Pierre Auger Observatory

Surface Detector Electronics Upgrade
FMECA – FDIR Document

Abstract:
This document describes a functional analysis of the Surface Detector Electronics Upgrade followed with a Failure Mode Effects and Criticality Analysis (FMECA). The objective of these analyses is to identify failure modes that could degrade or cause loss of the Surface Detector Electronics or Station, to be able to propose mitigation solutions.

This document contains also the failure detection, isolation and recovery (FDIR) process description, implemented in the Slow Control Unit of the SDEU.

Document written by:	P. Stassi Project System engineer	*Agreed by:*	T. Suomijärvi Task leader
Date:	*28 November 2014*	*Date:*	*28 November 2014*
Local Reference:	*ATRIUM-2221*	*Project Reference:*	*WP10-LPSC-10C*

Table of Content

ACRONYMS

AD	Applicable Document
ADC	Analog to Digital Converter
BGA	Ball Grid Array
CPU	Central Processing Unit
CR	Configurational Requirement
DAC	Digital to Analog Converter
DC	Direct Current
ER	Environmental Requirement
FADC	Flash ADC
FDIR	Failure Detection, Isolation and Recovery
FMECA	Failure Mode, Effects and Criticality Analysis
FMEA	Failure Mode, Effects Analysis
FPGA	Filed Programmable Gate Array
FR	Functional Requirements
GPS	Global Positioning System
HSIA	Hardware Software Interaction Analysis
H/W	HardWare
ICD	Interfaces Control Document
IR	Interface Requirements
LVDS	Low Voltage Differential Signaling
n/a	non applicable
OR	Operational Requirements
OTG	On The Go
PBS	Product Breakdown Structure
PCB	printed Circuit Board
PMT	PhotoMultiplier Tube
PPS	Pulse Per Second
PR	Physical Requirements
QR	Quality Requirements
RD	Reference Document
SDE	Surface Detector Electronics
SPF	Single Point Failure
SPMT	Small PMT
SR	Support Requirements
S/W	SoftWare
TBC	To Be Confirmed
TBD	To Be Defined
TBW	To Be Written
TC	Tele-Command
TM	TeleMetry
TPCB	Tank Power Control Board
UB	Unified Board
UC	Upgrade Committee
USB	Universal Serial Bus
UUB	Upgraded Unified Board
UHE	Ultra High Energy
UHECR	Ultra High Energy Cosmic Ray
VM	Verification Matrix
WP	Work Package

DOCUMENT CHANGE RECORD

Issue	Revision	Issue Date	Changes Approved by	Modified Pages Numbers, Change Explanations and Status
10	A	04/02/14		DRAFT for approbation
10	B	26/02/14	P. Stassi	Minor update
10	C	28/11/14	P. Stassi	Minor update

1. INTRODUCTION

1.1 *Purpose and scope*

This document describes a functional analysis of the Surface Detector Electronics Upgrade followed with a Failure Mode Effects and Criticality Analysis (FMECA). The objective of these analyses is to identify failure modes that could degrade or cause loss of the Surface Detector Electronics or Station, to be able to propose mitigation solutions.

This document contains also the failure detection, isolation and recovery (FDIR) process description, implemented in the Slow Control Unit of the SDEU.

1.2 *Documents*

1.2.1 *Applicable Documents*

AD1	Failure Modes Effects and Criticality Analysis (ECSS-Q-30-02A)
AD2	Procedure for Performing a FMECA (MIL- STD-1629A)
AD3	Reliability Prediction of Electronic Equipment (MIL-HDBK-217F2)

1.2.2 *Reference Documents*

RD1	SDEU Development Plan, WP10LPSC02
RD2	SDEU Specifications, WP10LPSC03
RD3	SDEU Electrical Interfaces Control Document, WP10LPSC05
RD4	SDEU Detectors Interfaces Control Document, WP10LPSC07

2. INSTRUMENT DESCRIPTION AND FUNCTIONS

2.1 *Introduction*

The current Surface Detector electronics was designed 15 years ago by using the technology available at that time. Evolution in processors, power consumption of electronics components and timing systems make it possible today to design and implement a higher performance electronics system for the Surface Detector array. The new electronics system will enhance the data quality in terms of improved resolution, extended dynamic range, and new trigger possibilities. Furthermore, the calibration and monitoring capabilities will be enhanced increasing the overall reliability of the data taking. A short description of the Surface Detector Electronics Upgrade (SDE Upgrade) proposal is given below.

