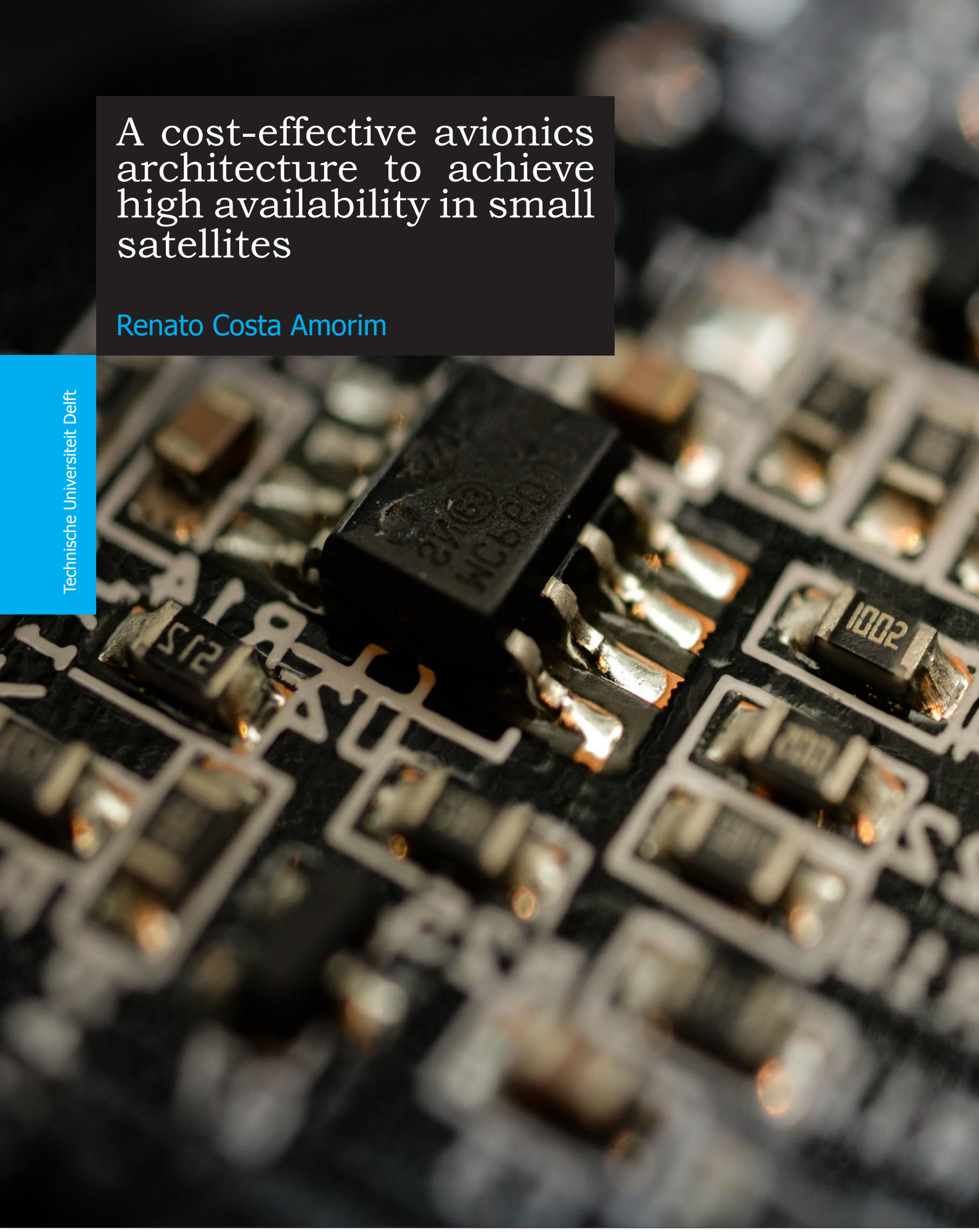
A cost-effective avionics architecture to achieve high availability in small satellites

Renato Costa Amorim

Technische Universiteit Delft



TU Delft Delft University of Technology

Challenge the future

1

[1]Cover image credits: Skitterphoto

A cost-effective avionics architecture to achieve high availability in small satellites

by

Renato Costa Amorim

in partial fulfillment of the requirements for the degree of

Master of Science
in Aerospace Engineering

at the Delft University of Technology,
to be defended publicly on Friday, October 18, 2019 at 10:00

Student number:	4728041	
Project duration:	February 4 , 2019 – October 18, 2019	
Supervisor:	Dr. A. Menicucci,	TU Delft
Thesis committee:	Prof. Dr. E. K. A. Gill,	TU Delft, chairman
	Dr. A. Menicucci,	TU Delft, supervisor
	Ir. C. de Wagter,	TU Delft
	Ir. R. Martins,	Evoleo Technologies, CEO

This thesis is confidential and cannot be made public until October 18, 2021.

TU Delft Delft University of Technology

EVOLEO TECHNOLOGIES *We evolve for you...*

'In general,
the greater the understanding, the greater the delusion;
the more intelligent, the less sane.'

- George Orwell, *1984*

Preface

Six years have passed since I first set foot in an university lecture. During this time I met amazing people, did things I never expected to do, changed countries numerous times and made it through the end. I am extremely proud to present the reader my MSc thesis report in the field of avionics systems for small satellites.

I had the goal to graduate from TU Delft since the beginning of my bachelors degree. I wanted to learn more about space and feel like I could contribute to a new world. TU Delft represented that. So, I kept pursuing that goal and when I finally arrived at campus it was one of the best days of my life. I learned so much during this period, met incredible people from all around the world, never doubting my decision. As the last days as a university student approach, I want to thank the people that made this accomplishment a reality.

First of all, I want to thank the people that guided me during this project. To my daily supervisor, Dr. Alessandra Menicuci, for always being ready with a variety of interesting thesis subjects and activities that would meet my interests. I am really grateful for helping me with the opportunity to perform my research at Evoleo Technologies. I would also like to thank all the people at Evoleo Technologies, in particular my external supervisor. Mr. Rodolfo Martins, CEO, for believing that I would be able to contribute to the development of small satellites and Pedro Ribeiro, for his good advice and guidance. Additionally to all TU Delft staff, some of the most motivated and knowledgeable people I have met.

An immense thank you to all my family, in particular my parents which offered me the opportunity to follow higher studies. Thank you for always supporting my outlandish plans and interests, giving me confidence to achieve them. We are nothing without our parents even when they don't exactly understand what you want to study.

To Maria, for your incredible support whilst preparing my application to TU Delft. I am eternally grateful for the way you were always positive, patient and caring despite my anxiety and difficult personality. I wouldn't be a TU Delft student if it weren't for you.

To my friends at Instituto Superior Técnico which made it so easy to move out of my parent's house. To René, Luís, Canas, Coelho, Negrinho, André and others: our memories working at the lab or roaming Lisbon at night will always be with me. You are some of the funniest aerospace engineers in world.

The good memories I take from TU Delft are the result of the time spent with Gilles, Thomas, Tiberiu, Patrick, Jaime, Steph and others. What a diverse group of young men that are ready to take on the world. Keep this motivation and I am sure we can change the world.

Some friends are for life and these I am sure are. Zé, Carriço, Gudes, Marco, Rita, we know each other since high school. We lived continents apart, shared the same apartment but most of all, we share our experiences, good or bad with each other. I have learned a lot with you all, making me the person I am today.

Renato Costa Amorim
Delft, October 2019

Executive Summary

The small satellite market is expanding mostly due to Earth observation (EO) constellations that plan to launch hundreds of similar satellites at significant lower costs compared to traditional platforms. Mini-satellites, or CubeSats, have shown the ability of commercial-off-the-shelf (COTS) electronics to work in space, despite lower reliability than space-qualified components. There is an interest from the space industry to utilize these commercial electronics due to improved performance and up to 1000 times lower component costs. However, it is necessary that avionics systems based on COTS components do not compromise mission reliability and availability figures.

The purpose of this report is to support the development of EO small satellites constellations (50kg to 200kg) by designing a cost-effective baseline avionics architecture that maximizes availability and reduces recurrent engineering and integration efforts. It shall understand the requirements for a system targeted at this market segment. The report shall also deliver a feasible baseline design that can be further developed into a flight system using current technologies.

The report starts by determining common functional and non-functional requirements of EO satellites in the 50kg to 200kg range. A baseline concept is developed into functional and physical architectures based on these requirements. Radiation analysis comparing candidate COTS and space-qualified technologies supports their concurrent utilization. Calculated event rates due to ionizing radiation are utilized to determine system availability figures for three reference low Earth orbits (400km to 1200km). System design and specifications are verified against requirements.

It is proposed that telemetry and telecommand coding/decoding at data link layer (TM/TC), command and data handling, input/output management (I/O), payload interface with data processing and storage and attitude control functions are similar for all platforms and can be implemented on a generic system. Target application are five year missions in low-Earth orbits at 400km to 1200km altitude and low to high inclinations. Separation of TM/TC, essential I/Os and reconfiguration functions into a dedicated supervisor unit based on space-qualified components enables additional functions to be implemented in two COTS-based units. The high reliability of the supervisor ensures minimal functionality and constant control of the spacecraft via ground link. Fault masking features and a two-stage boot process managed by the supervisor unit are designed.

Radiation analysis results suggest that destructive events are unlikely. Mitigable micro-latchups on the Zynq COTS system-on-a-chip (SoC), the most sensitive device, are to be expected. Lowest mean time between events is 200 days in solar maximum and highly inclined orbits. Other orbits and conditions were found to have orders of magnitude lower probability of destructive events occurring. Upsets in memories are correctable with adequate correction codes. Less than 9 hours downtime per year due to ionizing radiation effects, or more than 99.9% availability is estimated. Internal redundancy of COTS units has low impact on expected availability. The use of qualified components on the supervisor unit and storage of boot memory limits the overall system components cost to less than €100K in non-redundant configuration. Up to 10 times computational power improvement is possible by using the Zynq SoC compared to the LEON3FT GR712RC microcontroller. Configurable interface options are provided via custom design of PCB tracks. Single connectors with the possibility of internal cross-strapping via flexible backplane enables a redundant design option.

The research suggests that a highly-integrated avionics system could reduce recurrent design and component costs for small satellite constellations. Substantial performance improvements compared to qualified processing units are potentiated by the use of modern SoC. Flexibility in system configurations fulfill a variety of use-cases. COTS components, when supported by qualified components implementing essential functions, are thought to achieve high availability in spite of the harsh radiation environment. The proposed concept is found to be feasible for further development and validation at the prototype level.

List of Figures

1.1 Methodology employed in this thesis 4

2.1 Typical variation of cross section as a function of effective LET. Found in [1] 9

3.1 Functional units for SpaceMicro's Proton 2X Box. Credits: SpaceMicro 14
3.2 Basic operation of a LVDS circuit. Credits: Dave at ti 16
3.3 Dependability schemes. The left branches are related to fault tolerance whilst the right branches are related to fault avoidance. Since fault avoidance is against the paradigm surrounding this project, it will not be pursued at an high design level. 16

4.1 The number of operational satellites per mass category. Notice that the <150kg sector is largely populated. The 250kg to 300kg sector has a large increase in satellite number due to a Russian constellation of 42 military /commercial satellites. Derived from UCS satellite database [2]. 20
4.2 Orbital parameters as a function of satellite mass for currently operational 50kg to 200kg satellites. Derived from UCS satellite database [2] 21
4.3 Number of satellites per type of application for currently operational 50kg to 200kg satellites. Derived from UCS satellite database [2]. 21
4.4 The Skysat-3 from Planet's Skysat constellation. In the bottom of the image, an aperture cover that protects the imaging payload during launch is visible. Retrieved from space.skyrocket.de [3] 23
4.5 Lemur satellites in clean room (image credit: Spire Global) 24
4.6 The 2017 Flying Laptop mission, developed at the Institute of Space Systems (IRS) at the University of Stuttgart in Germany. Credits: IRS, University of Stuttgart. 24
4.7 Commercial EO constellations planned. (data from EuroConsult report: "Satellite-Based Earth Observation: Market Prospects to 2027" 25
4.8 Arrow platform from Airbus. Credits: Airbus DS 26
4.9 Three configurations for the SSTL-X50 platforms. From top to bottom: 22m GSD, 5m GSD, 0.7 GSD. Found in [4] 26
4.10 The InnoSat platform from OHB Sweden. The grey area is the satellite platform whilst the blue area is dedicated to the hosted payload. [5] 26

6.1 High Level Design Discovery Tree 36
6.2 **Concept A.1:** Example of a star topology architecture. Notice how each subsystem or component is individually connected to the SoC. Credits: Innovative FPGA 37
6.3 **Concept A.2:** In this example of a bus topology, there is a command data bus towards the communications and power subsystems. Credits: Intelligent Space Systems Laboratory at the University of Tokyo, Japan 37
6.4 Comparison between a conceptual artificial cell (bottom) and a biological cell (top). [6] 38
6.5 **Concept B.1:** Representation of an artificial cell composed of four proteins used on the 3U SME-SAT as an ADCS controller connected to an array of individual components. Credits: Surrey Space Center [7]. 38
6.6 **Concept B.2:** ExoMars SpaceWire Data-Handling Architecture composed of a central router that connects all instruments and camera to the processing units and mass memory [8]. 38
6.7 **Concept B.3:** ASNARO SpaceWire Data-Handling Architecture. A router connects all the platform electronics whilst a separate SpaceWire network connects the AOCS sensors and actuators to the AOCS computer [8]. 39

6.8 **Concept B.4:** Illustration of the main nodes of the TUBiX20 bus. Each node has its own processing power in the form of a μcontroller. Image credit: TU Berlin. 39
6.9 **Concept C.1:** Lunar Reconnaissance Orbiter data-handling architecture. In this architecture a router is used to connects the payloads to the command and data handling computer and to the communications systems [8]. 40
6.10 **Concept C.2:** BepiColombo Mercury magnetospheric orbiter data-handling architecture. "Each instrument is connected using a point-to-point link to the mission data processor, which contains two data-handling units, each of which contains a central processing unit and a SpaceWire router" [8]. 41
6.11 **Concept C.3:** System topology where a center router is used to link all units together in addition to a supervisor unit that provides SEFI detection and recovery amongst other functions [9]. 42
6.12 **Concept C.4:** A distributed architecture where a supervisor function is incorporated. The architecture of Cubesat KySat-2 seen in the figure applies this concept through a "heartbeat monitor" function [10]. 43
6.13 **Concept C.5:** BepiColombo Mercury polar orbiter data-handling. A shared memory unit is linked to 9 payloads and two downlink systems via 4 routers. Additionally, an OBC commands and supervises the operation of the payloads. [8]. 44
6.14 Pugh Matrix for high level concept trade-off. Notice that concept C.4 is the one with the highest score, followed by B.4, similar concept but without a supervisor. The highest contribution for the trade-off is in the form of the performance parameter, since it has a high weight and high score for this concept. 45
6.15 Proposed high level architecture. 46

