	Loss of UART, UART malfunction	No communication with sensor or comm errors	3	Housekeeping	Sensor not responding or receiving wrong data	1	Power cycle sensor. Change to redundant
FDIR-ICU-230	01-02	Watchdog	Permanent WD disabled	No reset on ICU	3	CDPU is not able to perform any transition involving a reset		1	Change to redundant

ICU									
FDIR	**FMEA Block**	**Function**	**Failure Mode**	**Consequence**	**Sev**	**Detection**	**Remarks**	**Recovery level**	**Recovery action**
FDIR-ICU-240	01-02	Watchdog	Unexpected WD activation	ICU reset	3	CDPU performs a reset without cause		4, 1	ICU Reset If problem persists change to redundant
FDIR-ICU-250	01-02	SW	Software error	ICU reset	3	Software error Trap	Event 0x4002 at boot	4	ICU Reset

Table 6-2. ICU FDIR procedures

6.2 HET-EPT

HET-EPT									
FDIR	**Circuit / Index**	**Function**	**Failure Mode**	**Consequence**	**Sev**	**Detection**	**Remarks**	**Recovery level**	**Recovery action**
FDIR-HE-010	04-0n	LCL	Open circuit	HET-EPT-n cannot be switched ON	3	No TLM received	Detected in housekeeping of HET-EPT on ground	1	Cold-reset. If problem persists Switch-off HET-EPT-n
FDIR-HE-020	04-0n	Power Input	Under voltage	HET-EPT-n will be switched off.	4	Check in HK the current voltage, compare against lower limit.	ICU sends event (0x4101)	3	Switch-off HET-EPT-n (Action 3)
FDIR-HE-030	04-0n	Power Input	Over voltage	HET-EPT-n will be switch off.	4	Check in HK the current voltage, compare against the upper limit.	ICU sends event	3	Switch-off HET-EPT-n (Action 3)
FDIR-HE-040	04-0n	Temperature	Over temperature	HET-EPT-n damage/ space craft damage	4	Check in HK the current temperature, compare against the upper limit.	ICU sends event	3	Switch-off (Action 3)
FDIR-HE-050	04-0n	FPGA	FPGA not working	Loss of HET-EPT -n	3	No TLM received	Detected in housekeeping of HET-EPT on ground	1	Cold-reset. If problem persists switch-off HET-EPT-n
FDIR-HE-060	04-0n	Serial link	Serial link error	Loss of communication	3	No TLM received		1	Cold-reset. If problem persists switch-off HET-EPT-n
FDIR-HE-070	04-0n	Serial link	Continuous CRC error	Loss of communication	3	Continuous CRC error in received TLM	ICU sends event if error > 30	1	Increment error counter. If problem persists ground switch-off HET-EPT-n
FDIR-HE-080	04-0n	EEPROM	EEPROM read-out error	HET-EPT cannot be configured	3	No read-out TLM or continuous TLM CRC error	ICU sends event (0x4160)	1	Cold-reset. If problem persists Switch-off HET-EPT-n

Table 6-3. HET-EPT FDIR procedures

6.3 STEP

STEP									
FDIR	**Circuit / Index**	**Function**	**Failure Mode**	**Consequence**	**Sev**	**Detection**	**Remarks**	**Recovery level**	**Recovery action**
FDIR-STE-010	02-01	LCL	Open circuit	STEP cannot be switched ON	3	No TLM received	Detected in housekeeping of STEP on ground	1	Cold reset. If problem persists switch-off.
FDIR-STEP-020	02-01	Power Input	Under voltage	STEP will switch off.	4	Check in HK the current voltage, compare against lower limit.	ICU sends event	3	Switch-off
FDIR-STEP-030	02-01	Power Input	Over voltage	STEP will switch off.	4	Check in HK the current voltage, compare against the upper limit.	ICU sends event	3	Switch-off
FDIR-STEP-040	02-01	Temperature	Over temperature	STEP damage/ space craft damage	4	Check in HK the current temperature, compare against the upper limit.	ICU sends event	3	Switch-off
FDIR-STEP-050	02-01	FPGA	FPGA not working	Loss of STEP	3	No TLM received	Detected in housekeeping of HET-EPT on ground	1	Cold reset. If problem persists switch-off
FDIR-STEP-060	02-01	Serial link	Serial link error	Loss of communication	3	No TLM received		1	Cold-reset If problem persists switch-off
FDIR-STEP-070	02-01	Serial link	Continuous CRC error	Loss of communication	3	Continuous CRC error	TM transmission not possible ICU sends event if error > 30	1	Increment error counter. If problem persists ground switch-off
FDIR-STEP-080	04-0n	EEPROM	EEPROM read-out error	STEP cannot be configured	3	No read-out TLM or continuous TLM CRC error	ICU sends event (0x4160)	1	Cold-reset. If problem persists switch-off.

Table 6-4. STEP FDIR procedures

6.4 SIS

SIS									
FDIR	**Circuit / Index**	**Function**	**Failure Mode**	**Consequence**	**Sev**	**Detection**	**Remarks**	**Recovery level**	**Recovery action**
FDIR-SIS-010	03-01	LCL	Open circuit	SIS cannot be switched ON	3	No TLM received	Detected in housekeeping of SIS on ground	1	If problem persists ground switch-off SIS-n.
DELETED									
DELETED									
FDIR-SIS-050	03-01	FPGA	FPGA not working	Loss of SIS	3	No TLM received		1	If problem persists ground switch-off
FDIR-SIS-060	03-01	Serial link	Serial link error	Loss of communication	3	No TLM received		1	Increment error counter. If problem persists ground switch-off
FDIR-SIS-070	03-01	Serial link	Continuous CRC error	Loss of communication	3	Continuous CRC error in TM	ICU sends event if error > 30	1	Increment error counter. If problem persists ground switch-off
FDIR-SIS-080	03-01	Status report	Bit flip not provided in Housekeeping	SIS is not working	4	Bit flip not provided in telemetry	Send event to ground 0x2003	1	If problem persists ground switch-off
FDIR-SIS-090	03-01	Power-off request	Bit signaling power-off request is signaled	SIS requests Power-off	4	Power-off bit set in telemetry	Send event to ground 0x2002	1	If problem persists ground switch-off

Table 6-5. SIS FDIR procedures