2.2 *SDEU Functional description (RD2)*

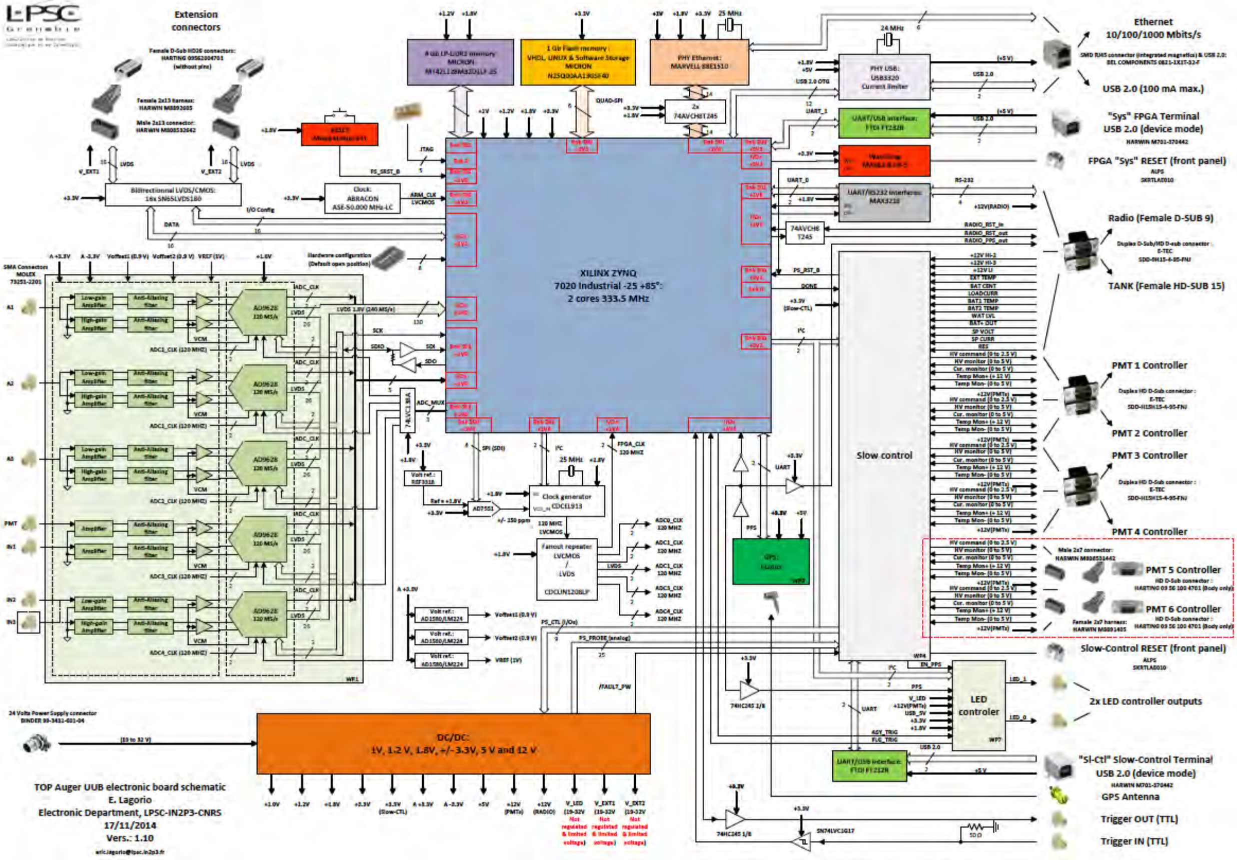

LPSC Grenoble
Extension connectors
Female D-Sub HD26 connectors: HARTING 09562004701 (without pins)
Female 2x13 harness: HARWIN M8892605
Male 2x13 connector: HARWIN M80-8532642
V_EXT1
V_EXT2
LVDS
Bidirectionnal LVDS/CMOS: 16x SN65LVDS180
Clock: ABRACON ASE-50.000 MHz-LC
ARM_CLK LVCMOS
I/O Config
DATA
JTAG
PS_SRST_B
4 Gb LP-DDR2 memory MICRON
1 Gb Flash memory: VHDL, LINUX & Software Storage MICRON N25Q00AA13GSF40
PHY Ethernet: MARVELL 88E1510
QUAD-SPI
2x 74AVCH8T245
25 MHz
Hardware configuration (Default open position)
XILINX ZYNQ 7020 Industrial -25 +85°: 2 cores 333.5 MHz
SMA Connectors MOLEX 73251-2201
A1
A2
A3
PMT
IN1
IN2
IN3
Low-gain Amplifier
High-gain Amplifier
Amplifier
Anti-Aliasing filter
AD9628 120 MS/s
ADC_CLK
VCM
LVDS 1.8V (240 MS/s)
ADC1_CLK (120 MHz)
ADC2_CLK (120 MHz)
ADC3_CLK (120 MHz)
ADC4_CLK (120 MHz)
SCK
SDIO
SDI
SDO
74LVC138A
ADC_MUX
SPI (SDI)
I²C
FPGA_CLK 120 MHz
Volt ref.: REF3318
AD7551
Clock generator CDCE913
+/- 150 ppm
120 MHz LVCMOS
Fanout repeater LVCMOS / LVDS CDCLVN1208LP
ADC0_CLK 120 MHZ
ADC1_CLK 120 MHZ
ADC2_CLK 120 MHZ
ADC3_CLK 120 MHZ
ADC4_CLK 120 MHZ
Volt ref.: AD1580/LM224
Voffset1 (0.9 V)
Voffset2 (0.9 V)
VREF (1V)
PS_CTL (I/Os)
PS_PROBE (analog)
/FAULT_PW
24 MHz
PHY USB: USB3320 Current limiter
USB 2.0 OTG
UART_1
UART/USB interface: FTDI FT232R
Watchdog
UART_0
UART/RS232 interface: MAX3218
RS-232
+12V(RADIO)
74AVCH8 T245
RADIO_RST_in
RADIO_RST_out
RADIO_PPS_out
PS_RST_B
DONE
+3.3V (Slow-CTL)
Slow control
+12V HI-2
+12V HI-3
+12V LI
EXT TEMP
BAT CENT
LOADCURR
BAT1 TEMP
BAT2 TEMP
WAT LVL
BAT+ OUT
SP VOLT
SP CURR
RES
HV command (0 to 2.5 V)
HV monitor (0 to 5 V)
Cur. monitor (0 to 5 V)
Temp Mon+ (+ 12 V)
Temp Mon- (0 to 5 V)
+12V(PMTs)
Ethernet 10/100/1000 Mbits/s
SMD RJ45 connector (integrated magnetics) & USB 2.0: BEL COMPONENTS 0821-1X1T-32-F
USB 2.0 (100 mA max.)
"Sys" FPGA Terminal USB 2.0 (device mode)
HARWIN M701-370442
FPGA "Sys" RESET (front panel)
ALPS SKRTLAE010
Radio (Female D-SUB 9)
Duplex D-Sub/HD D-sub connector: E-TEC SDD-9H15-4-95-FNJ
TANK (Female HD-SUB 15)
PMT 1 Controller
Duplex HD D-Sub connector: E-TEC SDD-H15H15-4-95-FNJ
PMT 2 Controller
PMT 3 Controller
PMT 4 Controller
PMT 5 Controller
PMT 6 Controller
HD D-Sub connector: HARTING 09 56 100 4701 (Body only)
Female 2x7 harness: HARWIN M8891405
Slow-Control RESET (front panel)
GPS: Motion
PPS
UART
EN_PPS
LED controler
LED_1
LED_0
V_LED
USB_5V
ASY_TRIG
FLG_TRIG
2x LED controller outputs
UART/USB interface: FTDI FT232R
USB 2.0
"Sl-Ctl" Slow-Control Terminal USB 2.0 (device mode)
GPS Antenna
74HC245 1/8
SN74LVC1G17
Trigger OUT (TTL)
Trigger IN (TTL)
24 Volts Power Supply connector BINDER 09-3431-601-04
(19 to 32 V)
DC/DC: 1V, 1.2 V, 1.8V, +/- 3.3V, 5 V and 12 V
+1.0V
+1.2V
+1.8V
+3.3V
+3.3V (Slow-CTL)
A+3.3V
A-3.3V
+5V
+12V (PMTs)
+12V (RADIO)
V_LED (19-32V Not regulated & limited voltage)
V_EXT1 (19-32V Not regulated & limited voltage)
V_EXT2 (19-32V Not regulated & limited voltage)
TOP Auger UUB electronic board schematic
E. Lagorio
Electronic Department, LPSC-IN2P3-CNRS
17/11/2014
Vers.: 1.10
eric.lagorio@lpsc.in2p3.fr

Figure 2.3.a: ***SDEU Functional Block Diagram***

The design objectives of the SDE Upgrade globally aim to increase the data quality (faster sampling for ADC traces, better timing accuracy, increased dynamic range), to enhance the local trigger and processing capabilities (more powerful local station processor and FPGA) and to improve calibration and monitoring capabilities of the Surface Detector stations.

The design objectives also aim for higher reliability and easy maintenance. An important feature in the design of the upgraded SD electronics is a facility for interfacing additional sensors. The speed of the upgraded CPU will be >10 times faster than the current one, with a commensurate increase in memory. This will allow much more sophisticated processing in the local station. The addition of accessible trigger IN/OUT and GPS 1 PPS signals will simplify time synchronization with other upgrade possibilities.

High speed USB interfaces and direct connection to the trigger will allow interfacing a variety of additional sensors.

The proposed upgrade involves the main electronics boards: the Unified Board and the Front End board of the current electronics. The interface board to the power system, the Tank Power Control Board (TPCB), will not be upgraded, and the interface to the communication system will also remain unchanged. Furthermore, new functionalities will be added to the tank calibration LED system and to the monitoring system. The dynamic range will be increased by adding a small PMT (SPMT) to the current 3 large 9 inch PMTs. All the functionalities will be implemented in a single board, called Upgraded Unified Board (UUB). The main design features of the proposed electronics are described below. The anode channel of the large PMTs will be split and amplified to have a gain ratio of 32. The signals will be filtered and digitized by commercial 12 bit 120MHz FADCs. The design of the current LED controller will be upgraded to enhance the precision of the calibration and to allow simulation of shower events. The upgraded system will extend the capabilities of the present system for both small and large signals. The least FADC count will have a 4 times smaller step than the present system, improving the precision of the low threshold triggers. 10 FADC channels will be implemented. This leaves extra channels for additional detectors.

2.3 *SDEU Interface Configuration (RD2)*

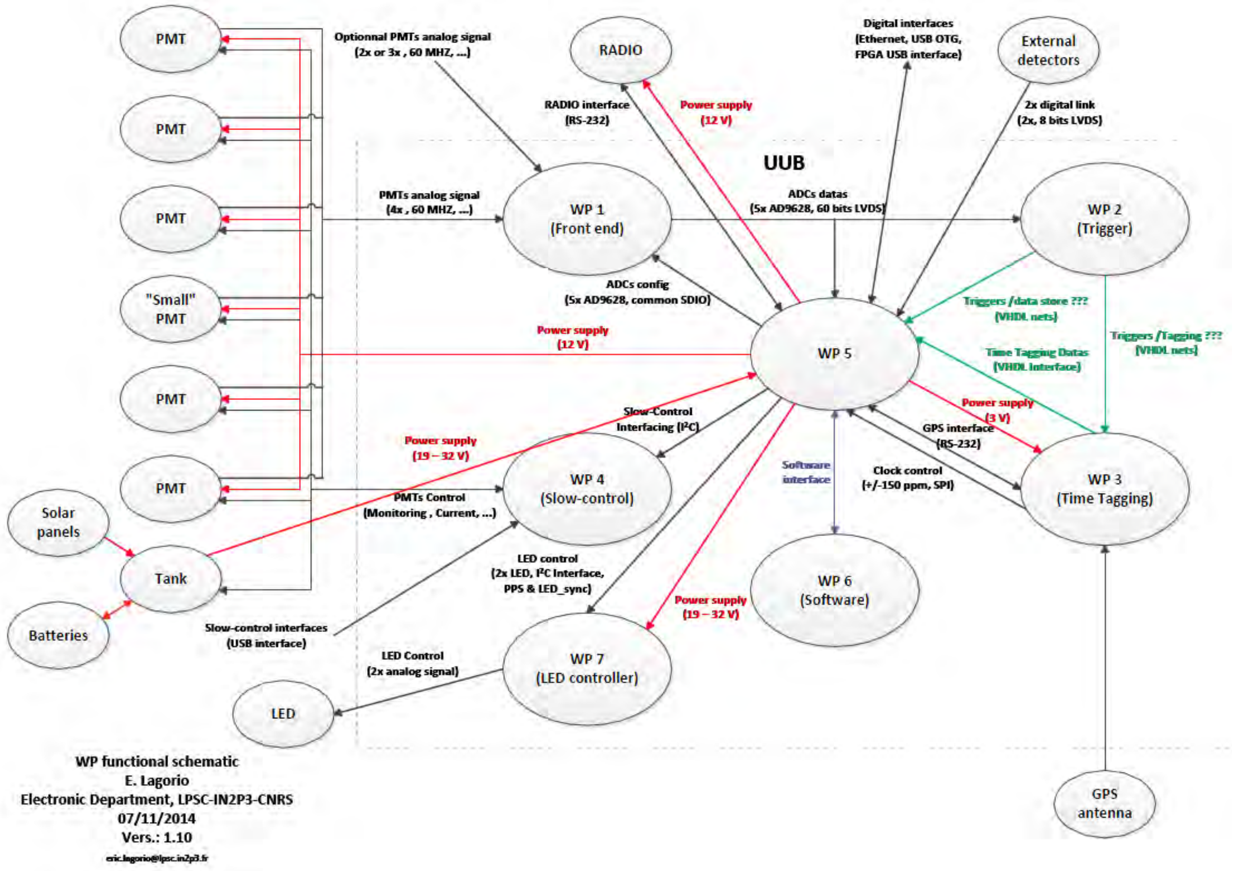
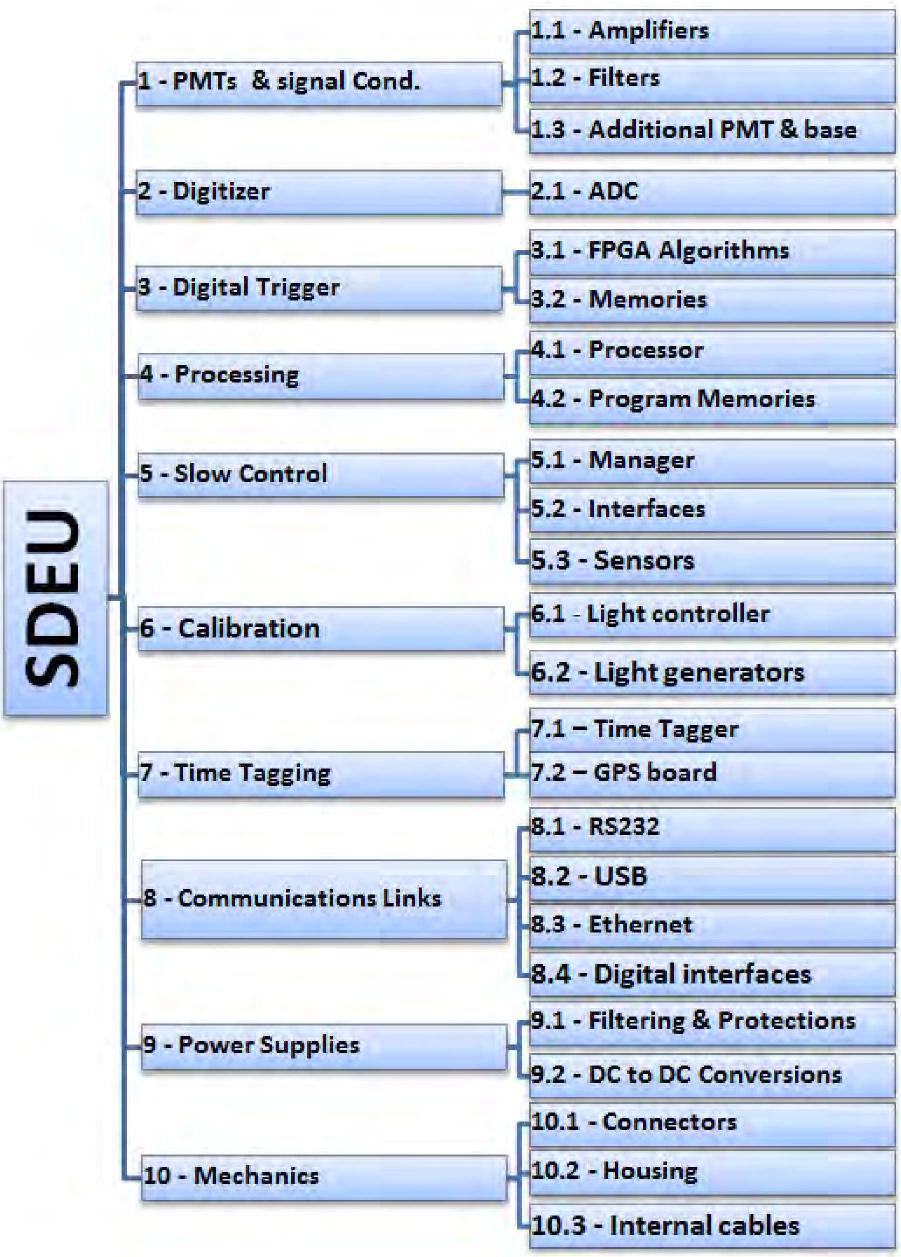