7.1 Function flow of the control of AOCS peripherals. The circle with cross symbol in the diagrams represents a logical "OR". 48
7.2 Functional flow for telemetry data. 50
7.3 Functional flow for telecommands. 51
7.4 Functional flow of payload telemetry collection. 52
7.5 Functional flow diagram of payload control. 53
7.6 Functional flow diagram for the supervisor subsystem. 53
7.7 Interfaces between the proposed avionics system and other S/C peripherals. 54

8.1 SAVOIR functional architecture as seen in the SAVOIR Data Handling Handbook. 57
8.2 Functional architecture for Version 1 58
8.3 Functional architecture for Version 2 59
8.4 Functional architecture for Version 3 60

9.1 The trajectory of an high energy ion penetrating through the avionics at an angle. Notice that depending on the incidence location and angle, the ion will strike multiple PCB's as its energy is much larger than the stopping power of the silicon. Positioning the nominal systems as the outer boards minimizes the probability of multiple ion strikes in nominal systems and shieldings redundant systems. 64
9.2 Three types of legacy cross-strapping methods as seen in SAVOIR data handling handbook. 65
9.3 A variety of internal cross-strapping schemes. 65
9.4 Exploded view of redundant board crossstraped to the same output pins via a PCB with flexible sides. Courtesy of Evoleo Technologies. 66
9.5 Assembled view of redundant board crossstraped to the same output pins via a PCB with flexible sides. Courtesy of Evoleo Technologies. 67
9.6 Physical architecture for the OBC unit. Not to scale. Blue lines: digital data; green lines: control; yellow lines: power; red lines: analog; brown lines: time and sync. 67
9.7 Physical architecture of PLIU unit. Not to scale. Blue lines: digital data; green lines: control; yellow lines: power; red lines: analog; brown lines: time and sync. 69
9.8 Physical architecture of the supervisor unit. Not to scale. Blue lines: digital data; green lines: control; yellow lines: power; red lines: analog; brown lines: time and sync. . . . 70
9.9 Internal architecture of the Zynq-7000 series SoC. Courtesy: Xilinx 71

9.10 Architecture of the HPDP data processor. Obtained from [11] 71
9.11 Voltage allocation in SLC, MLC and TLC NAND flash technologies. 73
9.12 An example design to accommodate ISO15, ISO35 and ISO1042 transceivers from Texas Instruments which share the same SOIC-16 package. In theory this design principal can be use to prepare the PCB for whatever transceivers that share some of its pinouts. Note that the pin allocation on the SoC can be configured. The pinouts were obtained in the transceivers datasheets available in Texas Instruments website. NC: Not-connected . . 75
9.13 Example of NanoD connector with twist pins for termination on printed circuit board. Courtesy of Sunkye. 79

10.1 Failure propagation in cross-strapped systems due to over-voltage failure. Diagram by Sven Ladstrom as in [12]. 83
10.2 Example of a current sense implementation using multiplexing of currents. 85
10.3 Basic implementation of a watchdog timer. 85
10.4 Boot and configuration process of the designed architecture. 86

11.1 Total absorbed dose in Si (SRIM2008) at High LEO orbit in best case conditions. The target Si is modelled at the center of aluminum spheres for calculation purposes. Notice the contribution of trapped protons compared to other species. Generated with SPENVIS. 92
11.2 Total ionizing dose absorbed for all reference orbits and weather conditions. Notice the much higher dose for the High LEO orbit and the relative effect of shielding across orbits. The target silicon material is modelled at the center of aluminum spheres with 2.5mm and 5mm thicknesses. Calculated using the SHIELDOSE-2 model from SPENVIS. . . . 93
11.3 Shielded flux for SSO orbit in best-case conditions and 2.5mm Al-equivalent shielding. Notice iron knee market with red arrow. Calculated with SPENVIS' short-term SEU rate tool. 94
11.4 Shielded integral flux in worst case conditions. Notice that the points in the plot representing the following orbits are overlapping: SSO 5.0mm and High LEO 5.0mm. Also, SSO 2.5mm e High LEO 2.5mm are also overlaped. 95
11.5 Shielded integral flux in best case conditions. Notice that the points in the plot representing the following orbits are overlapping: SSO-5.0mm, High LEO-5.0mm, SSO-2.5mm and High LEO-2.5mm. 96
11.6 Expected latchup rates for the Zynq-7000 VccAux power input for the reference orbits, weather conditions and shielding thicknesses. 98
11.7 Results of the SET rate by direct ionization for a COTS (SN65HVD251) and a rad-hard (SN55HVD233-SP) CAN transceivers. Assumes a 2.5mm aluminum-equivalent shielding. Calculated with SPENVIS' short-term SEU rate tool. 99
11.8 Upset rates for the NAND flash memories assuming a 2.5mm aluminum-equivalent shielding. Notice the effect of the changing orbits and weather conditions for each device. It is also interesting to notice the consistently lower upset rate of the SLC memory compared to the MLC counterparts. Calculated with SPENVIS' short-term SEU rate tool. 100
11.9 Results of the upset rates calculation for the Zynq internal memories assuming a 2.5mm aluminum-equivalent shielding. The OCM is shown to be less susceptible to upsets, with BRAM and CRAM presenting similar behaviours.Calculated with SPENVIS' short-term SEU rate tool. Columns from left to right: OCM, BRAM and CRAM. 101
11.10SEFI event rate comparison between SLC and MLC NAND flash. Assumes 2.5mm Al-equivalent shielding. Calculated using SPENVIS SEU rate tool. 102
11.11SEFI event rate comparison between SLC and MLC NAND flash. Assumes 5.0mm Al-equivalent shielding. Calculated using SPENVIS SEU rate tool. 102
11.12SEFI event rate for the Zynq-7000 SoC. 103

12.1 Reliability block diagram representative related to the system's availability. 109
12.2 Effect of warm redundant configuration in the systems availability compared to non-redundant configuration. Considers the use of SLC NAND flash. 111

List of Tables

2.1 Energy range of the main sources of radiation particles. As in [13]. 8

4.1 A selection of LEO small-sat constellations (non-exhaustive). These entries are thought to be representative off the industry and the needs of the sector in terms of technology. SSO: Sun-synchronous orbit. 22
4.2 Compilation of optical payloads for small satellites. 28

9.1 Specifications for a variety of NOR and EEPROM devices as seen in the manufacturers websites. Maximum TID values are under bias conditions. Endurance in number of write/erase cycles. ∆: No data 74
9.2 Assignment of Zynq pins in the OBC unit. 76
9.3 Assignment of Zynq pins in the PLIU. 76
9.4 Allocation of external interfaces to connectors. The connector ID is formed my amalgamation of the connector type (NanoD or MicroD) and number of pins with and identification the originating unit. 78
9.5 Configurations 1,2,3 consist of 3x 9 pin (2x SpaceWire + CAN + Analog) , 2x 15 pin (6UART) and 1x 25pin (Analogs). Configuration 4 pin allocation in table 9.4. Surface area of a 3U size A PCB is 16000 mm^2. 79

11.1 Details on the configuration of SPENVIS and its radiation models for best-case and worst-case space weather scenarios 91
11.2 Orbital parameters for the chosen reference orbits. Data collected from `heavens-above.com`, 05/07/2019 at 08:45 ECT. 92
11.3 Categories of radiation tolerance according to TID, SEE and SEL behaviour, as suggested by Furano et al [14]. The iron knee is the three decade drop in radiation integral flux usually between from 25 to 35 MeV.cm2 mg. 95
11.4 TID before appearance of faults for a selection of COTS and space qualified components. Although not found in literature, it is expected that the MT29F128 (MLC) has similar to better TID tolerance than the other Micron memories since it is built with a smaller feature size. Values for 3DFN from 3D Plus website (3d-plus.com) consulted in 25th July 2019. 96
11.5 Threshold LET for SEL for a selection of COTS and space qualified components.Although not found in literature, it is expected that the MT29F18 (MLC) has similar latchup behaviour as the other MT29F memories. *: micro-latchup with steps of approximately 0.1A recovered only by power cycle. 97
11.6 Device and Weibull parameters for the heavy ion exposure of a COTS (SN65HVD251) and a rad-hard (SN55HVD233-SP) CAN transceivers. The calculation assumes as a sensitive volume a rectangular parallelepiped of sides **L** by **L** and thickness **t**. The sides of the parallelepipeds are obtained from saturation cross sections. The thicknesses are assumed equal for both devices at 2 μm [15]. ∆: Data points used instead of Weibull parameters. 98
11.7 Device and Weibull SEU parameters for a selection of memories. The calculation assumes as a sensitive volume a rectangular parallelepiped of sides **L** by **L** and thickness **t**. The sides of the parallelepipeds are obtained from saturation cross sections and the thicknesses from the cited sources. ∆: Data points used instead of Weibull parameters. 100
11.8 Device and Weibull SEFI parameters for two SLC and MLC NAND flash devices. Notice the higher cross section of the MLC Flash. 101
11.9 Saturation cross section and threshold LET for SEFI on the Zynq-7020 SoC. 103

11.10Validation of SEU rate in best case conditions calculations for NAND flash memories. The ISS orbit considered in the reference sources is at 500km altitude and 56.4º inclination. Proba orbit at 98.3º inclination and 715km to 735km altitude. Both reference orbits consider 100 mils Al-equivalent shielding (2.54 mm). AP-8 min model with Creme96. . 104
11.11Validation of the SEU rates for Zynq's CRAM and BRAM at the ISS orbit. The reference source considers a ISS orbit of 400km altitude and 51,6º inclination. Reference considers 100 mils Al-equivalent shielding (2.54 mm). No information on the models used to model solar minimum conditions or calculate upset rates. No information on assumed sensitive thickness. 104

12.1 Configuration parameters 108
12.2 Non-redundant and warm-redundant MTTR for zynq SEFI and SEL. 109
12.3 Calculated availability for a non-redundant configuration using SLC NAND. 110
12.4 Minimum availability due to each fault mode in non redundant configuration. 111
12.5 Footprint comparison between COTS and space-qualified components. 112
12.6 ROM cost for main components of OBC unit. Non-exhaustive list. ∆: COTS. †: QML V. . 113
12.7 ROM cost for main components of PLIU unit. Notice the cost of the data-engine. Non-exhaustive list. ∆: COTS. †: QML V 114
12.8 ROM cost for main components of Supervisor unit. Xilinx Virtex-4QV part number XQR4VSX55-10CN1140V. Non-exhaustive list. ∆: COTS. †: QML V 114
12.9 Overall ROM component cost of proposed avionics. 115

13.1 Unverified system requirements. Relates to annex C.3. 118

A.1 Information in this table consists of information explicitly available from supplier's brochures and website and therefore might not fully represent the system's capabilities and specifications. 128
A.2 COTS AOCS peripherals and their specifications. For the peripherals were multiple factory configurations are available, "or" is used in the specification. ∆: Not applicable; †: Not found 130
A.4 Compilation of AOCS subsystem specifications of a selection of mission. The S/C were selected as representative of the reference mission on a basis of mass range, mission objective and use of a commercial satellite bus. Information retrieved from `eoportal.org`. ∆: Not applicable; †: Not found. 131
A.6 Single Core. EAR restriction applies for VA10820 and UT32. Prices for ceramic packages versions. Prices obtained from mouser.com or contact with supplier. TBD: to be determined132
A.8 Prices obtained from mouser.com or contact with supplier. Zynq Ultrascale part is XCZU9CG-2FFVB1156I. Zynq-7020 part is XC7Z020-CLG484. TBD: to be determined 133

C.1 High level functional requirements. The methodology for creating the requirements ID can be consulted in annex C. 141
C.2 High level non-functional requirements. The methodology for creating the requirements ID can be consulted in annex C. 142
C.3 System requirements related to AOCS functions. 145
C.4 System requirements related to TM/TC functions. TBD: to be determined 146
C.5 System requirements related to payload functions. 147
C.6 System requirements related to C&DH functions. TBD: to be determined 147
C.7 System requirements related to supervisor functions. TBD: to be determined 148
C.8 System non-functional requirements. 150

Nomenclature

Acronyms

ADS-B	Automatic dependent surveillance-broadcast
AI	Artificial intelligence
AIS	Automatic Identification System
ALU	Arithmetic logic units
AOCS	Attitude and orbital control systems
CLCW	Command link control words
COTS	Commercial-off-the-shelf
DMIPS	Dhrystone Millions of instructions per second
DSP	Digital Signal Processor
ECC	Error correction codes
EGSE	Electrical ground support equipment
EO	Earth Observation
EOL	End-of-life
FMECA	Failure mode, effects, and criticality analysis
FPA	focal plane array
FPU	Floating point unit
FSBL	First stage boot loader
GCR	Galactic cosmic rays
I/O	Input/Output
IC	Integrated circuit
ICD	Interface Control Document
IoT	Internet of Things
LEO	Low-Earth orbit
LVDS	Low voltage differential signal
MBU	Multiple bit upset
MCU	Microcontroller Unit
MEO	Medium Earth orbit
MIO	Multiplexed I/Os
NIR	Near-infrared

PCU	Power Conversion and Distribution Unit
PLIU	Payload Interface Unit
PM	processor messages
PPS	Pulse Per Second
PSDU	Power Supply and Distribution Unit
ROM	Rough order of magnitude
RTOS	Real-time operating system
SBU	Single bit upset
SoC	System on a chip
SPOF	Single point of failure
SpW	SpaceWire
SSBL	Second stage boot loader
SWaP-C	Size, weight, power and cost
TRL	Technology readiness level
UCS	Union of Concerned Scientists
VLIW	Very Long Instruction Word

Units

A	Ampere
cm	Centimeter
eV	Electron volt
g	Gram
Gy	Gray
J	Joule
KeV	Kilo electron volt
kg	Kilogram
km	Kilometer
Krad	kilorad
MeV	Mega electron volt
mg	Milligram
min	Minute
mm	Millimeter
n	Nuclei
rad	Rad
s	Second

sr	Steradian

Physics Constants

eV	$1.60217646 \times 10^{-19} J$
rad	$0.001 J/kg$

Contents

Preface iii

Executive Summary v

List of Figures vii

List of Tables xi

Nomenclature xiii

1 Introduction 1
- 1.1 Motivation . . . 1
- 1.2 Research objective . . . 2
- 1.3 Research questions . . . 3
- 1.4 Methodology . . . 3
- 1.5 Document structure . . . 5

2 Space Radiation Environment and Effects 7
- 2.1 The radiation environment . . . 7
- 2.2 Radiation effects on micro-electronics . . . 8
  - 2.2.1 Cumulative effects . . . 8
  - 2.2.2 Single event effects . . . 9
- 2.3 Reduction in availability . . . 10
- 2.4 Conclusions . . . 11

3 State-of-the-Art in Avionics 13
- 3.1 Functions . . . 13
- 3.2 Physical Architecture . . . 13
  - 3.2.1 Single Board Computers . . . 14
  - 3.2.2 Modular . . . 14
- 3.3 Processors . . . 14
- 3.4 Interfaces . . . 15
- 3.5 Risk mitigation strategies . . . 16
- 3.6 Conclusions . . . 17

4 Reference Missions 19
- 4.1 Historical perspective . . . 19
- 4.2 Mission types . . . 20
  - 4.2.1 Constellations . . . 21
  - 4.2.2 Technology demonstration . . . 23
  - 4.2.3 Science . . . 24
  - 4.2.4 Growth forecasts . . . 25
- 4.3 Spacecraft platforms . . . 25
  - 4.3.1 InnoSat by ÅAC Microtec . . . 26
  - 4.3.2 SSTL-X Series by Surrey Satellite Technology . . . 26
  - 4.3.3 Arrow by Airbus DS . . . 26
- 4.4 Payload analysis . . . 26
  - 4.4.1 Optical . . . 27
  - 4.4.2 Radar . . . 27
- 4.5 Conclusions . . . 28

5 High Level Requirements **31**
5.1 Functional requirements . . . 31
5.2 Non-functional requirements . . . 32
5.3 Key, killer & driving requirements . . . 32
5.4 Requirement verification . . . 32
5.5 Conclusions . . . 33

6 Concepts **35**
6.1 High level design option tree . . . 35
6.1.1 Centralized . . . 36
6.1.2 Distributed . . . 36
6.1.3 Hybrid . . . 39
6.2 Concepts trade-off . . . 41
6.2.1 Trade-off parameters . . . 41
6.2.2 Concept analysis . . . 42
6.2.3 Pugh matrix . . . 44
6.3 Proposed high level concept . . . 45
6.4 Conclusions . . . 45

7 System requirements **47**
7.1 AOCS . . . 47
7.2 TM/TC . . . 49
7.3 Payload interface . . . 49
7.4 C&DH . . . 50
7.5 Supervisor . . . 50
7.6 Non-functional . . . 50
7.7 Requirement analysis . . . 50
7.8 Requirement verification . . . 52
7.9 Conclusions . . . 52

8 Functional Architecture **55**
8.1 SAVOIR reference architecture . . . 55
8.1.1 Functional blocks . . . 55
8.1.2 SAVOIR functional architecture . . . 56
8.2 Proposed functional architecture . . . 56
8.2.1 Possible configurations . . . 57
8.3 Discussion . . . 60
8.4 Conclusions . . . 61

9 Physical Architecture **63**
9.1 Methodology . . . 63
9.2 Overview . . . 64
9.2.1 OBC . . . 66
9.2.2 PLIU . . . 68
9.2.3 Supervisor . . . 68
9.3 Processing units . . . 68
9.3.1 SoC . . . 69
9.3.2 Data processor . . . 69
9.3.3 Supervisor FPGA . . . 71
9.4 Memories . . . 72
9.4.1 Volatile . . . 72
9.4.2 Non-volatile . . . 72
9.5 Transceivers . . . 74
9.6 Interfaces . . . 75
9.6.1 Internal interfaces . . . 75
9.6.2 External interfaces . . . 78
9.7 Review of design and conclusions . . . 79

10 Protection Systems **81**
10.1 Fault masking . . . 81
10.1.1 Latch-up current limiter . . . 81
10.1.2 Galvanic isolation . . . 82
10.1.3 Fail-safe transceivers . . . 82
10.1.4 ECC . . . 83
10.1.5 Scrubbing . . . 84
10.2 Reconfiguration . . . 84
10.2.1 Functional monitoring . . . 84
10.2.2 Watchdog timer . . . 85
10.2.3 Boot and configuration process . . . 86
10.3 Conclusions . . . 87

11 Radiation Effects Analysis **89**
11.1 Radiation environment modelling . . . 89
11.1.1 SPENVIS . . . 89
11.1.2 Space weather scenarios . . . 89
11.1.3 Shielding . . . 90
11.1.4 Reference orbits . . . 90
11.1.5 Limitations of the analysis . . . 91
11.2 Comparison of radiation environments . . . 93
11.2.1 Total ionizing dose . . . 93
11.2.2 Shielded flux . . . 93
11.3 Radiation hardness assurance . . . 95
11.3.1 Total ionizing dose . . . 96
11.3.2 Single event latchup . . . 96
11.3.3 Single event transients . . . 97
11.3.4 Single event upsets . . . 99
11.3.5 Single event functional interrupt . . . 101
11.4 Validation . . . 103
11.5 Discussion . . . 104
11.6 Conclusions . . . 105

12 System Specifications **107**
12.1 Configurations . . . 107
12.2 Availability . . . 108
12.2.1 Methodology . . . 108
12.2.2 Sources of reduced availability . . . 109
12.2.3 System predicted availability . . . 110
12.3 SWaP-C . . . 112
12.3.1 Size . . . 112
12.3.2 Weight . . . 112
12.3.3 Power . . . 112
12.3.4 Cost . . . 113
12.4 Performance . . . 115
12.5 Conclusions . . . 115

13 Verification and Validation **117**
13.1 Verification of requirements . . . 117
13.1.1 Functional requirements verification . . . 117
13.1.2 Non-functional requirements verification . . . 118
13.2 Validation of the design . . . 118
13.3 Conclusions . . . 119

14 Conclusions **121**
14.1 Key outcomes . . . 121
14.2 Fulfillment of research objective . . . 122
14.3 Answers to research questions . . . 123

15 Recommendations **125**

A COTS components **127**
A.1 Avionics 127
A.2 AOCS peripherals 128
A.3 Satellite platforms 131
A.4 Low-Performance processing units 132
A.5 High performance processing units 132

B Preliminary FMECA **135**

C Requirements **139**
C.1 Requirements Identifier 139
C.2 High-level requirements 140
C.2.1 Functional requirements 140
C.2.2 Non-functional requirements 141
C.3 System requirements 143
C.3.1 Functional requirements 143
C.3.2 Non-functional requirements 148

Bibliography **151**

1

Introduction

This document is a high level systems design and analysis of an avionics architecture targeted at small satellites. It is the result of TU Delft and Evoleo Technologies' shared interest to potentiate the use of cost-effective commercial-off-the-shelf (COTS) technologies in the space industry without compromising on dependability. The performed work builds upon the conclusions and recommendations of the previously performed literature study [16].

The thesis contains research into the small satellite market in order to better understand how a new avionics system could be beneficial. It selects a design concept which is further developed based on requirements. The effects of radiation are analysed for low Earth orbit (LEO) missions. Metrics such as availability and cost are presented which allow comparison with current avionics systems available in the market. The contents of this thesis lay the foundation to produce a detailed design and prototype system to validate the design features of the proposed architecture.

This chapter introduces the project, describing with greater detail the motivation behind it and resulting research goals and questions. The methodology employed, which follows the systems engineering approach, is described. The outline of the document is presented at the end of this chapter.

1.1. Motivation

Space is inherently fascinating and useful for humanity. It is a land of fantasy, planets, stars, black holes and possibly alien life-forms, representing the unknown and humanity's drive to explore it. It is also a strategic location to observe and learn about the universe, our planet and us. From orbit, one has a wide view of meteorological phenomena, Earth's fauna and flora and of every human being. It is therefore of great interest for all humanity to sustainability explore and make use of space and its resources.

The space industry is known for being extremely challenging and costly. It takes an immense amount of work to design, build, test and launch any spacecraft. Besides all the specialized labour, the components inside a satellite are also specialized. The harsh radiation environment in space would destroy most electronics developed for every day use. High energy protons, electrons and ions are constantly flowing from all directions, affecting not only electronics but also biological tissues. To ensure the reliability of these very expensive space missions, components for space applications are designed to consider these challenges, built using special technologies and thoroughly tested. Only then are these qualified for space applications. Components that survive the radiation environment are also known as rad-hard, or radiation-hardened. This methodology has been successfully employed for decades and is one of the reasons why most space missions are successful and spacecraft perform their functions well beyond their nominal lifetime.

Interest in reducing the full cost of space missions has lead to the CubeSat concept. First, launch costs are reduced since CubeSats weight only a few kilograms, usually less than 20kg. Second, they employ electronics used in every day applications such as smartphones or microwaves. Additionally, these everyday technologies, by forces of open commercial markets, offer better performance at significantly lower costs. Due to these and other factors, CubeSats are a less expensive alternative to larger, more traditional satellites.

Nevertheless, this new-space era is not without challenges. The reliability of these platform is generally lower than what is seen in 'old-space' with many CubeSat mission failing immediately after launch. Furthermore, the radiation effects in these commercial-of-the-shelf (COTS) electronics leads to unpredictable effects that cause the satellite to behave in unintended ways or even to completely fail. These effects reduce the time the spacecraft is available to perform its mission, called availability.

Growth in the 50kg to 200kg satellite market is drawing the attention of the space industry as a potential big source of revenue. This mass range is the target range for concepts involving dozens to hundreds of similar satellites that work together towards the same goal. Together, these so-called 'constellations' have uninterrupted view of the Earth, providing real-time observation or supporting global communication networks. To enable these constellations, cost-effective satellite platforms need to be built expediently. This includes the avionics systems which are the electronics that control the spacecraft, or its brains.

Naturally, the performance to cost ratio of COTS components, as compared to qualified space equivalents is drawing the attention of these ventures and the entire space industry. The struggle is in developing systems based on COTS parts that offer the same reliability, available and functionality as it is seen in 'old-space' applications. One can found avionics based on commercial components but their functionality and reliability levels are not on par with qualified alternatives. Other ideas incorporate both component types on the same electronics board but with functional limitations. In this context, the European Space Agency (ESA) has invited industry from its member states to answer this issue. In the form of an open invitation to tender (ITT), AO9815 "COTS-based highly integrated computer system for mini/nano satellites", ESA asks for a computer system for these satellites to be built, suggesting the implementation of a Zynq system-on-a-chip. The first use-case would be determination and control of a spacecraft orbital attitude.

In December 2018, contacts with Evoleo Technologies, a small to medium-sized enterprise (SME) created in 2007 in Porto, Portugal, were initiated. It lead to the collaboration for this thesis project. Evoleo has four main areas of activity: space, infrastructure, industry and technology. Its experience in the space industry is in the design of rad-hard on-board computers for missions such as AlphaSat, power distribution units (one on-board the international space station (ISS) on the ANITA air quality monitor) and electrical ground support equipment (EGSE) besides other projects. Its has know-how in dependable [1] electrical and electronic systems both at hardware and software levels. Evoleo is interested in entering the new-space paradigm and increase its competitiveness by developing an avionics system that can be re-utilized for multiple missions and built on short notice. By integration of a large number of functionalities in a single avionics system, a monolithic system is envisioned. Such system would substitute a variety of others and therefore reduce integration complexity. The use of adequate design features, ensures reliability and availability whilst COTS components lead to lower costs.

From February 2019 until September 2019, this thesis project was developed at Evoleo facilities in Porto, Portugal under constant supervision by Evoleo engineers in particular Mr. Rodolfo Martins, the company's CEO and MSc Electronics Engineer. Weekly contact with the supervisor from TU Delft, Dr. A. Menicucci provided extra guidance, ensuring the good progress and quality of this work.

1.2. Research objective

The thesis project will strive to produce a baseline avionics architecture that fulfills the aforementioned issues, contributing to the development of a next generation of smallsats. For that end, the state-of-the-art in spacecraft platforms, Earth observation payloads and sub-systems will be considered in order to generate requirements. Furthermore, a combination of commercial and space-grade components, along with fault protection methods will be analyzed, traded-off and incorporated into the design in order to achieve high availability at an effective cost. The radiation response of the main technology bricks will be characterized and event rates for representation orbital environments calculated. The achieved availability of the design will be calculated making use of these results. The final design is then compared to relatable system for size, weight, power, cost and availability.

The research objective can be distilled into the following statement:

Obj-1: To support the development of EO small satellites constellations (50kg to 200kg) by de-

[1] Dependability: reliability, availability, maintainability and safety. Also known as RAMS.

signing a cost-effective baseline avionics architecture that maximizes availability and reduces recurrent engineering and integration efforts.

1.3. Research questions

The review of literature and analysis of commercial markets together with the aforementioned research objective propels the idealization of research questions. Each of these questions provides a steering function, addressing a major issue in the design and characterization of an avionics architecture. By answering these questions, a meaningful design will be produced at the end of the thesis.

The first step in a new avionics design is to determine which functions the system must provide. Furthermore, it is necessary to create a design that facilitates spacecraft design and reduces integration efforts from the get-go. These two issues are the essential first steps and questions to address. As the research objective states, maximizing availability is another major goal of the thesis. It is paramount to investigate how this can be achieved whilst still maintaining the performance/cost ratio at a high level. This includes the development of adequate protection systems and the usage of COTS components. Finally, the system must be characterized in order to validate the design solution developed during the thesis work.

These key points are compiled in a set of research questions. From one to five, they lay out the most fundamental questions that need to be answered in an almost chronological fashion. Question four also includes three sub-questions that are useful to better answer the main question. Each of the following questions has a dedicated identifier (RQ) followed by a number. In the case of sub-questions, a number/letter combination is used.

- **RQ-1:** What functional units should an avionics architecture have in order to reduce recurrent engineering and integration efforts?
- **RQ-2:** How can a new avionics architecture contribute to reduce recurrent engineering and integration efforts?
- **RQ-3:** How can the design maximize system availability in a cost-effective way?

  RQ-3A: What protection systems are required to increase availability?

  RQ-3B: How can the combination of space-grade and commercial components be exploited to achieve high availability?

  RQ-3C: How does the combination of space-grade and commercial components affect overall cost?
- **RQ-4:** What are the expected performance and dependability figures for this architecture?

1.4. Methodology

Designing a complex system requires careful planning of work packages that follow a well established methodology. By following to a large extent, and until possible, the system engineering process and the V-model [17], it is expected that this thesis project will fulfill the proposed research objective and answer its questions successfully.

The thesis project begins with a background research into the small satellite market and avionics systems which builds upon the knowledge obtained in the literature review [16]. This enables the characterization of reference missions and payloads which are the target of the system to be designed. Also, understanding the current avionics system in the market provides better understanding of what are the technologies, capabilities or characteristics that could be beneficial for the future of the industry.

Following these activities, a list of high level system requirements is generated. Gathering and selecting a number of conceptual ideas, and comparing them to these requirements gives the first idea of the system's layout and functionality. The definition of lower level requirements is achieved after a better understanding of the reference S/C platforms and functions is achieved. At this stage, the most challenging requirements can already be pointed out.

After these requirements are set, the functional architecture is designed and analyzed. It shall fulfill the system's expected functionality and for that, the SAVOIR reference architecture is used as a

starting point. Functions and message types from SAVOIR are utilized to developed a new functional architecture in the form of a diagram.

Main technology bricks are gathered, compared and selected, in order to determine how COTS components can be employed. These include processing units, memories and transceivers. An iterative process designs the physical architecture whilst considering functional allocation and interface compatibility. With the physical architecture defined, a number of protection systems for fault masking and reconfiguration are selected and described.

Radiation environments and effects for reference missions are presented and discussed. Upset rates due to radiation effects are calculated using the SPENVIS tool for a variety of components and validated with available literature. This radiation analysis process is important as it concludes on the suitability, dangers and impacts of using commercial ICs in the avionics. Following these results, the availability of the system can also be calculated. It follows that the most significant culprits of availability reduction can be identified.