PMT
PMT
PMT
"Small" PMT
PMT
PMT
Solar panels
Tank
Batteries
LED
Optionnal PMTs analog signal (2x or 3x , 60 MHZ, ...)
RADIO
RADIO interface (RS-232)
Power supply (12 V)
Digital interfaces (Ethernet, USB OTG, FPGA USB interface)
External detectors
2x digital link (2x, 8 bits LVDS)
UUB
PMTs analog signal (4x , 60 MHZ, ...)
WP 1 (Front end)
ADCs datas (5x AD9628, 60 bits LVDS)
WP 2 (Trigger)
ADCs config (5x AD9628, common SDIO)
Power supply (12 V)
WP 5
Triggers /data store ??? (VHDL nets)
Time Tagging Datas (VHDL Interface)
Triggers /Tagging ??? (VHDL nets)
Power supply (19 – 32 V)
Slow-Control Interfacing (I²C)
Power supply (3 V)
GPS interface (RS-232)
Software interface
Clock control (+/-150 ppm, SPI)
WP 4 (Slow-control)
PMTs Control (Monitoring , Current, ...)
WP 3 (Time Tagging)
LED control (2x LED, I²C Interface, PPS & LED_sync)
Power supply (19 – 32 V)
WP 6 (Software)
Slow-control interfaces (USB interface)
LED Control (2x analog signal)
WP 7 (LED controller)
GPS antenna
WP functional schematic
E. Lagorio
Electronic Department, LPSC-IN2P3-CNRS
07/11/2014
Vers.: 1.10
eric.lagorio@lpsc.in2p3.fr

Figure 2.4.a: Interface configuration

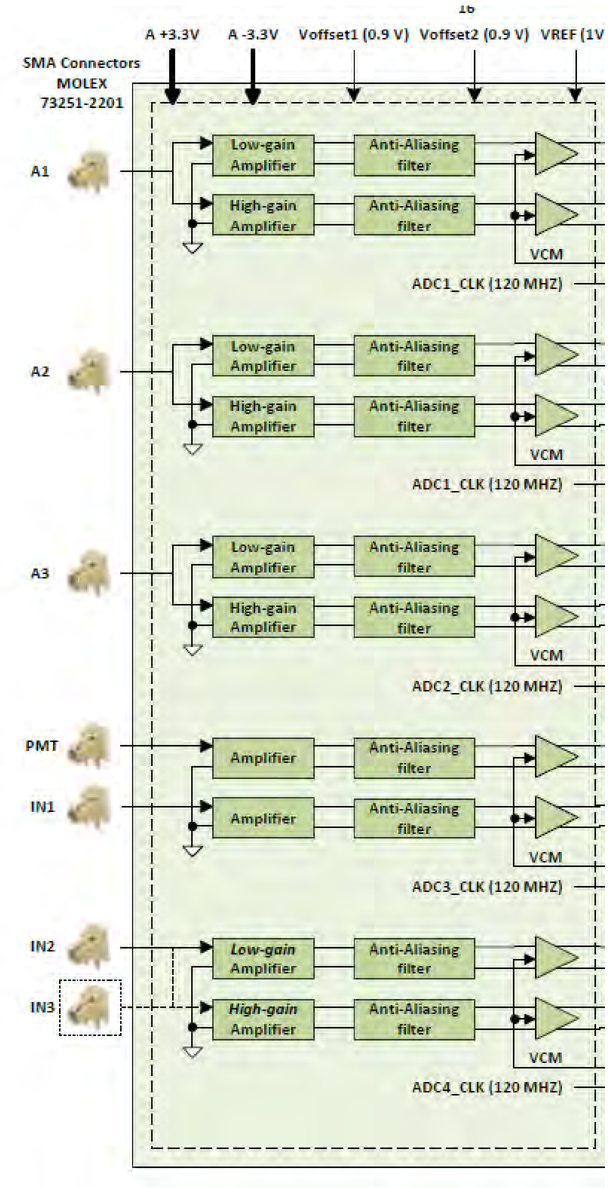
Figure 2.4.a shows the interface between the UUB and the other part of the SD.