Along with the calculated system availability, other metrics such as size, weight, power, cost and performance are presented. Comparison with other avionics unit validate the concretization of the research goal. The verification of the design against requirements is the last step in this methodology.

Figure 1.1 presents a graphical representation of this methodology:

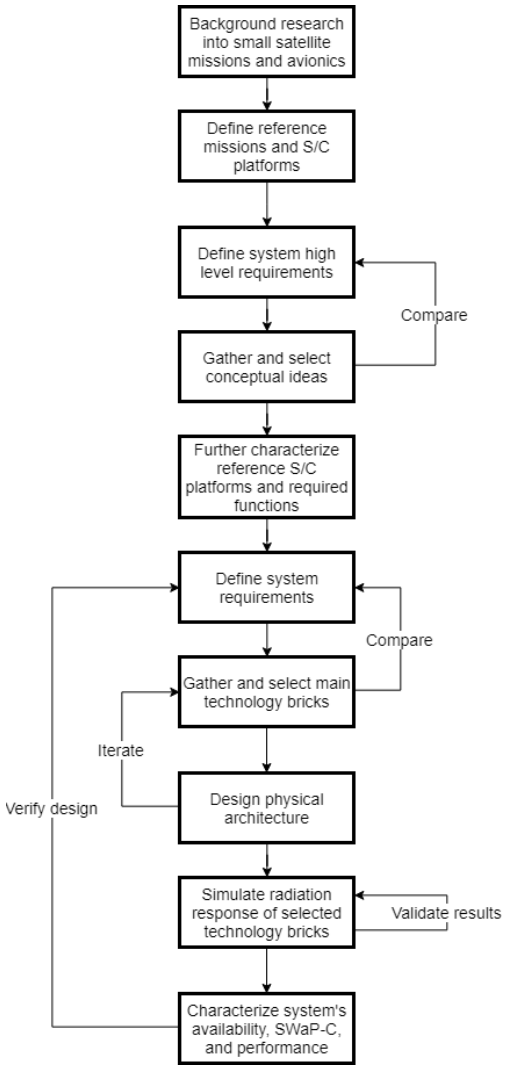


Figure 1.1: Methodology employed in this thesis

1.5. Document structure

This document is composed of 15 chapters and 3 appendixes. Each chapter is further composed of multiple sections and subsections for improved readability. A bibliography compiles the sources consulted to produce this work.

Chapter 1 is an introduction to the document and thesis work including research objective and questions. Chapter 2 provides background into the space radiation environment and its effects on electronic systems. To complement this background, Chapter 3 dwells on the state-of-the-art in avionics units for small satellites. The target missions for this project are found and characterized in chapter 4. This is used to generate high level requirements in chapter 5. The first concepts to fulfill the requirements are generated and traded-off in chapter 6. The understanding of the system to be designed is further elaborated with system requirements in chapter 7. The functional architecture is presented and discussed in chapter 8. Chapter 9 presents the proposed physical architecture and its main building blocks. In addition, chapter 10 presents the employed protection systems for fault tolerance and reconfiguration. Chapter 11 characterizes the radiation environment expected for the reference missions and calculates the event rates for some of its building blocks. The system is characterized in chapter 12 in terms of availability, size, weight, power, cost (SWaP-C) and performance. The achieved design is verified against requirements and validated in chapter 13. The project is reviewed and conclusions are taken in chapter 14 which also includes the answer to the research questions. Finnally, suggestions for future work are elaborated in chapter 15.

Appendix A contains a variety of COTS components that were considered during this project. It includes processing units and AOCS peripherals. Appendix B contains a preliminary FMECA analysis of the avionics. Finally, appendix C presents both high and system level requirements defined during this thesis project and their compliance.

2

Space Radiation Environment and Effects

Arguably the most important cause of avionics faults in space is the radiation environment. The bundle of energetic particles one encounters in orbit and beyond causes damage to avionics, from memory errors to malfunctions to complete failure. Previously, a literature study on this topic was performed which described with greater detail these issues [16]. In this chapter, a review of the most important aspects of radiation environment in space will support the development of this avionics system.

The chapter begins with an explanation of the radiation environment in terms of particles' energies and distribution. Following that, both cumulative as well as single event effects are described considering the physical mechanisms as well as its consequences. The chapter concludes with a reflection on how the aforementioned effects translate into a reduction of the availability of an avionics system.

2.1. The radiation environment

Outside of the Earth's atmosphere, energetic particles create a radiation environment which causes devastating effects on electronic and biological systems. Radiation takes the form of electrons, protons or heavy ions of multiple origins and energy levels. Either trapped in magnetic fields or travelling from the Sun or the galaxy, understanding this environment and the effects it has on systems is of major importance in any space mission [18].

The Sun produces high energy particles that are released into the Solar System in the form of solar wind and solar flares. Solar wind consists of a stream of charged particles which escape the Sun's gravity field, mostly electrons, protons and alpha particles. Sometimes, fast-moving burst of plasma (in the form of protons) are released from more active regions of the Sun's surface. Usually accompanying these events, sudden flashes of increased brightness also occur, named solar flares. In these events, high energy ions and electrons are emitted which strongly interact with the Earth's magnetic field, affecting its shape and behaviour [19].

For those particles released by the Sun, a percentage of them are captured by the magnetic field of the Earth and become trapped. In two torodial shaped belts, named Van Allen belts, electrons and protons are scattered in higher concentrations in an inner and outer belts. In the inner belts, located mostly at altitudes between 1000km and 6000km, high energy protons are present [20]. In the outer belt, extending from 13000km to 60000km, high energy electrons dominate. Due to the misalignment between the Earths magnetic field and rotation axis, in an area approximately over Brazil, the inner belt becomes as close as 200km to the Earth's surface, in the so called "South Atlantic Anomaly". In this region, low flying spacecraft are expected to encounter increased radiation [21].

Another contribution to the radiation environment in space are high energy particles external to the Solar system in their origin. These particles, known has galactic cosmic rays (GCR) , are thought to be originated from inside the Milky Way or even outside the galaxy. They are almost isotropic in nature. The most energetic particles that can hit a spacecraft are from these galactic cosmic rays, with energies above 1000MeV [22].

This wide range of energies and sources of radiation are compiled in table 2.1, where it can be seem that heavy ions from galactic cosmic rays are by far the most energetic particles.

Radiation belts	Electrons	eV - 10 MeV
	Protons	keV - 500 MeV
Solar flares	Protons	keV - 500 MeV
	Heavy ions	1 to a few 10 MeV/n
Galactic cosmic rays	Protons and heavy ions	Max flux at 300MeV/n

Table 2.1: Energy range of the main sources of radiation particles. As in [13].

2.2. Radiation effects on micro-electronics

The exposure of electronics to radiation can have both cumulative effects as well as effects due to a single ionizing particle. This radiation alters the behaviour of the electronics circuits by energy deposition which may degrade the perform of the device, increase its power consumption, produce faults and errors in its operation or even destroy the device. The study of the effects of radiation in integrated circuits is paramount in order to create a system that will perform its mission in space as expected [23].

A complete and detailed analysis of the radiation behaviour of the entire system as well as of individual components enables the creation of strategies used to cope with the effects of radiation, maintaining the reliability and availability of the spacecraft. Following the previously mentioned literature study, a synthesis of these issues is presented here.

2.2.1. Cumulative effects

The long-term energy deposition into a target device is referred to as cumulative effects. The gradual modification of its electrics characteristics is related not only to ionizing particles but also to non-ionizing particles, thus leading to two cases: ”total ionizing dose” and ”displacement damage” respectively [24].

Ionizing radiation interacts with the atoms of the target device to generate electron-hole pairs. The energy deposition is achieved either directly by the incoming charged particle or by secondary effects related to the sudden loss of energy of this particle. In the first case, a ionization track is created in the particle's path. In the second, the deceleration of the particle creates photons which are released as high energy X- or gamma-rays, now capable of creating an ionization path. This is called the Bremstrahlung effect, specially important when radiation shields are used, since the shielding material will be responsible for the creation of this secondary radiation [24].

The dominant cumulative effect is the shift of threshold/gate voltages in MOS devices and the creation of leakage paths. In the first case, the shift in voltage alters the behaviour of transistors and in the second case, increase power supply currents are expected as the radiation dose accumulates [24]. These effects are sensitive to the bias condition imposed on the device. Typically, unbiased (powered-off while exposed) devices are able to accumulated higher doses until failure, up to double the total dose [25].

The total absorbed dose is measure in Grays, defined as one Joule of energy absorbed per kilogram of matter. However, the *rad* is a more commonly used unit, defined as 0.01 Grays. To calculate the total absorbed dose, the following formula is applied [26]:

$$TID = F \times LET \times 1.6 \times 10^{-5} \tag{2.1}$$

where F is the particle fluence measured in the plane normal to the beam in $ions/cm^2$ and LET is expressed in $MeVcm^2/mg$.

The LET, or linear energy transfer is a measure of the energy transferred through ionization by a particle per unit length (equation 2.2) [26],

$$LET(x) = \frac{1}{\rho}\frac{dE}{dx}(x) \qquad \text{(units of } MeVcm^2/mg\text{)} \tag{2.2}$$

where ρ is the target density (mg/cm^3), E is the particle energy (MeV) and the x is the range (cm). The effective LET accounts for the angle of incidence of the ion beam according to an inverse cosine law. As the angle of incidence deviates from the normal of the plane of incidence, the path length of the ion through the sensitive volume (the volume sensitive to charge deposition) increases, therefore increasing the effective LET.

Testing for TID is usually performed at a laboratory by exposure to a radioactive source such as Cobalt-60 or X-rays. The device is exposed until certain accumulated dosages are achieved before being tested for performance, functionality and power consumption. The exposure is resumed up to another accumulated dose before the device is tested again. This process is prolonged until the device fails [27].

2.2.2. Single event effects

As opposed to cumulative effects, single events effects are a consequence of a single high-energy particle, as the name implies. This particle deposits large amounts of energy in a localized region of the circuit, therefore causing an instantaneous perturbation. Said perturbations can be permanent and non-recoverable (hard-errors) or recoverable (soft-errors). The deposited energy leads to charge collection in the device which causes unwanted current paths or induces unwanted currents [18].

As with total dose effects, the linear energy transfer is an important measurement of the device's sensitivity to radiation. The increase in LET is linked to the number of SEE observed. Above a certain threshold LET, SEE are noticed in a device. Additionally, the device cross-section (the number of events per particle fluence) can be compared in order to understand the device's response for particles of multiple energies [28]. It is common to determine the cross section vs LET curve as a standard means to compare the radiation hardness of devices. This curve, as seen in 2.1, shows that below a certain LET threshold no events are detected and the increase in the number of detected events stagnates when the cross section saturation line is reached.

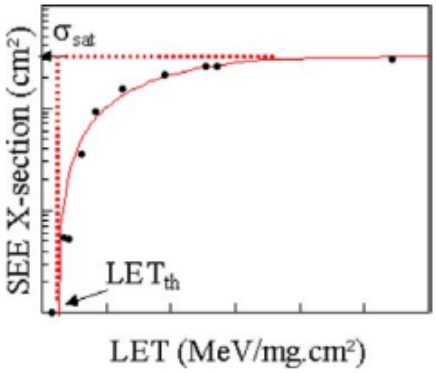


Figure 2.1: Typical variation of cross section as a function of effective LET. Found in [1]

Testing for SEE requires the usage of ion accelerators, which generate beams of heavy ions or protons that strike on the device. A mix of different ion species are used in order to vary the LET during experiment. Additionally, degraders, usually as copper plates, are placed between the ion source and the device under testing for the same end. In order to detect the consequences of radiation, dedicated test software and hardware is employed. By running the device under testing (DUT) whilst exposed to radiation, high current states, memory or functional errors can be detected by the test setup which provides engineers with an understanding of the systems' behaviour whilst in space [26].

The most relevant SEE on modern OBC are upsets (SEU), latchups (SEL), functional interrupts (SEFI) and transients (SET). These may lead to reduction in computing availability which, as stated in the introduction motivates the work of this thesis.

SEU

When a memory component is hit by an ionizing particle, storage data can be corrupted. In these cases, a single event upset happens due to the energy deposition of the particle inducing an excess restoring current on a memory's cross-coupled inverter. Depending on the particle's angle of incidence,

more than one memory bit can be affected at a single time. These cases are referred to as multiple bit upsets (MBU). The flipped bit can be corrected by rewriting, if error detection and correction codes are employed [18].

Single event upsets can occur in all memory cells, including those for mass storage, RAM or registers. The most susceptible technologies are SRAM and DRAM with Flash, MRAM, FERAM and CRAM presenting higher tolerance to SEU. [29].

SEL

Radiation can also originate high current states in transistors. In this cases, a low-impedance path is created between the input and the output nodes of the transistor and the high current state can only be eliminated once the power is removed. The timely detection and power removal in these situations is paramount, as the high current can eventually destroy the device. Another type of event has also been identified which consists of small increases in current, but not above the maximum specified. These events, name micro-latchups are usually observed as step-changes in power consumption. Consequences are notwithstanding nefarious with permanent damage being observed [30].

This susceptibility of devices for latchups is dependent on the underlying technology. Commercial devices usually have a low threshold for latchups. The previously performed literature study has revealed a large range in LET thresholds for SEL across the most popular micro-controllers for small satellites. Latch-ups were detected readily at even the lowest LET values for some devices while other commercial devices supported up to 86 $MeVcm^2/mg$ [16].

Nevertheless, manufacturing methods such as SOI (silicon on insulator) improve immunity at the expense of increased cost. Additionally, the decrease of supply voltages may also improve immunity due to the fact that thresholds voltages will soon fall below the voltage required to hold the latchup [9].

SEFI

Another effect of radiation is the temporary loss of device's functionality, leading to a SEFI (single-event functional interrupt). A high energy strike that causes an upset in control circuitry of memories and processors, corrupts the control data in registers and memories used for operation control. In these cases, consequences are unpredictable and range from the program being halted, destruction of normal program control flow, endless loops, self-resets and inability to operate peripherals. Again, only power cycle or reset of the device is able to restore functionality [9].

SET

Transient effects are, as the name suggests, those which are momentary in nature. A high energy particle able to deposit enough charge on a sensitive node leads to a voltage/current excursion affecting the normal operation of a device [31].

These types of events are most noticeable at output ports where negative or positive going signals are generated. The height and duration of these pulses are dependent on each device and the deposited energy. Transients are sensed by an input port at the other signal end as a certain logic value. The mismatch between intended and observed logic values are a source of errors in the communication link [32].

2.3. Reduction in availability

The aforementioned single event effects are, as expected, not desirable in the context of spacecraft flying high above the atmosphere or in deep space without constant human control. In these scenarios, the effects of radiation may cause the system to not perform the functions it was supposed to perform. If at a given instant or period of time, even though all required external resources are provided to the system, namely power and data, it does not perform its predefined function, the system is said to be unavailable [33]. The availability is an important attribute of a system and is increasingly important in the space domain. Spacecraft are expected to become more autonomous and require less human operation and ground contact. Faults shall be autonomously detected and recovered from and operations are expected to rely on clever computer vision and artificial intelligence [14].