2.4 *SDEU Product tree (RD1)*



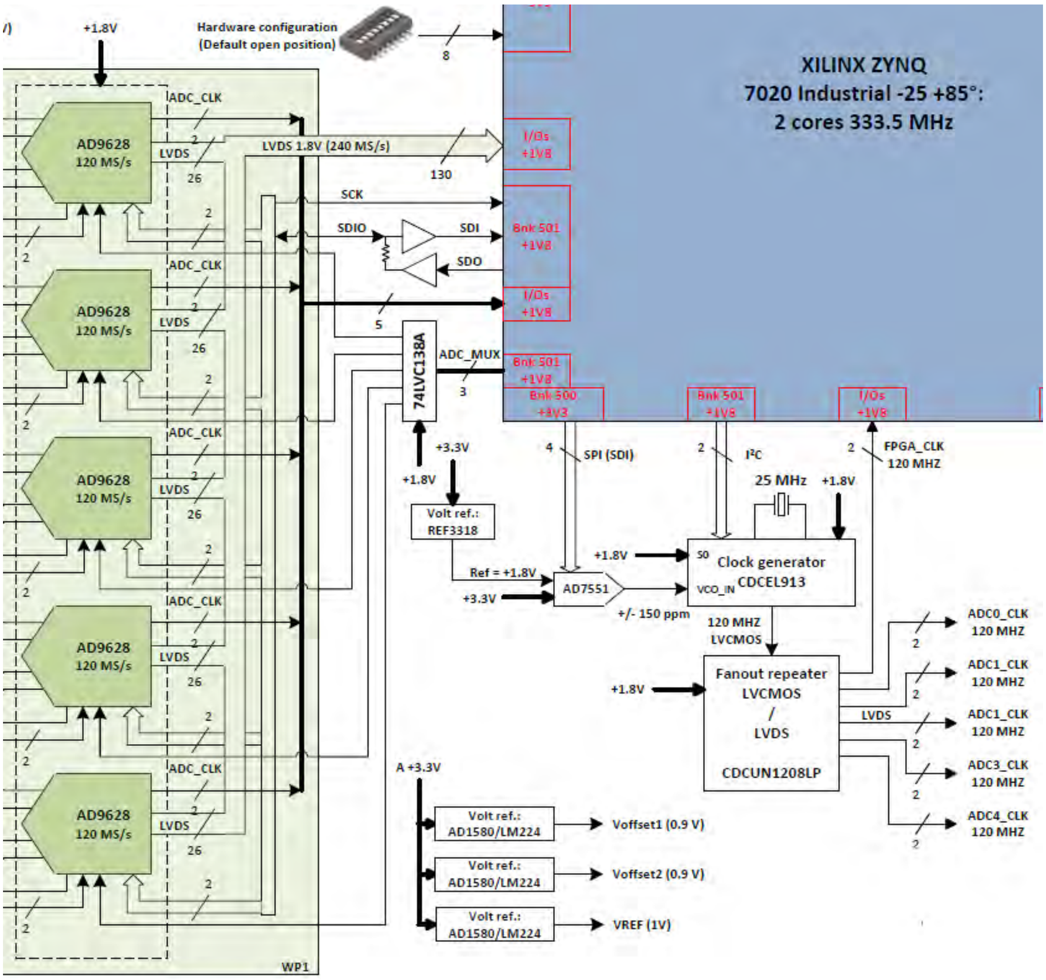
3. PRODUCT DESCRIPTION DIAGRAMS

3.1 *PMT and signal conditioning,*



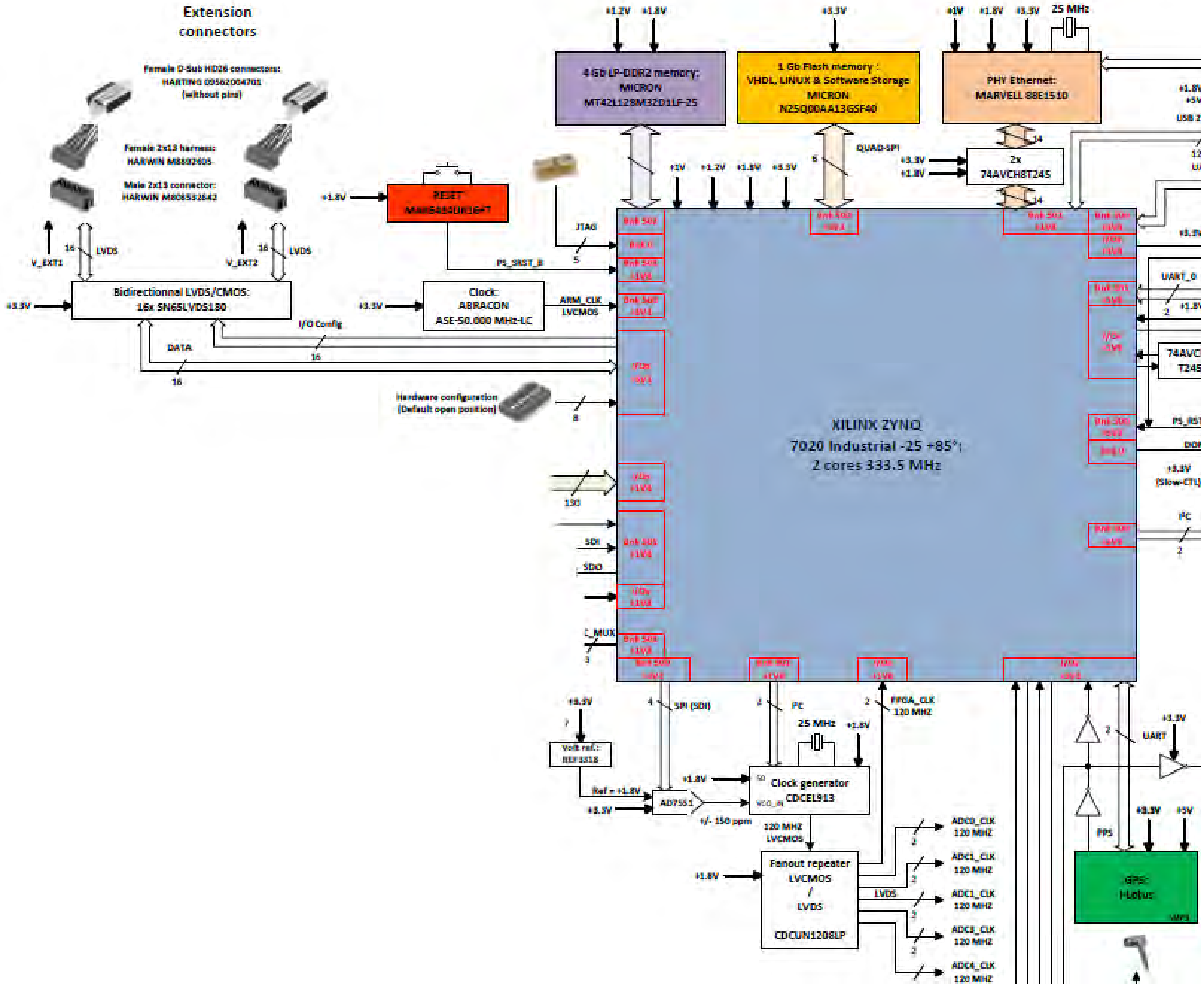
10 ADC channel are implemented, 6 for the three 9 inch actual PMTs anodes (IN1, IN2, IN3), one for the SPMT anode. The other channels are used by the ASCII detector. The design will be adjusted after the detector test phase.

3.2 *Digitizer*



The signals will be digitized by commercial 12 bits 120MHz dual FADCs, with analog differential inputs and LVDS digital outputs.

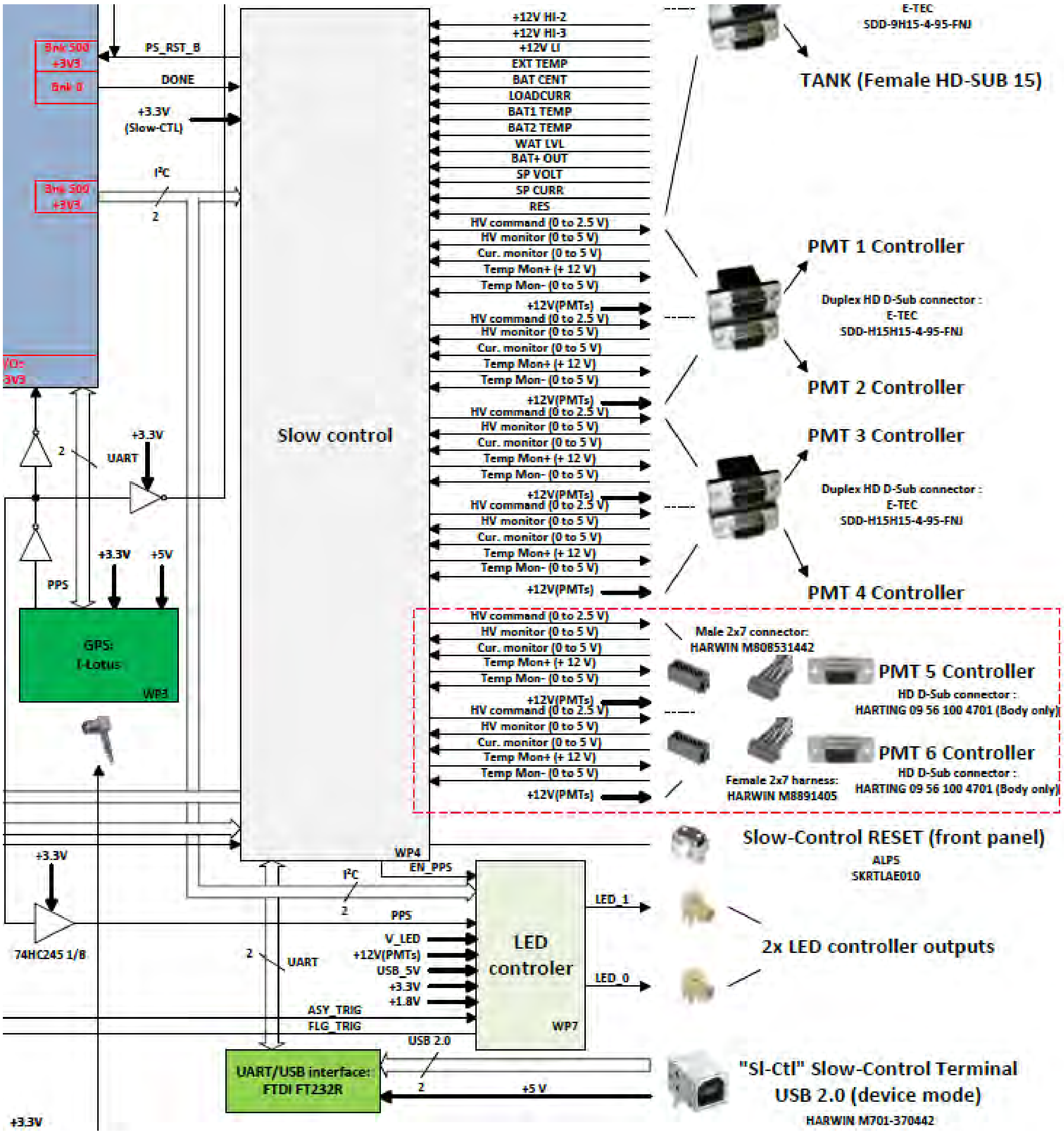
3.3 *Processing, Trigger and Time tagging,*



The processing unit is based on an architecture with an FPGA containing an LINUX based embedded ARM processor. The trigger and time tagging functionalities will also be implemented in the FPGA. The speed of the upgraded CPU will be >10 times faster than the current one, with a commensurate increase in memory. This will allow much more sophisticated processing in the local station.

The commercial GPS board with enhanced accurate precision in timing is used with an upgraded Time Tagging algorithm contained in the FPGA.

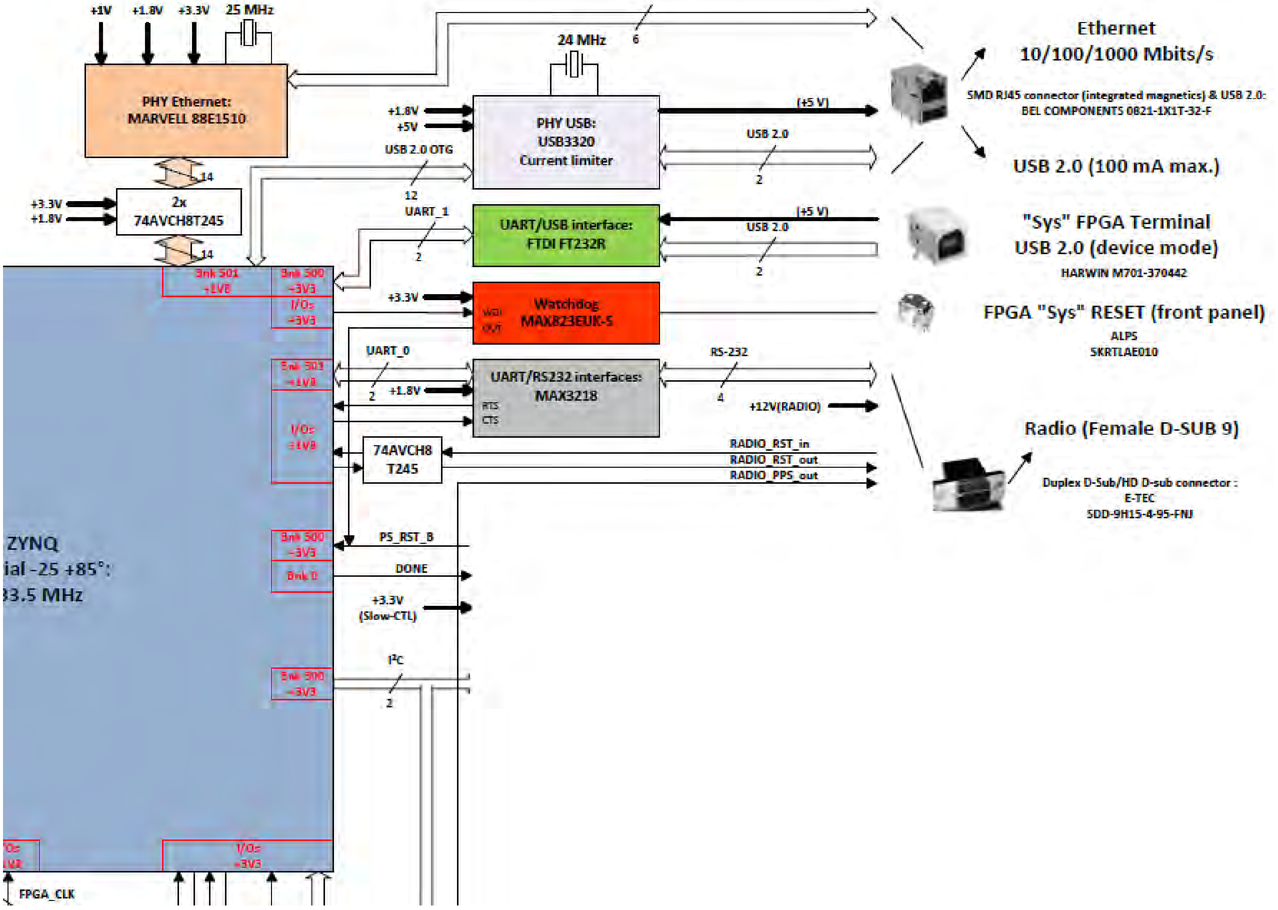
3.4 *Slow Control and Calibration unit,*