Availability is a valuable feature in services such as telecommunications or global positioning. In these cases, availability is a measure of the percentage of time that the system is usable by a receiver, user or application. Satellite owners promise users a certain level of availability as part of their service

so it is an important driver in the design of a satellite constellations and its individual segments. Decision power is also affected by a satellite's availability as it is the case with defence applications where troops on the ground expect a satellite link to be available at all times. Communications, global positioning and surveillance based in satellite systems are used by defence organizations around the globe to acquire an edge over the enemy or foreign states. Earth observation also benefits with increased availability of satellites as natural events and catastrophes can be better dealt with when satellite data is reliable. If an Earth monitoring satellite is unavailable, important climate events such as hurricanes, floods, volcanic eruptions or tsunamis are not detected in due time, compromising rescue operations [34].

Autonomous fault detection isolation and recovery algorithms, in conjunction with hardware features, are indispensable for increased availability. Without these, spacecraft might be stuck in unwanted conditions until a radio link is establish and the fault can be corrected (if such a feature is provided by the avionics suite). In the meantime, the spacecraft is unavailable. Furthermore, onboard autonomy to deal with issues such as the ones originating from radiation exposure reduce the required human interact effort in order to solve problems, thus reducing operational cost and complexity [35].

Events such as latchups and functional interrupts are the major causes of reduced availability. Frequent actions which require halt of normal program flow to ensure system integrity are also considered to reduce availability. This includes self-checks or rewriting of memories suffering from SEU. All of these events are consequence of the chosen architecture and components. Hence, the understanding of SEE and handling of its consequences is indispensable if one targets a high availability system.

2.4. Conclusions

This chapter presented essential knowledge of the radiation environment in LEO and respective effects. It presented both cumulative as well as single event effects in their most important varieties. How a device's sensitivity to radiation is measured was also introduced. Finally, how these events affect the systems availability was discussed.

Radiation has both long term as well as single events effects. There is a multitude of SEE related to the sensitive volume it hits. It follows that the impact of radiation on the system is dependent on the radiation environment, the device in question and the mitigation techniques employed. Achieving high availability depends on a radiation hardness assurance process which considers all three aspects. Latchups, functional interrupts and upsets that require time-consuming recovery methods are the main sources of reduced availability.

Only a small introduction to the topic of radiation effects on micro-electronics was possible. This introduces the reader to the main issues so it is able to better understand the thesis context and the content of later chapters. For further knowledge on this topic, the reader is advised to read the previously performed literature study [16] and Schwank et al introduction to radiation hardness assurance [36].

3

State-of-the-Art in Avionics

In this chapter, the current state-of-the-art in relevant avionics systems is given, aided by means of a compilation of COTS avionic systems available in annex A.1. It focuses on five main aspects of the systems: 1) What functions do these systems perform; 2) what is the physical architecture of the system; 3) which processor and processing architectures are currently in use and in plan; 3) what risk mitigation strategies are used, with particular focus on the radiation aspects; 4) what type and number of interfaces are available.

At the end of the chapter the reader shall have acquired a greater understanding of avionics systems currently available in the market. Additionally, it shall be concluded on what are challenges and opportunities associated with these systems.

3.1. Functions

The functions performed by the avionics systems are dependent on the mission and type of S/C. Generally, they can be divided and described in the following way [37]:

- **TM/TC:** The telemetry/telecommand system, or TM/TC handles some of the functions required to connect with a ground station. In general, spacecraft health data, payload data and telecommands are concentrated in this unit that applies communication protocols at the data link layer of the OSI model. This process occurs for both incoming uplink data, which is routed to respective sub-systems, and to ongoing downlink data. The TM/TC interfaces with external RF front-ends over digital interfaces.
- **PLIU:** The PLIU or payload interface unit is responsible for collecting and sometimes pre-processing payload data, controlling the payload(s). It is often the case that this unit also stores data before routing it to other systems. Data compression or pre-processing algorithms can also be performed here in accordance to the mission requirements.
- **I/O interface:** A large number of sensors and actuators are present in modern satellites. Modules responsible for I/O interfacing provide functions such as analog to digital conversion, support for multiple data buses, debug and programming ports.
- **C&DH:** The command and data handling functions are responsible for the management of the spacecraft such as running a real-time operating system, task scheduling and execution, spacecraft monitoring and other flight software.
- **AOCS:** The attitude and orbit control system runs the required algorithms and operates an array of peripherals in order to correctly point the spacecraft and, in the case a propulsion system is present, maneuver the spacecraft.

3.2. Physical Architecture

Avionics functions can be performed by separate physical units or concentrated in a single unit. Common architectures are the single board computer (SBC), adequate to less complex satellites, and

the multiple modules interconnected via a backplane [38]. There are advantages and disadvantages for each of these solutions. This section presents the main features of each solution.

3.2.1. Single Board Computers

As the name suggests, the single board computer consists of a flat circuit board with all required electronic components such as processors, memories and interfaces. It can perform one single function or a combination of all the functions described above. Due to its small form factor, it is widely used in CubeSats, in the form of a PC/104 board. For larger spacecraft, sizes increase to around 350 mm by 250 mm sides (commonly referred by the supplier as 3U SBC). Although the small compact size is an advantage in some situations, it affects the possible complexity of the device and, specially, the number of interfaces. For that reason, SBC are used as general processing systems which can be employed as the main on-board computer for small S/C or to provide distributed processing power in larger missions.

3.2.2. Modular

A different architecture relies on the distribution of avionics functions across different modules as seen in figure 3.1. Despite the larger form factor, it enables flexibility for the designers to select adequate modules and redundancy schemes as well as the number of interface connectors. In the case of small satellites, the modules with backplane solution is the most popular. Products using PCI 104S (SpaceMicro Proton box), 6U PCI (Seakr) or 3U cPCI (Aitech) buses are common. With this solution, suppliers can fulfill a larger number of missions by assembling the avionics system in modules according to the client's needs. For instance, data storage can be increased by adding a dedicated module, interfaces changed and reliability increased by duplication of modules. In addition, each module can be sold separately which further increases profitability.

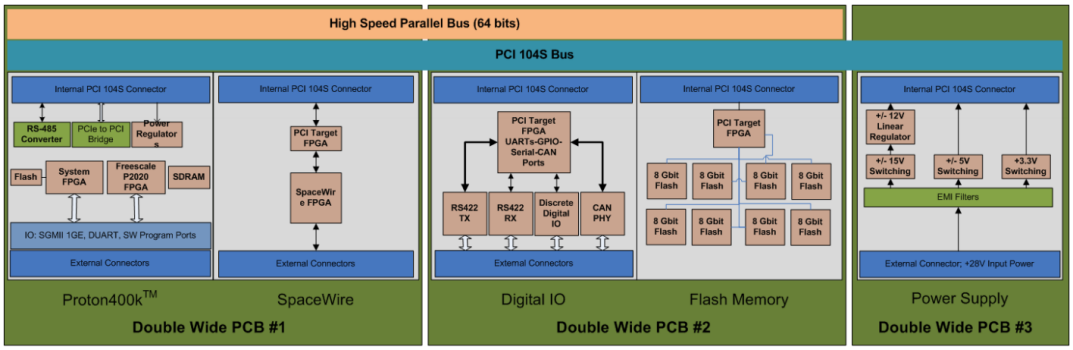


Figure 3.1: Functional units for SpaceMicro's Proton 2X Box. Credits: SpaceMicro

3.3. Processors

As opposed to CubeSats, which apply modern COTS or automotive grade processors, satellites above 50kg are still relying on rad-hard processors [39]. This is observed by analysis of current and planned missions and also by the available products in the avionics market. Rad-hard processors offer protection against radiation effects and due to their proven reliability are thought to be adequate for commercial satellites. The most common processors for these spacecrafts are:

- **LEON:** A 32-bit processor core, originally designed by ESA and then by Gaisler Research. It is based on the SPARC-V8 RISC architecture and designed for harsh environments. The LEON-3FT is a fault-tolerant version of the LEON-3 and it is commonly seen in space applications in the dual-core GR712RC and the UT699 devices by Aeroflex Gaisler and Aeroflex Colorado Springs, respectively [39]. An updated version, the LEON-4 was released in 2010 and it is seen in the rad-hard GR740 chip by Cobham Gaisler, with flight models expected to be available in 2020. This processor is described in synthesizable VHDL so it is also seen implemented in FPGAs [40].

- **ERC32:** A 32-bit SPARC-V7 RISC processor developed in the 90's for space applications and now owned by Microchip. The currently used version, the ERC32 Single Chip is implement in a

radiation tolerant TSC695F by Microchip. The company's website now mentions that this chip should not be considered for new designs as new models are in offer [39].

- **PowerPC e500:** This is another 32-bit core commonly used in network processors. It is mostly used in space applications in the form of the dual-core P2020 processor from Freescale, introduced in 2008 [41].
- **PowerPc 750:** The 700 series are 32-bit processors and are known for their use by Apple since 1997. The 750 is the base design for the RAD750 chip by BAE Systems, introduced in 2001 as a radiation hardened version of the 750 processor [42].

These architectures are either implemented as ASICs or in FPGAs. In addition to a processing core, systems are seldom employing a FPGA chips as I/O interfaces, payload interfaces or board supervisors due to their programming flexibility. The most common FPGAs models are [43]:

- **Microsemi RTAX** (Anti-fuse, 150nm)
- **Xilinx Virtex-5QV** (SRAM, 65nm)
- **Microsemi RTG4** (Flash, 65nm)

Previously, a literature review of micro-processors/controllers and SoCs for small satellites, in particular, CubeSats was performed [16]. In this document, a trend in the usage of highly integrated microcontroller units (MCU) was described along with some radiation performance characteristics. Common architectures include, PIC, ARM, MSP and STM. Satellite manufacturer SSTL, developed a new avionics system, CoreDHS, using a combination of a rad-hard LEON-3FT with a Zynq-7000 series SoC featuring dual ARM Cortex-A9 processing cores. The addition of the SoC enables tasks that have high computational demand but lower criticallity, such as image compression algorithms, to be performed much faster [44].

3.4. Interfaces

According to the general complexity of a system, interfaces are required for both data and power transmission. In these cases, a large variety of interface protocols and connectors are seen. A survey of the most common interfaces in components for all S/C subsystems was performed and quickly showed the trends in this area. [1]

Serial communications are commonly used in space applications as pin count is lower than parallel communications. Most common bus protocols for serial communications are MIL-STD-1553B, SpaceWire and CAN. Other serial protocol such as I2C and SPI are not as widespread in the small satellite industry, mostly used in micro-satellites.

The most common interfaces are arguably the TIA/EIA standards more commonly known as RS (Recommended Standard). The RS-232, RS-422 and RS-485 are complete standards which not only include electrical characteristics, but also physical and mechanical ones such as the description of the connector. Although maximum data rate is low, in the order of the Mbps, it is a reliable, legacy standard that fulfills the demands to exchange basic telemetry and telecommand signals across the S/C.

For more simple components communication protocols are not in place and data is sent in the form of analog signals. As it will be seen later, sensors and actuators such as temperature sensors or AOCS components often have analog interfaces for output and input. In these cases, general purpose input/output pins (GPIO) pins are required as well as analog to digital converters (A/D) in order for transform the signals into digital.

For high speed communications, required in payloads, other standards are used. Ethernet, RapidIO and SpaceWire are common as well as low voltage differential (LVDS) signals such as RS-644. The main advantages of LVDS are twofold: in one hand, the differential signal method, where signal is measured as the voltage difference across two wires, allows for higher speeds due to the lower voltage swings; secondly, the twisted pair is more immune to external electromagnetic noise both due to the coupled electromagnetic fields of both cables and the use of differential signals which eliminates noise sources that equally affect both wires. The basic operation of a LVDS circuit is seen in figure 3.2.

[1] The observations made in this subsection are derived from compiled information on COTS parts available online. This survey is available in annex A

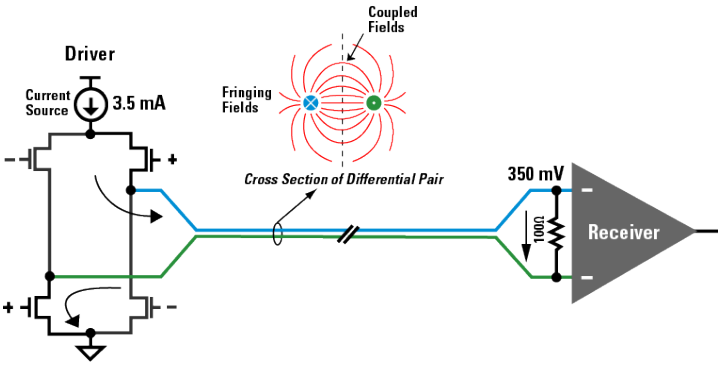


Figure 3.2: Basic operation of a LVDS circuit. Credits: Dave at ti

3.5. Risk mitigation strategies

The means to assure high dependability are diverse and require special attention since the early stages of the design process. These can be segmented according to the way high dependability is achieved and the faults are handled. A compilation of fault tolerance and avoidance techniques is presented in figure 3.3. These two major view points (fault tolerance and fault avoidance) represent two distinct concepts in spacecraft design. The first relies on the fact that faults are inevitable, due to unpredictable environmental or operational effects, and focuses on handling these faults in order to avoid failures. In contrast, the second view-point tries to totally avoid faults during mission lifetime and, therefore, avoid failure [45] [33].

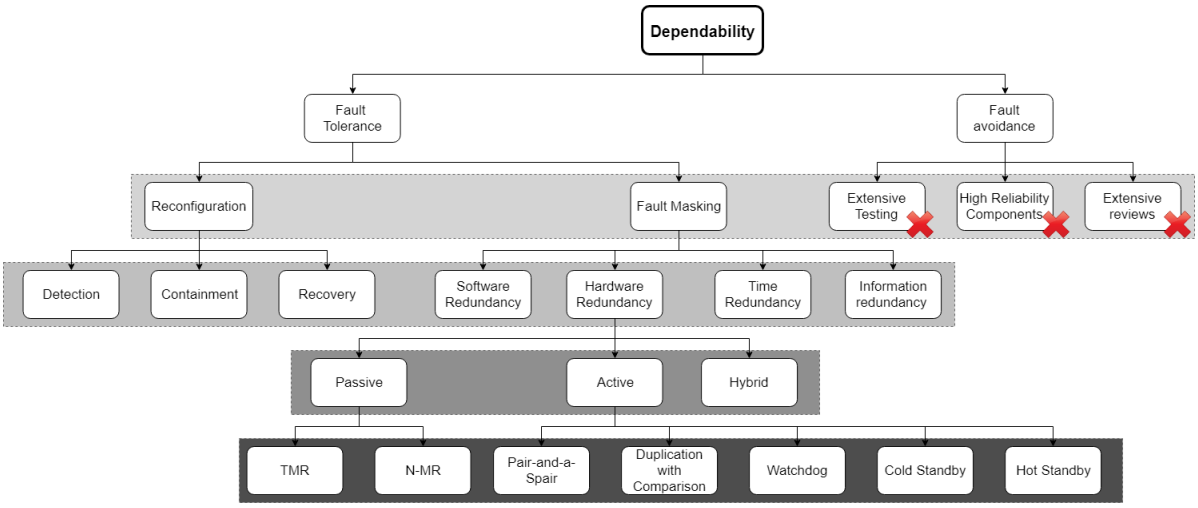


Figure 3.3: Dependability schemes. The left branches are related to fault tolerance whilst the right branches are related to fault avoidance. Since fault avoidance is against the paradigm surrounding this project, it will not be pursued at an high design level.

As mentioned in the definition of this project, the goal is to apply fault tolerance to a new avionics architecture in order to achieve high dependability figures, taking into consideration that fault avoidance is not suitable for the new class of cost efficient small satellites. Therefore, the right branch of the tree is not considered as a viable concept for further development. With this elimination, the fault tolerance branch is the one remaining, with the two main techniques, fault masking and reconfiguration. Fault masking is any process that prevents a fault to propagate in the system and introduce errors that may lead to failure. Reconfiguration is the process of reconfiguring a system in order to eliminate a faulty component and restoring the systems functionality. With it, a faulty component would not be recognized and handled, leaving the system exposed to potential errors and failures. Together, both approaches allow a system to detect a fault, avoid its propagation, and recover from it into a well-known, safe and functional state. Following this line of thought, the proposed avionics suite will include both fault masking and reconfiguration techniques in order to assure proper fault tolerance.

Fault masking is a concept that allows multiple implementations. As seen in figure, 3.3, masking can be achieved by redundancy, either in the form of software, hardware, time or information. In the form of software, redundancy is achieved by the addition of software functionality that surpasses the basic needs, so that it is possible to detect and tolerate faults. Similarly, hardware redundancy is the addition of extra hardware components that are able to detect and tolerate a fault. Additional information can also be added to a system, so that errors can be detected and corrected. Time redundancy is the use of additional time than the required to perform a function so that transient faults are tolerated. Within these categories, methodologies are varied, taking many forms according to the designers creativity and mission requirements. .

As it is described in chapter 2 and in [16], the radiation environment in space increases the risks of mission failure. In order to assure certain reliability levels, avionics designers have employed a variety of strategies, some reviewed in [16] and [9]. The most common in small satellites are:

- **Rad-hard components:** As seen above, designers are still relying in rad-hard processors specially designed for space applications. In addition to that, many other space qualified components such as memories and discrete logic elements are procured. Despite their high cost and lead times, they assure high reliability.
- **Redundancy:** The use of redundant design elements has been a historical strategy that prolongs mission lifetime in the case of a fault occurring. This strategy is strongly employed in the small satellite industry at the processor level by incorporating an additional, cold-spare processing board.
- **EDAC:** EDAC stands for error correcting and detection codes. It consists in dedicated algortihms to detect and corrected flipped memory bits. In the case of a bit flip due to SEE, additional versions of the same data or additional bits can be employed to restore original data.
- **TMR on FPGA gates:** FPGA manufactures now offer the possibility to automatically introduce triple modular redundancy in the logic gates when compiling a design. Besides other internal risk mitigation features, this tool simplifies the design process necessary to achieve the desired reliability levels.
- **Supervisors:** The supervisor monitors the spacecraft for unexpected changes that may affect the devices functionality. It continuously checks the system's status by means of periodic messages or others to quickly identify a loss of functionality and apply recovery methods such as reconfiguration.

3.6. Conclusions

The chapter reviewed the state-of-the-art in avionics for small satellites. It presented the main functionalities and how they are implemented in either SBC or modular systems. Common rad-hard processors were presented, complementing the research into micro-controllers for small satellites performed during the literature study. From this exercise, interface protocols were also identified along with risk mitigation strategies. These were divided into fault tolerance and fault avoidance categories.

It is possible to conclude from the aforementioned information and annex A.1 that small satellites (>50kg) are still relying on fault avoidance as a way to manage risks. Modern MCU and SoC are only now being utilized to their potential. Modular architectures are often utilized in these satellite as well as space qualified components. SBC are mostly used for <50kg platforms as the single OBC or in larger platforms for distributed computational power. Some products were found to provide high levels of integration and functionality. However, the lack of information makes it difficult to estimate the contribution of COTS components such processors, transceivers and memories. Promising products which possibly follow this combination are the OBC-100 + ACC-100 from Berlin Space Technologies and Proton 2X box suite with the Zynq-7020 option from Space Micro.

A new avionics suite for the 50kg to 200kg segment requires a synergy between fault tolerance mechanisms and modern commercial technology so that dependability levels are achieved without excessive cost overhead. It is concluded that such a solution does not yet exist in the market, in particular one that offers the same functionalities and dependability figures as rad-hard based solutions. The project shall develop a system that offers the same functionality as current avionics suites for 50kg

to 200kg platforms in an integrate package. The use of COTS technologies for these ends is still unexplored, as opposed to what is seen in CubeSats. Hence, determining the best application of COTS components would benefit the cost-effectiveness and performance of these spacecraft.

4

Reference Missions

In this chapter, the historical perspectives and short to medium term trends in the small satellite segment are presented. This discussion is reserved to satellites with a mass between 50kg and 200kg due to the growth predictions in this segment. Those satellites with lower masses, such as CubeSats, or higher masses are only presented when a comparison is justified.

An historical perspective of this market provides support to understand the applications these satellites are used for. Each of these applications will be described using reference missions as examples. This will improve understanding of the similarities and differences between missions and the requirements it imposes on space systems and respective avionics. The expected growth in each of these categories will be presented and justified, corroborating the focus of this thesis on the 50kg to 200kg market.

Furthermore, the commercial interest in this segment is demonstrated by presenting a selection of spacecraft platforms dedicated to fulfill the aforementioned applications. These platforms will further improve the understanding of this segment, in specific the requirements these applications/platforms pose on the avionics. Earth observation payloads are also characterized in order to derive requirements. The conclusions of this chapter support the selection of the 50kg to 200kg segment as one benefiting from the development of highly recurrent avionics suite.

4.1. Historical perspective

As a starting point to understand the context surrounding the small satellite market, the Union of Concerned Scientists (UCS) satellite database was consulted. In this database, almost 2000 operational satellites currently orbiting the Earth can be found. The last update dates to the end of November 2018. Assembled by experts, it contains relevant technical information about each satellite.

From this initial database, a shortlist was generated by retrieving the entries corresponding to satellites within the selected mass range of 50kg to 200kg. This shortlist contains 115 satellites, launched from 1993 to November 2018. Including all entries of the complete database, the predominance of this mass range is visible (see figure 4.1), only disturbed by a large number of satellites in the 250kg to 300kg range, related to a large Russian military communications constellation. These are 42 ”Rodnik/Strela-3” satellites and their civilian version ”Gonets” launched between 2001 and 2015.

A first analysis aimed at determining if satellite mass was a predictor of other characteristics, namely orbital inclination and perigee, electrical power, expected lifetime and function. It was found that mass was not a good predictor of any of these parameters, however, by plotting these relationships, other conclusions were found. In particular, orbits were found to be very similar in all entries, with sun-synchronous orbits between 400km and 800km being widely popular, as seen in figure 4.2. Other observed orbits vary from equatorial to 132°. The consumed power was dispersed across all entries and not directly correlated to the mass of the satellite, which can be seen as representative to its overall size. The total generated power ranges from 14W to 200W. The expected lifetime also follows the same conclusion with the numbers ranging from 1 year to 5 years in orbit. Additionally, no increase in expected lifetime with date of launch was found.

These 115 satellites can be divided into 4 categories as shown in figure 4.3: Communications, Space

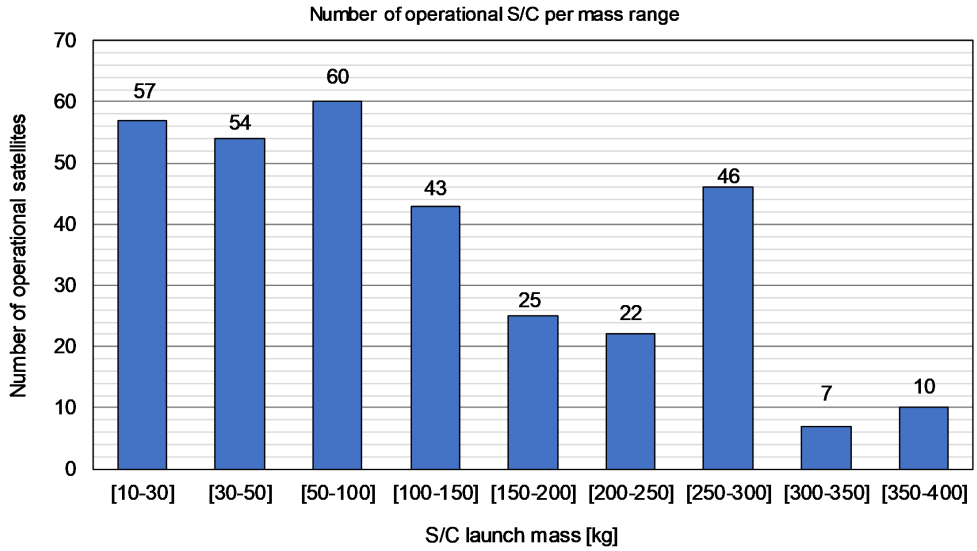


Figure 4.1: The number of operational satellites per mass category. Notice that the <150kg sector is largely populated. The 250kg to 300kg sector has a large increase in satellite number due to a Russian constellation of 42 military /commercial satellites. Derived from UCS satellite database [2].

Science, Earth Observation (EO) and Technology Development/Demonstration (TechDemo). Additionally, a combination of these is also possible. The database revealed that EO satellites are dominant, with 69 operational satellites, more than half. Another great proportion is attributed to TechDemo with 26 entries, followed by space science (7), multiple applications (6) and communications (4). A trend is already noticeable in the EO segment due to the increasing number of operational satellites. There are 16 operational, launched between 2010 and the end of 2014, whilst there are 43 operational satellites for this application launched between 2015 and the end of 2018. It was found that there are no particular concentration of entries with a certain mass range for any application.

Finally, the demographics of the issues were studied, with the goal to determine any particular countries or continents dominant in this field. The two dominant countries in this area are China with 29 operational satellites followed by the USA with 17 units. Asian countries operate 50% of satellites, followed by North America and Europe with 23% and 18%.

4.2. Mission types

As seen with the previous analysis, the applications of small satellites in LEO can be segmented into three major categories: LEO-based constellations, technology demonstrators and scientific [34]. Within the constellations segment, a distinction is also possible between remote sensing/earth observation and communications satellites. Each of these applications poses different requirements on the orbiting platform and, therefore, to the avionics subsystem.

A selection of meaningful missions for each application was made in order to understand these differences. Information on the spacecraft platforms was collected from news articles, websites such as ESA's eoPortal and Gunter's Space Page, corporate websites and publications. The following parameters were assessed when available in literature or online:

- Launch date;
- Payload(s);
- Avionics architecture and functions;
- AOCS components and requirements;
- Nominal and achieved lifetime;
- Reliability, Availability, Maintainability and Safety (RAMS) figures;

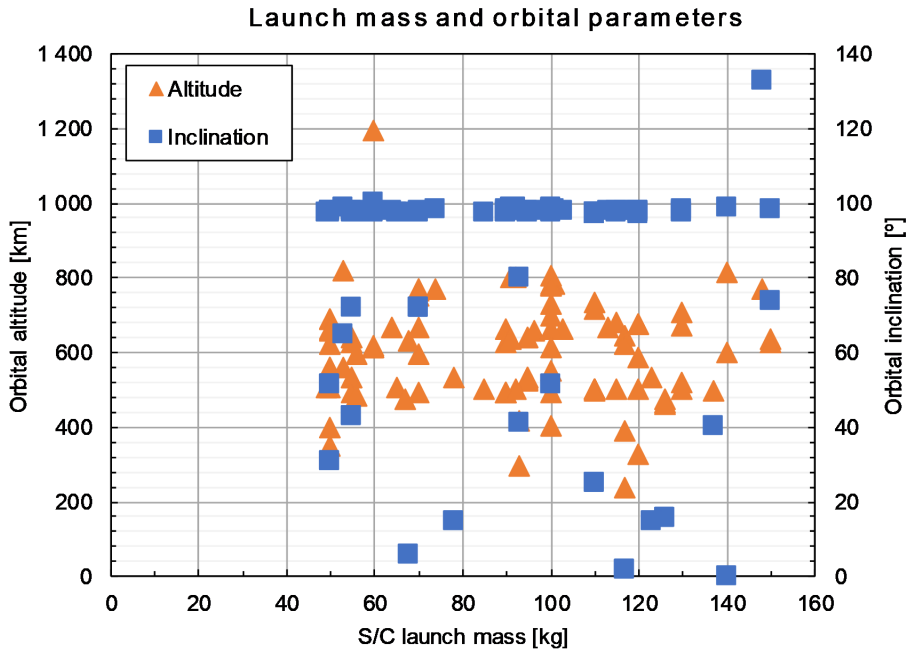


Figure 4.2: Orbital parameters as a function of satellite mass for currently operational 50kg to 200kg satellites. Derived from UCS satellite database [2]

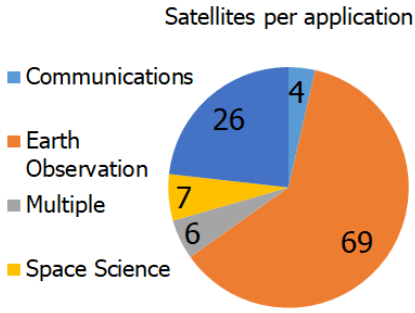


Figure 4.3: Number of satellites per type of application for currently operational 50kg to 200kg satellites. Derived from UCS satellite database [2].

- Generated Data;
- Downlink capabilities;

4.2.1. Constellations

The demand for high capacity, low-latency broadband services and high spatial and temporal resolution imagery services is driving the commercial interest in small satellite constellations. The current understanding is that these large amounts of data enable other downstream services that create value by interpreting them. Using large numbers of satellites, the entire Earth is under persistent surveillance enabling unprecedented revisit times. Any location on Earth can be watched or serviced at all times, and everything and everyone connected. [46]

As the demand for the services increases, the number of large constellations deployed is also expected to increase. Figure 4.7 presents a forecast for EO satellite launches, showing not only the increased number of launches but also a wide variety of companies operating in this segment [46]. Additionally, the need to upgrade and renovate fleets generates a constant demand for satellite components such as avionic systems [34].

The following table 4.1 is a collection of a diverse set of commercial LEO small-sat constellations. This set of proposed and active constellations was considered as a meaningful representation of the industry, compiling a variety of LEO applications, payloads and spacecraft sizes, and therefore, it was used to better understand the state-of-the-art.