The slow control system is derived from the Auger Engineering Radio Array design; incorporating a separate micro-controller (MSP430) is used. 64 channels are implemented for the slow control ADC. Currently 35 channels are required; leaving free channels for test purposes and for additional detectors.

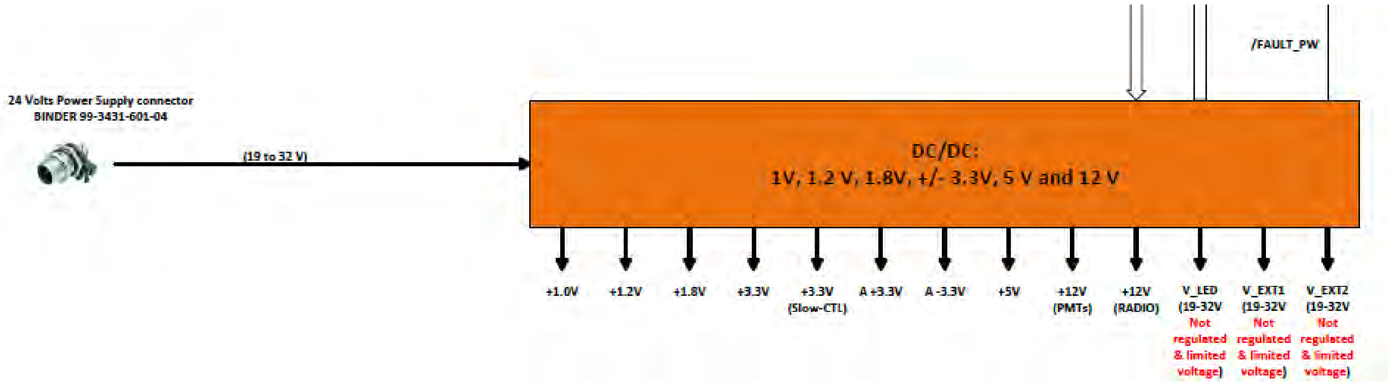
An USB communication link is dedicated to the Slow Control system monitoring.

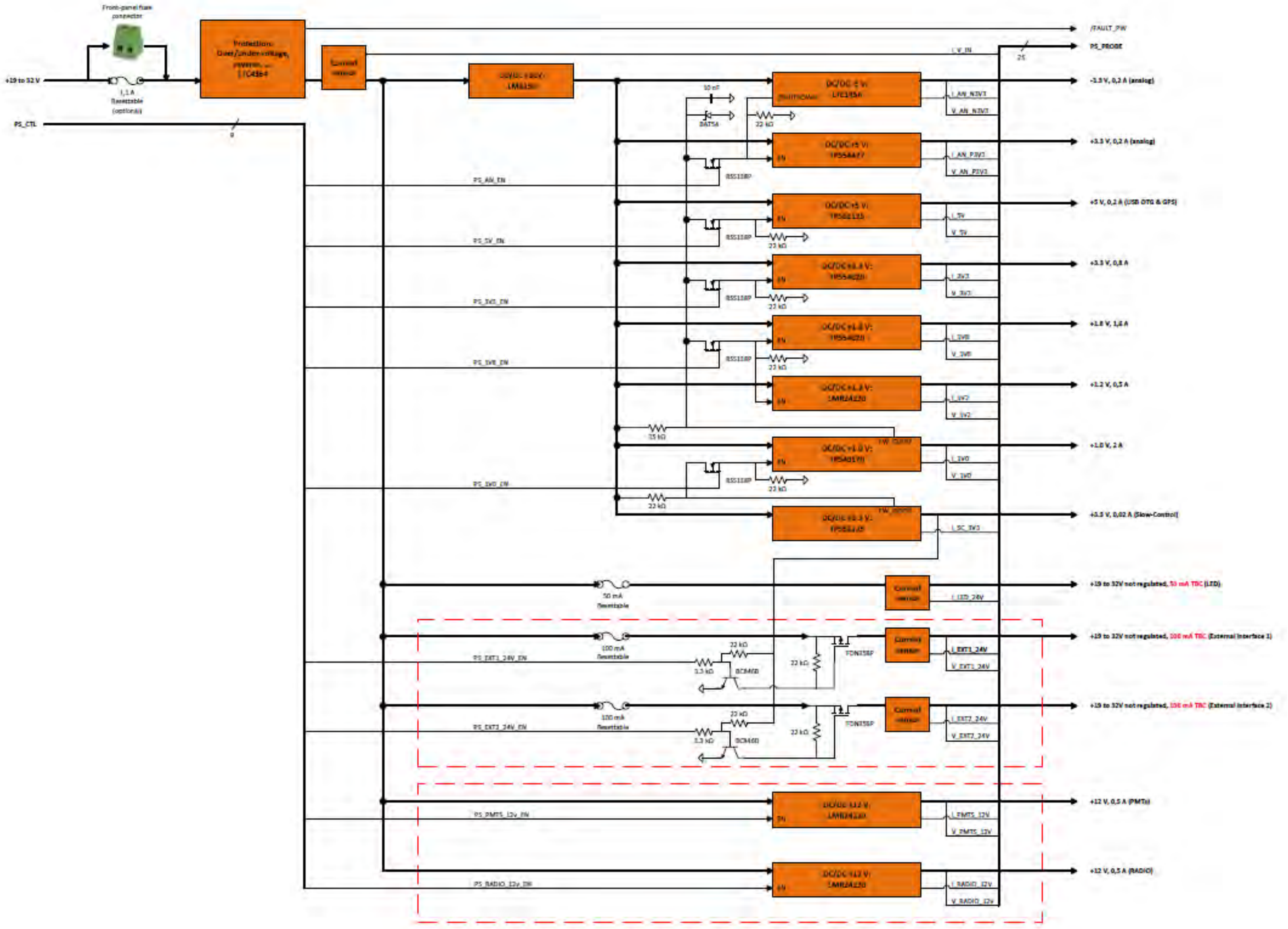
3.5 *Communication links,*



Ethernet and UBS OTG are implemented for communication purpose. A dedicated USB port is implemented for FPGA system monitoring.