Constellation	**Application**	**Number of units**	**Satellite weight [kg]**	**Orbital altitude & inclination [km, º]**
OneWeb [47] [48]	Global Internet	720	150	1200
Spire [49] [50]	AIS, ADS-B, Weather Observation	125	4	650, Various
Sky and Space Global Pearls [51]	Mobile Voice and Data	200	10	650, 0
AisTech [52]	EO (Thermal), AIS, ADS-B	150	3 to 12	600
Helios Wire [53]	IoT	>3	20	-
AstroCast [54] [55]	IoT	80	4	600, 97
Aerial & Maritime	AIS, ADS-B	80	5	-
Planet Flock	EO (Visible)	100	5	400, 52
Planet RapidEye	EO (Visible)	5	150	620, 98
Planet SkySat[56]	EO (Visible)	27	120	450, SSO
Earthi Vivid-i	EO (Visible)	15	100	550
ICEYE	EO (SAR)	18	70	500, 98
AxelSpace AxelGlobe	EO (Visible)	20	80	600, SSO

Table 4.1: A selection of LEO small-sat constellations (non-exhaustive). These entries are thought to be representative off the industry and the needs of the sector in terms of technology. SSO: Sun-synchronous orbit.

Earth observation/Remote sensing

Earth observation/remote sensing platforms are key enablers for services in a number of existing and emerging markets, such as agriculture, Earth mapping, disaster and resource monitoring and economic modelling. These LEO satellites are able to cover the entire Earth in multiple wavelengths in five days, or in one day if five satellites are used (based on a 660km swath) [4]. The large amounts of generated data then feed a variety of downstream services that process the raw data using complex algorithms and artificial intelligence to enable smart decision making. High definition video and sub-meter ground sampling distance is possible for platforms within the mass range [34].

In this sector, an array of companies are operating constellations or in the process of validating their technology. Companies like OneWeb, Planet, Earthi, AxelSpace, Satelogic and Exact View are all basing their business plans in data generated from their satellite constellations, operating in LEO and with masses situated in the 50kg to 200kg range. In some cases, such as Planet's Flock constellations, CubeSats are also used although the form factor poses restrictions on the optical payload and achievable performance figures. The payload is usually a single telescope and sensor setup producing Gigabytes of data per day. Partnerships with experienced spacecraft manufacturers are common as a way to developed their own manufacturing capabilities, although Euroconsult predicts that manufacturing outsourcing will stay constant at 86% until 2026. The satellites follow the manufacturer's available platforms and technologies which seldom include a combination of COTS and rad-hard parts, with dual redundancy in most subsystems. In terms of avionics, available information on the platforms points at the use of rad hard processors based on LEON3FT and PowerPC architectures. The number of satellites per fleet ranges from tens to hundreds of units, deployed in batches [57].

In this segment, a typical example are the SkySat satellites by Planet (formerly Skybox Imaging) built to acquire high resolution panchromatic and multi-spectral images of the Earth (see figure 4.4). Based on a commercial platform, Surrey Satellite Technology's SSTL-50, they weight around 120kg and were first launched in 2013. As payloads, they contain a Ritchey-Chretien Cassegrain telescope with 3 CMOS detectors [3]. By following the SSTL-50 platform, these satellites are expected to have a dual redundant, distributed architecture with separate modules for communications, payload interface and command and data handling. The AOCS system is composed by a variety of sensors and actuators to enable ±0.1º attitude control accuracy and includes a High Performance Green Propulsion system by ECAPS . The nominal lifetime is 6 years. Based on the SkySat-1 and 2, the prototype satellites for the constellation, the on-board data storage capacity is 768GB, downlinked via X-band at 470 Mbps [58]. A different example is the ICEYE-X1 launched in early 2018 by Finnish startup ICEYE. It contains a prototype SAR (Synthetic Aperture Radar) designed to provide near real time SAR imagery in X-band at a 10m resolution. It weighs 70kg and includes a 3.25 meter long deployable antenna. It is expected to operate for a maximum of 3 years at an altitude of 500km [59].

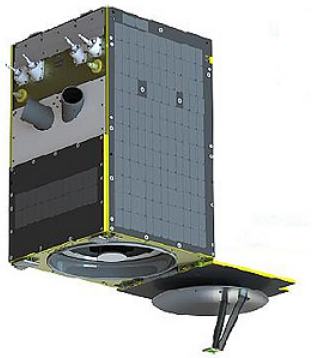


Figure 4.4: The Skysat-3 from Planet's Skysat constellation. In the bottom of the image, an aperture cover that protects the imaging payload during launch is visible. Retrieved from space.skyrocket.de [3]

Communications

Another use of LEO is in the creation of global communication networks. The leveraged position in orbit enables coverage of the entire globe providing high-capacity, low-latency communications, tracking systems for maritime vessels (AIS) and aircraft (ADS-B) or Internet of Things (IoT) networks. Also, affordable internet access from space, not before accessible to remote or impoverished populations will contribute to a change in their paradigm and be a massive benefit to their development [34].

As with EO constellations, a number of commercial players are already establishing their position. In this case, focus is also given to MEO and larger satellites, as it is the case with Iridium, SpaceX and Telesat constellations. As opposed to EO spacecraft, that deploy large optical payloads, communication satellites are able to rely on smaller platforms, usually CubeSats (3U or 6U). In these cases, small patch or deployable antennas contribute to lowe size and mass. As launch cost is related to spacecraft mass, these mass savings by using CubeSats are extremely attractive. Some examples of commercial ventures in this area are Aerial & Maritime (AIS and ADS-B), AstroCast (IoT), Helios Wire (Machine to Machine) and Spire (AIS and ADS-B), besides others. Avionics architectures with no redundancy and rad-tolerant or rad-soft processors are chosen. The lifetime is affected by this with nominal lifetimes of 5 years planned at maximum with some companies planning to decommission a unit after 2 years in orbit. As with EO satellites, polar orbits at 400km to 600km are the norm, with more equatorial orbits also used for some constellations [1].

The first Lemur-2 satellites by Spire were launched in 2015 with multiple others being launched every year since. These satellites, shown in figure 4.5) carry a GPS radio occultation payload and AIS and ADS-B payloads. Commercial CubeSat components are used, including separate boards for telemetry, payload interface, AOCS control and on-board computing empowering modern SoCs and FPGAs. Lifetime for these platforms is currently limited to less than 5 years due to these technologies including the available propulsion options. Redundancy is usually not employed and recurrent replacement of the fleet is expected with Spire expecting to retire a satellite after 2 years of service. The telemetry data is not as massive as with EO applications as these are communications satellites. S and X-bands are used in Lemur-2 as well as with other satellites, with UHF/VHF being another option [49].

A different perspective is demonstrated by OneWeb's Arrow platform, built by Airbus. This is a 150kg spacecraft designed for a minimum of 5 years at 500km to 1500km. Designed to be a highly reliable, flexible platform hosting payloads up to 80kg, it will serve as the base for OneWeb's global internet service. Using the Ku-band, 648 of these satellites will enable global 50 megabits/second downlink bandwidth [60] [61].

4.2.2. Technology demonstration

The most effective and intuitive way to test space technology is to, in fact, flying it in space. Due to the challenging characteristics of space flight, new technology is required to show its value in space as guest payloads thus acquiring flight heritage in the eyes of satellite integrators. With the proliferation of small satellites, the cost to access space is reduced, and more spacecraft with an array of experimental components and payloads are being sent to space.

[1] Based on analysis of missions from UCS satellite database [2]

Figure 4.5: Lemur satellites in clean room (image credit: Spire Global)

As startups launch their first pathfinders up to ten experimental systems, including scientific experiments, are flown in individual missions. Time in orbit is reduced to one or two years to reduce costs while meeting the mission goals.[2].

The 2017 Flying Laptop mission, developed at the Institute of Space Systems (IRS) at the University of Stuttgart in Germany, contains ten technologies onboard that it plans to demonstrate and validate. These include an high-performance OBC, laser communications and AOCS components among others. A redundant avionics architecture is employed in each of the three boards, securing command processing and normal operations, telemetry decoding/encoding and input/output management. A dedicated FPGA monitors and controls the payloads and handles its data. Fault avoidance is achieved by using a qualified UT699 LEON3 processor. The Spacecraft is 3-axis stabilized and has an expected lifetime of two years. Up to 2GB of payload data can be store onboard a flash memory before being downloaded via S-band [62] [63]. The spacecraft is shown in figure 4.6.

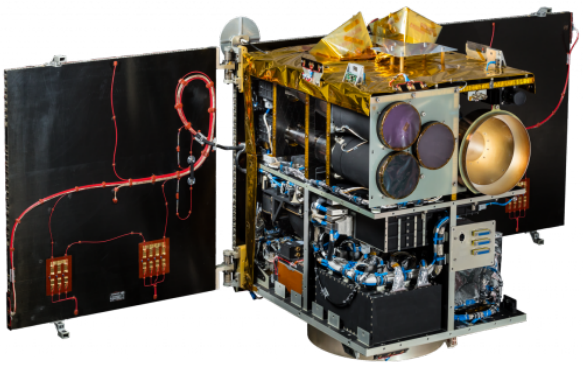


Figure 4.6: The 2017 Flying Laptop mission, developed at the Institute of Space Systems (IRS) at the University of Stuttgart in Germany. Credits: IRS, University of Stuttgart.

4.2.3. Science

This application has been greatly favored by the proliferation of small satellites, mostly CubeSats. Currently, science teams are less restricted in terms of which experiments to fly due to cost reductions. Despite the growth in the total number of scientific missions launched, analysis of the UCS database revealed that this growth is support by micro-satellites with weights below 50kg.

The typical mission consists on a satellite equipped with a large variety of payloads, each dedicated to observe a certain phenomena. A dedicated payload interface data handling unit is usually employed to integrate the multitude of payloads with the rest of the avionics system. The acquired data is then stored onboard before it is downlinked. Due to the large number of instruments, the data handling and

[2]Based on analysis of missions from UCS satellite database [2]

storage requirements can be more demanding than what is seen in missions with less and more simple payloads. The lifetime is dependent on each mission and is often extended way beyond the nominal value if the spacecraft is still operating nominally.

4.2.4. Growth forecasts

An analysis of the prospects for the small satellite market (figure 4.7) has a positive outlook for the future of the industry. According to Euroconsult [46], 3700 small satellites are expected to be launched between 2016 and 2025, a $22 billion prediction. The EO sector is expected to launch a massive number of units, more than 200 on 2022 alone, in order to build the fleets for the constellations, some mentioned in 4.1. These missions are mostly based in optical systems, 71%, with radar representing 8% and the following percentages a combination of technologies [46].

These growth predictions are clear and show how much LEO will play a role in the future of economy. In fact, outsourcing in satellite manufacturing is expected to increase to 86% in 2026, in opposition to in-house manufacturing, further opening the doors to new ideas and companies in the satellite industry.

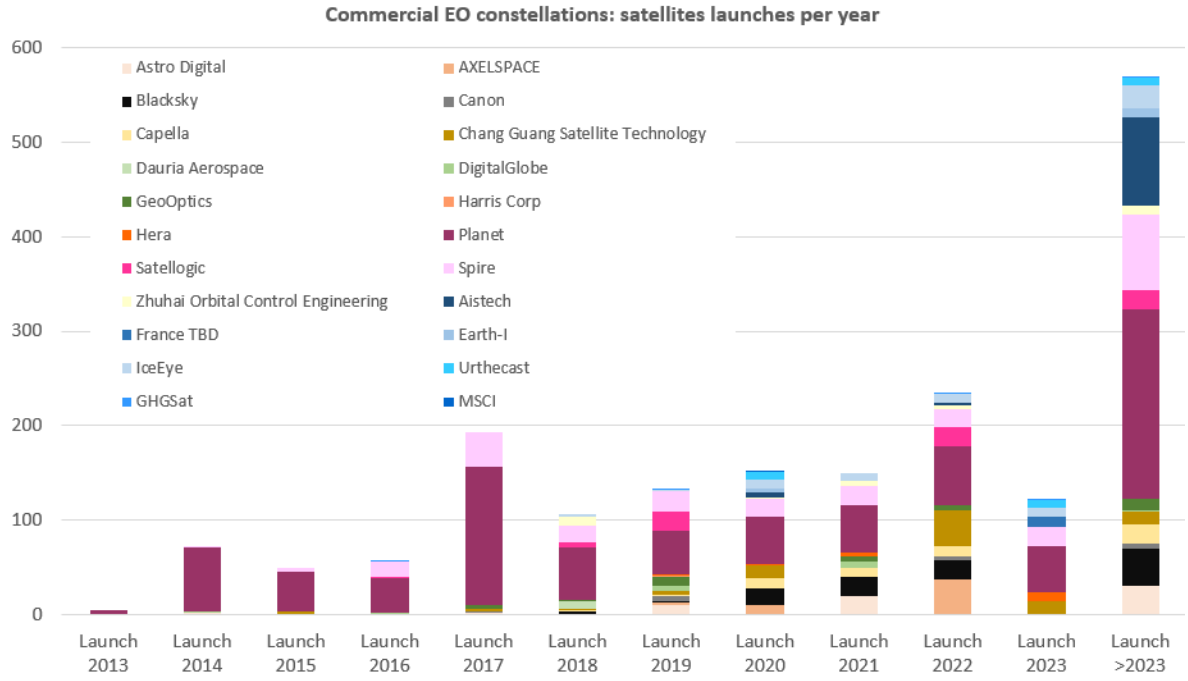


Figure 4.7: Commercial EO constellations planned. (data from EuroConsult report: "Satellite-Based Earth Observation: Market Prospects to 2027"

4.3. Spacecraft platforms

Due to large growth expected in small satellites (see 4.2.4), satellite integrators are investing in a next generation of S/C platforms and components able to fulfill the market demand. As the space industry moves from custom manufacturing to higher production levels, a gap is opening for the companies able to offer the best platform for the commercial satellites expected to be launched. These requirements are different from the traditional space industry. In the future, the cost/performance ratio is bond to reduce as it is expected in a growing market.

A number of companies have shown interest in providing a versatile, commercially attractive platform for small satellites. These platforms are designed to accommodate a range of different payloads with low integration effort and lead times. By offering a platform with a complete set of sub-systems and flight heritage, optimized for piggyback launches, costs and risks for the satellite owner are reduced. The following commercial S/C platforms are exemplifying of this trend.

4.3.1. InnoSat by ÅAC Microtec

The InnoSat platform is a joint programme between AAC Microtec and OHB Sweden (prime contractor). It is designed for LEO missions, mostly scientific, of up to 5 years. The spacecraft mass is only 40kg with additional 15 kg available for payload. This basic platform can be adapted to incorporate larger solar panels (40W up to 120W) or a propulsion system. Telemetry and payload data can be downlink via S-band or X-band with data rates not exceeding 50Mbps. The pointing accuracy is ±0.01º. The first flight for this S/C bus shall be in 2019, in the MATS (Mesospheric Airglow/Aerosol Tomography and Spectroscopy) Swedish satellite mission [64] [5]. A render of this platform is shown in figure 4.10.