3.6 *Power supplies,*

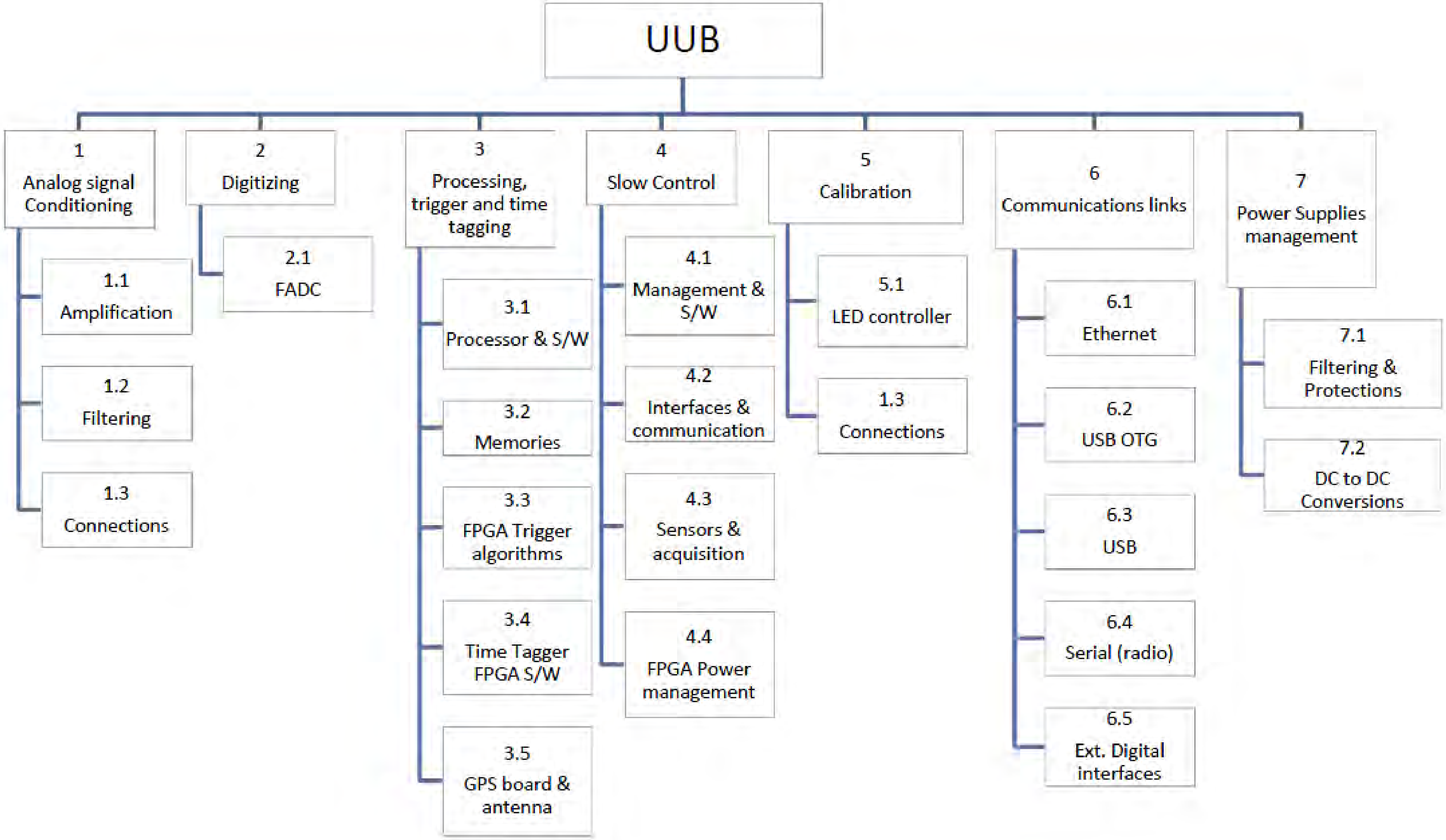

/FAULT_PW
24 Volts Power Supply connector
BINDER 99-3431-601-04
(19 to 32 V)
DC/DC:
1V, 1.2 V, 1.8V, +/- 3.3V, 5 V and 12 V
+1.0V
+1.2V
+1.8V
+3.3V
+3.3V (Slow-CTL)
A +3.3V
A -3.3V
+5V
+12V (PMTs)
+12V (RADIO)
V_LED (19-32V Not regulated & limited voltage)
V_EXT1 (19-32V Not regulated & limited voltage)
V_EXT2 (19-32V Not regulated & limited voltage)



All power supplies are built from the +19 to +32 Volts supplied by the solar panels system and the TPCB.

4. UUB FUNCTIONAL ANALYSIS

4.1 *Functions identification and hierarchical structure*



5. SDEU-UUB FAILURE MODE, EFFECTS AND CRITICAL ANALYSIS (FMECA)

Note: Severity Classification used for this analysis (AD1, AD2).

I - Catastrophic	= A failure which may cause SD station loss.
II - Critical	= A failure which may cause major system damage which will result on SDE loss.
III - Marginal	= A failure which may cause minor system damage which will result in delay or loss of part of SDE availability.
IV – Minor	= A failure not serious enough to cause system damage but which will result in unscheduled repair.

5.1 *Analog Signal Conditioning Failure Mode and Effects Analysis (FMEA)*

ID #	Item Description	Function Description	Failure Mode	Most Probable cause	Failure Effect on			Severity	Failure Mode Detection	Remarks
					SDEU	SD Station	PAO			
1.1	**Analog signal conditioning**	Input connection	No or wrong signal	Bad cleanliness Or SMA connector degraded	1 PMT signals unavailable	Science losses on one PMT	Science loss on one station	*IV - Minor*	Off line monitoring	Maintenance requested
1.2		Input buffer	No or wrong signal	Amplifier failure	1 PMT signals unavailable	Science losses on one PMT	Science loss on one station	*IV - Minor*	Off line monitoring	Maintenance requested
1.3		Low or high gain amplification	No or wrong signal	Amplifier failure	1 PMT low or high gain signals unavailable	Science losses on one PMT	Science loss on one station	*IV - Minor*	Off line monitoring	Maintenance requested
1.4		Anti-aliasing filter	No or wrong signal	Discrete component connection failure	1 PMT signals unavailable	Science losses on one PMT	Science loss on one station	*IV - Minor*	Off line monitoring	Maintenance requested

5.2 *Digitizing FMEA*

ID #	Item Description	Function Description	Failure Mode	Most Probable cause	Failure Effect on			Severity	Failure Mode Detection	Remarks
					SDEU	SD Station	PAO			
2.1	**Digitizing**	Signal digitizing	No or Wrong digital signal	ADC Failure	1 PMT signals unavailable	Science losses on one PMT	Science loss on one station	*IV - Minor*	Off line monitoring	Maintenance requested

5.3 *Processing, Trigger and Time tagging FME.*

ID #	Item Description	Function Description	Failure Mode	Most Probable cause	Failure Effect on			Severity	Failure Mode Detection	Remarks
					SDEU	SD Station	PAO			
3.1	**Processing, Trigger and Time tagging**	Processing	No or wrong processing	S/W corrupted	Not available	Not available	Science Loss	*III - Marginal*	Off line monitoring & Slow control on site	
3.2				Power supply failure	Not available	Not available	Science Loss	*II - Critical*	Off line monitoring & Slow control on site	
3.3				FPGA failure	Not available	Not available	Science Loss	*II - Critical*	Off line monitoring & Slow control on site	
3.4		Memory R/W access	No or wrong data in R/W process	Memory chip failure	Not available	Not available	Science Loss	*II - Critical*	Off line monitoring	
3.5				Connection failure	Not available	Not available	Science Loss	*II - Critical*	Off line monitoring	
3.6				Power supply failure	Not available	Not available	Science Loss	*II - Critical*	Off line monitoring & Slow control on site	
3.7		Trigger algorithm	No or wrong trigger signal	Analog signal not present	Not available	Not available	Science Loss	*III - Marginal*	Off line monitoring	
3.8				S/W corrupted	Not available	Not available	Science Loss	*III - Marginal*	Off line monitoring	
3.9				FPGA failure	Not available	Not available	Science Loss	*II - Critical*	Off line monitoring & Slow control on site	
3.10		Time Tagging process and GPS operation	No or Bad Tagging	S/W corrupted	Time tagging not available	Science Loss	Science Loss	*III - Marginal*	Off line monitoring	
3.11				FPGA failure	Not available	Not available	Science Loss	*II - Critical*	Off line monitoring & Slow control on site	
3.12			No or wrong 1PPS signal	GPS Board failure	Time tagging not available	Science Loss	Science Loss	*III - Marginal*	Off line monitoring	
3.13				Connection failure	Time tagging not available	Science Loss	Science Loss	*III - Marginal*	Off line monitoring	
3.14				Antenna failure	Time tagging not available	Science Loss	Science Loss	*III - Marginal*	Off line monitoring	
3.15				Power supply failure	Not available	Science Loss	Science Loss	*III - Marginal*	Off line monitoring & Slow control on site	

5.4 *Slow Control FMEA*

ID #	Item Description	Function Description	Failure Mode	Most Probable cause	Failure Effect on			Severity	Failure Mode Detection	Remarks
					SDEU	SD Station	PAO			
4.1	**Slow Control**	Processing and S/W	No or wrong processing	Micro-controller failure	Not available	Not available	Science Loss	*II - Critical*	Off line monitoring & Slow control on site	
4.2				S/W corrupted	Not available	Not available	Science Loss	*II - Critical*	Off line monitoring & Slow control on site	
4.3		I/O, interface & Communications	No or wrong data reading	S/W corrupted	Slow control data not available	Not available	Science Loss	*III - Marginal*	Off line monitoring & Slow control on site	
4.4				Sensor failure	Part of Slow control data not available	Not available	Science Loss	*III - Marginal*	Off line monitoring & Slow control on site	
4.5				Interface chip failure	Not available	Not available	Science Loss	*III - Marginal*	Off line monitoring & Slow control on site	
4.6				Peripheral unit or connection failure	Part of Slow control data not available	Not available	Science Loss	*II - Critical*	Off line monitoring & Slow control on site	
4.7			No or wrong data writing	S/W corrupted	Slow control data cannot be send	Not available	Science Loss	*II - Critical*	Off line monitoring & Slow control on site	
4.8				Interface chip failure	Not available	Not available	Science Loss	*II - Critical*	Off line monitoring & Slow control on site	
4.9				Connection failure	Part of Slow control data not available	Not available	Science Loss	*III - Marginal*	Off line monitoring & Slow control on site	
4.10		FPGA Power supplies control	No or wrong data R/W	Micro-controller failure	Not available	Not available	Science Loss	*II - Critical*	Off line monitoring & Slow control on site	
4.11				S/W corrupted	Part of Slow control data not available	Not available	Science Loss	*II - Critical*	Off line monitoring & Slow control on site	
4.12				Connection failure	Part of Slow control data not available	Not available	Science Loss	*II - Critical*	Off line monitoring & Slow control on site	

5.5 *Calibration FMEA*

ID #	Item Description	Function Description	Failure Mode	Most Probable cause	Failure Effect on			Severity	Failure Mode Detection	Remarks
					SDEU	SD Station	PAO			
5.1	**Calibration**	LED Controller signal generation	No or wrong signal	Component failure	Calibration not available	Calibration not possible if needed	Possible science Loss	*IV - Minor*	Off line monitoring	
5.2				Bad cleanliness Or SMA connector degraded	Calibration not available	Calibration not possible if needed	Possible science Loss	*IV - Minor*	Off line monitoring	
5.3			No FPGA communication	FPGA failure	Not available	Not available	Science Loss	*II - Critical*	Off line monitoring & Slow control on site	
5.4				Connection failure	Calibration not available	Calibration not possible if needed	Possible science Loss	*III - Marginal*	Off line monitoring & Slow control on site	
5.5			No synchronization with 1 PPS signal	GPS unit failure	Calibration and time tagging not available	Science Loss	Science Loss	*III - Marginal*	Off line monitoring	
5.6				Connection failure	Calibration and time tagging not available	Science Loss	Science Loss	*IV - Minor*	Off line monitoring	
5.7			No or wrong delay in the signal	Component failure	Fake showers not available	Fake showers not available	Science Loss	*IV - Minor*	Off line monitoring	

5.6 *Communications links FMEA*

ID #	Item Description	Function Description	Failure Mode	Most Probable cause	Failure Effect on			Severity	Failure Mode Detection	Remarks
					SDEU	SD Station	PAO			
6.1	**Communications links**	Ethernet communication	No or wrong communication	Interface component failure	Ethernet not available	Ethernet not available	No effect	*IV - Minor*	On site	
6.2				FPGA failure	Not available	Not available	Science Loss	*II - Critical*	Off line monitoring & Slow control on site	
6.3				S/W corrupted	Ethernet not available	Ethernet not available	No effect	*IV - Minor*	On site	
6.4		USB OTG Communication	No or wrong communication	Interface component failure	USB for ext. device not available	USB for ext. device not available	No effect	*IV - Minor*	On site	
6.5				FPGA failure	Not available	Not available	Science Loss	*II - Critical*	Off line monitoring & Slow control on site	
6.6				S/W corrupted	Interface component failure	USB for ext. device not available	No effect	No effect	*IV - Minor*	
6.7		USB FPGA device mode Communication	No or wrong communication	Interface component failure	FPGA maintenance not available	Possible science loss	Possible science loss	*IV - Minor*	On site	
6.8				FPGA failure	Not available	Not available	Science Loss	*II - Critical*	Off line monitoring & Slow control on site	
6.9				S/W corrupted	FPGA maintenance not available	Possible science loss	Possible science loss	*IV - Minor*	On site	
6.10		USB slow control device mode communication	No or wrong communication	Interface component failure	Slow Control maint. not available	Possible science loss	Possible science loss	*IV - Minor*	On site	
6.11				FPGA failure	Not available	Not available	Science Loss	*II - Critical*	Off line monitoring & Slow control on site	
6.12				S/W corrupted	Slow Control maint. not available	Possible science loss	Possible science loss	*IV - Minor*	On site	
6.13		Serial communication (radio)	No or wrong communication	Interface component failure	Not available	Not available	Science Loss	*III - Marginal*	Off line monitoring	
6.14				FPGA failure	Not available	Not available	Science Loss	*II - Critical*	Off line monitoring & Slow control on site	
6.15				S/W corrupted	Not available	Not available	Science Loss	*III - Marginal*	Off line monitoring	
6.16		External digital communication (LVDS)	No or wrong communication	Interface component failure	External data not available	Possible science loss	Possible science loss	*IV - Minor*	Off line monitoring	
6.17				FPGA failure	Not available	Not available	Science Loss	*II - Critical*	Off line monitoring & Slow control on site	
6.18				S/W corrupted	External data not available	Possible science loss	Possible science loss	*IV - Minor*	Off line monitoring	

5.7 Power supplies FMEA.

ID #	Item Description	Function Description	Failure Mode	Most Probable cause	Failure Effect on			Severity	Failure Mode Detection	Remarks
					SDEU	SD Station	PAO			
7.1	**Power supplies**	+/- 3.3V production for analogic	No or wrong voltage	DC/DC failure	Analog FE unavailable	Not available	Science Loss	*III - Marginal*	Off line monitoring & Slow control on site	
7.2				Connection failure	Analog FE unavailable	Not available	Science Loss	*III - Marginal*	Off line monitoring & Slow control on site	
7.3		+3.3V, +1.8V, +1.2V, +1V production for digital	No or wrong voltage	DC/DC failure	Not available	Not available	Science Loss	*II - Critical*	Off line monitoring & Slow control on site	
7.4				Connection failure	Not available	Not available	Science Loss	*II - Critical*	Off line monitoring & Slow control on site	
7.5		+3.3V and +19 to 32V for LED controller	No or wrong voltage	DC/DC failure	Calibration not available	Calibration not possible if needed	Possible science Loss	*III - Marginal*	Off line monitoring & Slow control on site	
7.6				Connection failure	Calibration not available	Calibration not possible if needed	Possible science Loss	*III - Marginal*	Off line monitoring & Slow control on site	
7.7		+3.3V for Slow control	No or wrong voltage	DC/DC failure	Slow control not available	Not available	Science Loss	*II - Critical*	Off line monitoring & Slow control on site	
7.8				Connection failure	Slow control not available	Not available	Science Loss	*II - Critical*	Off line monitoring & Slow control on site	
7.9		+12V for PMTs	No or wrong voltage	DC/DC failure	1 PMT signals unavailable	Science losses on one PMT	Science loss on one station	*IV - Minor*	Off line monitoring & Slow control on site	
7.10				Connection failure	1 PMT signals unavailable	Science losses on one PMT	Science loss on one station	*IV - Minor*	Off line monitoring & Slow control on site	
7.11		+12V for Radio com.	No or wrong voltage	DC/DC failure	Not available	Not available	Science Loss	*III - Marginal*	Off line monitoring	
7.12				Connection failure	Not available	Not available	Science Loss	*III - Marginal*	Off line monitoring	
7.13		Ext1 or Ext2 +24V	No or wrong voltage	Component failure	Ext +24V unavailable	No effect	Science Loss	*IV - Minor*	Off line monitoring	

5.8 *Criticality Analysis*

5.8.1 *Critical Items lists*

Failure rate definition: **λp** = number of failures/10^6 hours. The data source is the AD3 document. The general parameters for each part are:

- Junction Temperature = 67 °C (45 + 22)
- Environment factor = G_F (Ground, Fixed)
- Learning factor= 1 (>2 years production)

5.8.1.1 Analog Signal Conditioning

ITEM	Function	Failure Rate (λp)	Remarks
ADA4927	Amplifiers, buffers	0.039	
Discrete SMD	filters	0.720	
SMA Socket	connectors	0.011	

5.8.1.2 Digitizing

ITEM	Function	Failure Rate (λp)	Remarks
AD9628	ADC digitizer	0.065	

5.8.1.3 Processing, Trigger and Time tagging

ITEM	Function	Failure Rate (λp)	Remarks
ZINQ 7020 Indus.	FPGA	0.530	
MT42L128M32D1LG-25	Memories DDR	0.140	
N25Q00AA13GSF40	Memories Flash	0.071	
M12M I Lotus	GPS board	0.030	
Motorola T2000	GPS Antenna	0.010	estimated
N type	Connectors	0.011	estimated

5.8.1.4 Slow Control

ITEM	Function	Failure Rate (λp)	Remarks
MSP430F2618	Micro controller	0.490	
ADG608	8 Ch. Multiplexor	0.066	
LTC2637	DAC	0.066	
BMP085	Pressure sensors	0.020	

5.8.1.5 Calibration

ITEM	Function	Failure Rate (λp)	Remarks
LM224D	Amplifiers	0.039	
AD5316	DAC	0.066	
MMBT3904LT1	Transistors	0.160	
SMA	Connectors	0.011	

5.8.1.6 Communications links

ITEM	Function	Failure Rate (λp)	Remarks
Marvell 88E1518	Eth interface	0.080	
USB3320	USB OTG interface	0.080	
FTDIFT32232R	USB interface	0.080	
MAX3218	Serial interface	0.080	
74AVCH8T245	Buffers drivers translator	0.080	

5.8.1.7 Power supplies

ITEM	Function	Failure Rate (λp)	Remarks
LM3150	DC/DC converter	0.065	
LTC1174	DC/DC converter	0.065	
TPS62125	DC/DC converter	0.065	
TPS54020	DC/DC converter	0.065	
LMR24220	DC/DC converter	0.065	
TPS40170	DC/DC converter	0.065	
BSS138P	FET Switch	0.160	
BC846B	Bip. transistor	0.160	
FDN358P	FET Switch	0.160	
?	Resettable fuse	0.560	estimated

5.8.2 *Critical Analysis process*

The process performed here is following the AD3 document. The aim of the critical analysis is to calculate Criticality Number for Failure Mode (Cm), representing the level of criticality for each failure mode, and the Item Criticality Number (Cr), representing the level of criticality for each considered item (component). The item criticality number helps the designer to isolate the most critical components and to propose mitigation solutions (redundancy, protection, etc.).

According to the AD3 document Cm and Cr are defined as follow:

$$Cm = \beta.\alpha.\lambda p.t \quad and \quad Cr = \sum_{n}^{1}(\beta.\alpha.\lambda p.t)_n$$

With:
n = number of failure mode for each component or item.

β = failure effect probability, these values are the conditional probability that the failure effect will result in the identified criticality classification, given that the failure mode occurs. The β values represent the level as to the conditional probability the loss will occur and should be quantified in general accordance with the following table:

Failure Effect	**β value**
Actual loss	1.00
Probable loss	>0.10 to <1.00
Possible loss	>0.00 to <0.10
No effect	0

α = Failure Mode Ratio, This number is the probability expressed as a decimal fraction that the component or item will fail in the identified mode. If all potential failure modes of a particular component or item are listed, the sum of the α values for that component or item will equal one.

λp = number of failures/10^6 hours as defined earlier.

t = Duration of the applicable experiment, usually express in hours.

5.8.2.1 Critical Analysis Table

ID #	ITEM (component)	Function	Failure Mode ID#	Severity	Failure Effect Probability (β)	Failure Mode Ratio (α)	Failure Rate (λp)	Operating Time (t, hours)	Failure Mode Criticality (Cm)	Item Criticality (Cr)	Remarks
1	ADA4927	Amplifier	1.2	IV. Minor	0.1	0.5	0.039	131400 (15 years)	256.23	512.46	
			1.3	IV. Minor	0.1	0.5			256.23		
2	Discrete SMD	Filter	1.4	IV. Minor	0.1	1	0.720		9460.80	9460.80	
3	SMA socket conn.	I/O connection	1.1	IV. Minor	0.1	0.7	0.011		101.18	144.54	
			5.2	IV. Minor	0.1	0.3			43.36		
4	AD9628	FADC	2.1	IV. Minor	0.5	01	0.065		4270.50	4270.50	
5	ZINQ 7020	FPGA	3.3	II Critical	0.5	0.1	0.530		3482.10	34821.00	
			3.9	II Critical	0.5	0.1			3482.10		
			3.11	II Critical	0.5	0.1			3482.10		
			5.3	II Critical	0.5	0.1			3482.10		
			6.2	II Critical	0.5	0.1			3482.10		
			6.5	II Critical	0.5	0.1			3482.10		
			6.8	II Critical	0.5	0.1			3482.10		
			6.11	II Critical	0.5	0.1			3482.10		
			6.14	II Critical	0.5	0.1			3482.10		
			6.17	II Critical	0.5	0.1			3482.10		
6	MT42L128M32D	Memories	3.4	II Critical	0.5	1	0.140		9198.00	9198.00	
7	N25Q00AA13GSF40	Memories	3.4	II Critical	0.5	1	0.071		4664.70	4664.70	
8	M12M I-Lotus	GPS board	3.12	III. Marginal	0.5	0.5	0.030		985.50	1971.00	
			5.5	III. Marginal	0.5	0.5			985.50		
9	T2000 Motorola	GPS Antenna	3.14	III. Marginal	0.1	0.5	0.011		72.27	144.54	
			5.5	III. Marginal	0.1	0.5			72.27		
10	N Socket Conn	Antenna conn.	3.13	III. Marginal	0.1	0.5	0.011		72.27	144.54	
			5.5	III. Marginal	0.1	0.5			72.27		
11	MPS430F2618	Micro controller	4.1	II Critical	0.3	0.5	0.490		9657.90	19315.80	
			4.10	II Critical	0.3	0.5			9657.90		
12	ADG608	Multiplexor	4.5	III. Marginal	0.5	0.5	0.066		2168.10	4336.20	
			4.8	II Critical	0.5	0.5			2168.10		
13	LTC2637	DAC	4.8	II Critical	0.3	1	0.066		2601.72	2601.72	
14	BMP085	Pressure sensor	4.4	III. Marginal	0.1	1	0.020		262.80	262.80	
15	LM224D	Amplifier	5.1-5.7	IV. Minor	0.5	1	0.039		2562.30	2562.30	
16	AD5316	DAC	5.1-5.7	IV. Minor	0.5	1	0.066		4336.20	4336.20	
17	MMBT3904LT1	Transistor	5.1-5.7	IV. Minor	0.3	1	0.160		6307.20	6307.20	
18	Marvell 88E1518	ETH Interface	6.1	IV. Minor	0.7	1	0.080		7358.40	7358.40	
19	USB 3320	USB OTG Interface	6.4	IV. Minor	0.7	1	0.080		7358.40	7358.40	
20	FTDIFT32232R	USB Interface	6.7	IV. Minor	0.7	0.5	0.080		3679.20	7358.40	
			6.10	IV. Minor	0.7	0.5			3679.20		
21	MAX3218	Serial interface	6.13	IV. Minor	0.7	1	0.080		7358.40	7358.40	
22	74AVCH8T245	Buffers drivers	6.16	IV. Minor	0.7	1	0.080		7358.40	7358.40	
23	LM3150	DC/DC converter	7.1	III. Marginal	0.5	0.25	0.065	131400	533.81	2135.25	

ID #	ITEM (component)	Function	Failure Mode ID#	Severity	Failure Effect Probability (β)	Failure Mode Ratio (α)	Failure Rate (λp)	Operating Time (t, hours)	Failure Mode Criticality (Cm)	Item Criticality (Cr)	Remarks
			7.3	II Critical	0.5	0.25		(15 years)	533.81		
			7.5	III. Marginal	0.5	0.25			533.81		
			7.7	II Critical	0.5	0.25			533.81		
24	LTC1174	DC/DC converter	**7.1**	III. Marginal	0.5	1	0.035		2299.50	2299.50	
25	TPS62125	DC/DC converter	**7.1**	III. Marginal	0.5	0.333	0.065		1422.08	4266.23	
			7.3	II Critical	0.5	0.333			1422.08		
			7.7	II Critical	0.5	0.333			1422.08		
26	TPS54020	DC/DC converter	**7.3**	II Critical	0.5	1	0.065		4270.50	4270.50	
27	LMR24220	DC/DC converter	**7.3**	II Critical	0.5	0.333	0.065		1422.08	4266.23	
			7.9	IV. Minor	0.5	0.333			1422.08		
			7.11	III. Marginal	0.5	0.333			1422.08		
28	TPS40170	DC/DC converter	**7.3**	II Critical	0.5	1	0.065		4270.50	4270.50	
29	BSS138P	FET Switch	**7.3**	II Critical	0.5	0.5	0.160		5256.00	10512.00	
			7.5	III. Marginal	0.5	0.5			5256.00		
30	BC846B	Transistor	**7.13**	IV. Minor	0.3	1	0.160		6307.20	6307.20	
31	FDN358P	FET Switch	**7.13**	IV. Minor	0.3	1	0.160		6307.20	6307.20	
32	? FUSE	Resettable fuse	**7.13**	IV. Minor	0.3	1	0.56		22075.20	22075.20	

5.8.3 *Criticality Matrix*

The criticality matrix provides a way to identify the most critical components regarding the number of failure mode versus the severity level.

Part Reference	Part ID #	Part Criticality (Cr)	Number of Failure Mode			
ZINQ 7020	5	34821.00			10	
? FUSE	32	22075.20	1			
MPS430F2618	11	19315.80			2	
BSS138P	29	10512.00		1	1	
Discrete SMD	2	9460.80	1			
MT42L128M32D	6	9198.00			1	
Marvell 88E1518	18	7358.40	1			
USB 3320	19	7358.40	1			
FTDIFT32232R	20	7358.40	2			
MAX3218	21	7358.40	1			
74AVCH8T245	22	7358.40	1			
MMBT3904LT1	17	6307.20	2			
BC846B	30	6307.20	1			
FDN358P	31	6307.20	1			
N25Q00AA13GSF40	7	4664.70			1	
ADG608	12	4336.20		1	1	
AD5316	16	4336.20	2			
AD9628	4	4270.50	1			
LM3150	23	4270.50		2	2	
TPS54020	26	4270.50			1	
TPS40170	28	4270.50			1	
TPS62125	25	4266.23		1	2	
LMR24220	27	4266.23	1	1	1	
LTC2637	13	2601.72			1	
LM224D	15	2562.30	2			
LTC1174	24	2299.50		1		
M12M I-Lotus	8	1971.00		2		
ADA4927	1	512.46	2			
BMP085	14	262.80		1		
T2000 Motorola	9	144.54		2		
N Socket Conn	10	144.54		2		
SMA socket conn.	3	144.54	2			
			IV	III	II	I
			Increasing level of Severity →			

Increasing level of Item Criticality →

5.9 *Critical Analysis conclusions*

The Critical Matrix indicates the most critical components producing the most sever effect on their failure modes. Those components are typically the FPGA, micro controller and the DC/DC converter. A redundant design for these components cannot be considered but some mitigation solutions must be implemented in the design to reduce the effects of the most critical components, see below:

- Separate power supplies between FPGA and micro controller
- Do not provide voltage to all DC/DC with only one DC/DC converter avoiding to create a single point failure (SPF) on the power supply unit
- Implement internal voltage and current monitoring, in addition to an internal failure detection, isolation and recovery (FDIR) mechanism performed by the Slow Control micro controller (WP7).
- Implement DC/DC protections and technics to improve their reliability.
- Use secure mechanisms in the S/W to read and write memories to be able to detect memory failure.
- Use gold plated connectors and keep a high level on cleanliness.
- Use high reliability cabling and soldering process to avoid bad connections and contacts.
- Use inverted logic for on board switches (normal state in open circuit)

All these solution are included as requirements in the specification list for the UUB design. The next chapter describes the FDIR mechanism to be implemented in the Slow Control unit.

6. FAILURE DETECTION, ISOLATION AND RECOVERY (FDIR)

6.1 *Introduction*

The FDIR mechanisms reported here consider the actions performed by the Slow Control unit for some failure mode on the power supplies inside the UUB system.

The following information shall be considered for each failure mode:
- Symptoms triggering the software actions.
- Actions of the software (failure isolation and recovery)
- Effect of the software actions on the system functionality (SDE).

6.1.1 *Philosophy*

The Fault Detection Isolation and Recovery (FDIR) system implemented in the SDE UUB Slow Control unit must permit the system to respond automatically in case of failures detected in respect of the following philosophy:
- Keep the system in a safety state for itself and the detectors connected to it.
- Record all the needed information on the system, allowing the users to take the best decision for maintenance action, in case of failure.

6.2 *Software Action on Failures (SDE UUB internal FDIR)*

All the failure described here will trigger action only from the Slow Control, Unit.

ID#	Failure Mode	Detection Method	Symptom Trigger	Isolation	Recovery	Slow Control Actions
1	FPGA S/W failure a loading	An acknowledge message is send by the FPGA to signal a good S/W loading	No acknowledge message received	**Yes**	**Yes**	- Load a mirrored version of the S/W sited in in another part of the memory - Write a message in the non-volatile Slow Control memory
2	FPGA core voltage failure	The core voltage is monitored every second	The core voltage is below 0.9 Volts	**Yes**	**No**	- Shut down all the FPGA power supplies in a delay below one second - Write a message in the non-volatile Slow Control memory
3	Symmetric voltage failure	The symmetric power supply is monitored every second	One of the polarity voltage values of the symmetric power supply is different with more than 10 % of the other, regardless of the polarity.	**Yes**	**No**	- Shut down the symmetric power supply in a delay below one second - Write a message in the non-volatile Slow Control memory
4	External 24V failure	The voltage and the current on the +24V provided on the 2 extension connectors are monitored every second	- The voltage value after the switch is below 17 Volts - The current value on each line is over 100 mA per line	**Yes**	**No**	- Shut down the considered +24V line on the extension connector - Write a message in the non-volatile Slow Control memory - Send an alarm on the telemetry for the monitoring S/W (TBC)

End of document