4.3.2. SSTL-X Series by Surrey Satellite Technology

Surrey Satellite Technology is a company with a large presence in the small satellite segment supporting satellite constellations from Planet and Earth-i. The new X-series spacecraft, seen in figure 4.9, are planned to substitute the legacy platforms and introduce better performance figures in order to adapt to the markets. These satellites are particularly prepared for EO missions by offering imaging payloads in the visible and near-infrared (NIR) spectrums, with high definition video capabilities, high data storage (up to 1 Tbyte), downlink (S or X-band up to 500Mbps) and high speed data bus. Reliability is assured by the use of dual-redundant systems. The platform also offers modularity in subsystems' configurations and avionics configurations. These satellites have an expected lifetime of over five years and weight between 50kg and 300kg, with 85W peak power. The first prototype, Carbonite 1 was launched successfully in 2015. [4]

4.3.3. Arrow by Airbus DS

Aerospace company Airbus Defense and Space has, together with constellation operator OneWeb, developed a S/C platform for the 150kg class, shown in figure 4.8. This platform is designed to support OneWeb's global internet constellations composed of 720 satellites. These satellites are designed to host 60kg to 80kg payloads for a minimum of 5 years in LEO. It is equipped with a Xenon based electric propulsion system which enables up to 700km of orbit raising capability. OneWeb's downlink requirements aren't as demanding as EO optical constellations so expected downlink data rates in this platform is 480kbps. Nevertheless, Airbus offers a Ka-band upgrade to achieve a 1.6Gbps data link. Its solar wings provide up to 250W of power [60] [65].

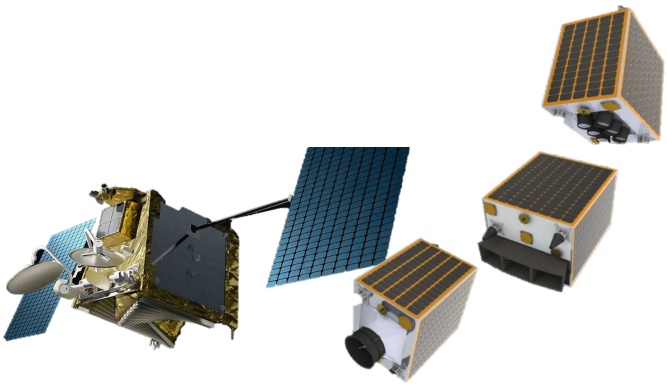


Figure 4.8: Arrow platform from Airbus. Credits: Airbus DS

Figure 4.9: Three configurations for the SSTL-X50 platforms. From top to bottom: 22m GSD, 5m GSD, 0.7 GSD. Found in [4]

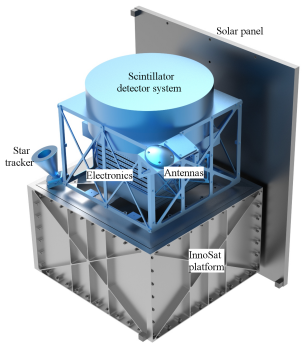


Figure 4.10: The InnoSat platform from OHB Sweden. The grey area is the satellite platform whilst the blue area is dedicated to the hosted payload. [5]

4.4. Payload analysis

The previous sections shed some light into EO satellite constellations. However, it is necessary to build on that knowledge about payloads in order to properly develop and cluster requirements. In this section, optical and radar payloads will be characterized in accordance to similarities and differences

regarding the requirements they impose on avionics systems.

A selection of variables is used in order to characterize these payloads. At this stage of the project, the most relevant ones are the payload type, market share, interfaces and data protocols.

The following two sub-sections will provide quantitative and qualitative results for each of these variables. At the end of this section it will be possible to derive high level requirements that enable the avionics system to handle the expected payload types.

4.4.1. Optical

There are two major types of optical payloads according to their architecture. This distinction is of major importance when it comes to avionics requirements so they will be dealt separately. A table with a compilation of diverse optical payload systems aimed at the target mass range is given in table 4.2.

Type I: Fully independent

The first payload architecture is an almost autonomous system. It consist of all the optics and electronics required to interpret telecommands, capture the image, process data, store the data and prepared the downlink message to be sent to the RF unit. The payload only interacts with the S/C avionics in order to receive telecommands and send housekeeping telemetry. It may also receive a pulse-per-second (PPS) signal from the GPS unit for synchronization purposes. The payload unit interfaces with the RF unit (usually X or S-band) in order to send the payload data via a high speed downlink.

In this payload architecture, all the required electronics to perform the above functions are integrated into a monolithic payload unit or in a dedicated accompanying unit. In terms of integration with the main S/C avionics, this system translates into a significant reduction in complexity as it functions like a simple RTU without large data transfer or processing requirements. Some examples of this architecture can be seen in the JSS-54/56/61 payloads from Jena Optroniks [66], NAOMI from SSOT mission [67] or the payload from the NEMO-HD mission [68]. Special attention is justified for the JSS-54 payload as it is installed in the RapidEye Constellation from Planet [66]. This can be understood as a sign that commercial constellations are interested in acquiring complete systems from external suppliers that reduce integration complexity.

Type II: Semi-Dependent

These payloads consist of all the optics, focal plane array (FPA) , proximity electronics and some level of pre-processing electronics. Unlike the type I payloads, their memory capabilities are reduced, usually to some hundred megabytes RAM memory to act as a buffer. Acquired data is sometimes pre-compressed and then sent to a separate PLIU or to the main avionics for storage and downlink via serial interface. This PLIU can either be a commercial product or a custom design for that specific mission.

In this case, an external device is required to, not only operate the payload, but also to retrieve payload data. This adds significant requirements to the avionics system. The performed research shows that data rates have a wide range since image resolution, number of spectral bands, and frame rate can vary widely. As an example, the Streego payload from Media Laro Technologies, a multispectral imager consisting of a FPA and proximity electronics, has a pixel rate of 158Mpx/s at 10 bit per pixel in video mode. This translates into a 1.5 Gbits per second data rate, which is assumed to be further compressed in the proximity electronics before it is sent via a RS-644 serial data interface [69]. In comparison, the HySI hyperspectral imager, flown in India mini satellite 1 (IMS-1) in 2007 produced 4 Mbps [70]. Some payloads of relevance with this architecture are Streego [69] and HyperStreego [71], HyperScout [69], HySI [70] and Tropomi [72].

4.4.2. Radar

SAR payloads are, in general, not widespread in small satellites due to their SWaP requirements. The large power required for the radar limits this payload to large satellites. Nevertheless, feasibility studies are investigating the use of this payload in smaller satellites [74]. Some new mission, such as ICEYE, a 70kg spacecraft are now demonstrating the capabilities of <200kg satellites [75]. In terms of architecture, the concepts and products with available information are all type II.

Payload	Interfaces	Data	Required Pointing Accuracy
JSS-54/56/61 [66]	2x PPS, 2x CAN, 2x serial TM	CCSDS formatted Triple DES encryption Up to 120Gbit internal storage Up to 4x 50Mbps	0.2º
Streego [69]	RS-644, 2x CAN, Trigger	8,10 or 12 bit 1550Mbps	——
NAOMI [67]	2x Glink, Analog TM, serial TM, PPS	10 or 12 bit 64Gbit internal storage	——
HySI [70]	TC, Serial	16 bit 8 Mbps	0.1º
Nemo-HD [73] [68]	CAN, 2x Ethernet	——	0.03º

Table 4.2: Compilation of optical payloads for small satellites.

This type of payload generates large amounts of data so usually the duty time is only a fraction of the orbital period. The orbit duty cycle is typically limited by the capability to transmit the data to the ground. An efficient data compression is essential for these systems [76] [77]. Data rates are high, with the one in BIOMASS (>300kg) at 270Mbps [78], Sentinel at 1Gbps and a feasibility study for 130kg satellite at 1.5Gbps [74]. Larger platforms will have even higher data rates, up to 60Gbps[78].

Data is usually in 8 bits, transmitted to OBC for storage by high speed serial (ex. sRIO [74] [77] or MIL-STD-1553 [79]). Since data rate is very high, storage requirements are also demanding, at hundreds of Gbyte. The resolution of these systems is restricted by physical size of antenna and transmitting power. The pointing accuracy needs to be at hundredth of a degree level [80] [81].

4.5. Conclusions

This chapter provided an overview of the main aspects related to the reference missions for the avionics system. It was supported by the analysis of operational and future small satellite missions to conclude on their similarities and differences. It informed on popular mission concepts and parameters, S/C specifications and onboard payloads.

Current and future missions in the intended mass range were found to fly between 400km and 1200km with a large concentration of missions in high inclination orbits. These can be divided into categories: Earth observation, technology demonstration and scientific. Mission lifetime is typically 5 years. Power produce for the entire satellite varies between 40W to 200W depending on the number of solar panels. Payloads for Earth observation mission can be divided into the ones that require minimal interfaces with the main avionics and others which are more reliant on external systems. The former, is able to collect, process and store payload data including interfacing with RF units. The main avionics only provides control and collects housekeeping telemetry via serial bus interface. The latter, expects an PLIU to receive the observation data in real-time, provide storage and other functions related to the control of the payload.

The small satellite market is definitely a growing segment due to the contributions of LEO constellations. Euroconsult predicts that between 2016 and 2025, this segment will generate 3700 units and 22 billion dollars with EO constellations corresponding to 54% of market share. Due to this growth projections, EO satellites were found to be adequate reference missions for the design of a new avionics system. In this segment, EuroConsult also predicts the focus on optical payloads with 71% predominance and radar instruments with 8%, with the rest of the missions composed of GNSS instruments or a combination of instruments. Hence, optical payloads are assumed. The payload is expected to be of type II, requiring a high speed data link to the main avionics. This leads to a design adaptable to a large variety of missions. The following list compiles the main characteristics of the reference mission:

- Earth observation constellations.
- LEO - 300km to 1300km altitude, 0°to 98°inclination.
- 50kg to 200kg satellite.
- Up to 200W of total S/C power.
- Up to 500Mbps downlink.

- Optical payload - up 400Mbps of raw payload data, requiring up to 64GB of storage.

The following chapter takes into consideration these findings and selected reference missions to develop high level requirements. These translates into a organized list the implications of the selected reference missions on the avionics system.

5

High Level Requirements

Earth observation constellations were found to be an use-case which could benefit from an integrated avionics solution leveraging COTS components. A summary of the characteristics of these constellations was presented on the previous chapter. The following step in the system design is to write high level requirements.

The initial high level requirements are of major importance. They establish the first direction the project must take and support all other developments from this point onward. These requirements are divided into functional and non-functional ones. They are written with special caution to not cause any unnecessary restrictions in later stages of the design process, whilst supporting concept selection. Hence, they are not particularly detailed or technical.

In this chapter, the project's high level requirements are described with a requirement list provided in annex C.2. At the end of this chapter, the baseline specifications for the avionics design shall be clear to reader. Following this chapter, it is possible to begin designing and selecting concepts that might fulfill the project's goal.

5.1. Functional requirements

The functional requirements describe the high level functions expected from the avionics system, related to section 3.1. As it is mentioned in the introduction and concluded in the previous chapter, this project strives to produce a design able to integrate multiple avionics functions in a single package, thus reducing recurrent engineering costs. Therefore, it includes functions related to TM/TC, PLIU, I/O interface, C&DH and AOCS. The system is also envisioned to receive a 28V unregulated power input from the S/C platform and provide regulated secondary voltages internally as needed.

The central functionality of the system is the C&DH of the platform by running a real-time operating system. This shall be able to coordinate task execution, monitor the S/C and operate any other avionics units. For that end, it shall provide processing power, data storage and interfaces to the exterior. The minimum set of interfaces shall be a serial data bus, analog interfaces, time and clock sync. The unit shall be able to both receive these clock and sync signals from external units as well as distributed them internally and externally. This functionality is commonly known as an OBC in other commercial products.

In order to stabilize and point the platform to its target, the system shall be able to interact with AOCS peripherals. These can be either digital or analog interfaces according to the platform. Processing power is required to run the AOCS algorithms. According to the previously performed research, it is expected that 20 AOCS peripherals are connected, including nominal and redundant units. Location data is provided by an external GPS unit. At least one propulsion units is to be interfaced via serial interface.

Data layer coding/decoding of telemetry/telecommands is expected. The CCSDS standards are to be implemented along with the ability to interface with nominal and redundant RF units via serial interfaces. The TM/TC function is also expected to gather telemetry data from each system unit as well as distribute telecommands.

Following the conclusions in 4, the avionics unit shall support the expected payloads for EO applications. This includes two distinct payloads per platform to be controlled via a serial interface with at least two high speed differential pairs for data transfer per payload. Regarding the payload data, a minimum data rate of 400Mbps per payload is to be supported with ability to store more than to 64GB of observation data.

A list of the discusses high level functional requirements is presented in annex C.2.1.

5.2. Non-functional requirements

The non-functional requirements dwell on characteristics and constraints on the avionics system. The main categories found to be important at this stage are the ones related to dependability, environment definition, SWaP and cost.

As concluded in chapter 4, the typical EO mission has a duration of 5 years in LEO aboard a 50kg to 200kg satellite. These orbits have altitudes between 300km and 1300km at both low and high inclinations. Operating temperatures are expected to fluctuate between -30ºC and +60ºC according to similar products. The system shall handle these conditions, in particular the challenges associated with the radiation environment both in terms of TID as well as single event effects.

As one of the main aspects of this thesis project, dependability figures are to be taken into consideration since early stages of the design. These depend strongly on the application environment. The system shall operate without significant performance and functional degradation for a minimum of 5 years in the expected orbits. Lower limits for availability are set at this stage at 99.9% (8h 46min downtime per year) in the worst case conditions, expected to be encountered at solar maximum. Also, the availability shall be maintained autonomously with minimal ground intervention.

Physical characteristics are roughly defined in order to maintain competitiveness in the market. Physical envelope shall be smaller than 200 x 200 x 200 mm with a combined weight with casing of less than 5 kg. Peak power consumption shall be lower than 40W at end-of-life (EOL) . Typical power consumption should be less than 20W.

The avionics shall make use of COTS parts as much as possible, not subject of third party access restrictions such as ITAR. It shall provide tailoring to the mission both in terms of functionality as well as performance without requiring major redesigns. Additionally, internal redundancy shall be supported. For that end, modularity is expected with no negative significant effect on the dependability figures. Rough order of magnitude (ROM) cost of components should be lower than 100000€.

The list of non-functional is found in annex C.2.2.

5.3. Key, killer & driving requirements

In this section, the most relevant requirements will be identified and categorized. The key requirements are those that have the largest influence on the reaching the project's goal, providing an answer to the research questions. The driving requirements are those that are likely to have a large influence on the design, hence they drive the design. Finally, the killer requirements are those that are already identified as being extremely hard to achieve.

The key requirements are thought to be the goal to design an avionics suite with all the expected functions whilst using of COTS components (HLR-O04). Achieving this functionality level with mainly COTS components is fundamental to reduce recurrent engineering costs and potentiating the small satellite market.

The most important driving requirement is the 99.9% availability in worst case conditions, as the widespread use of COTS components requires additional design features in order to achieve this figure (HLR-R04). This requirement represents the design challenge accepted for this thesis project.

Finally, no particular killer requirements were identified at this stage of development. It is thought that the technical characteristics and dependability potential of COTS components, as will be demonstrate in chapter 10, combined with appropriate fault handling methods are able to fulfill the purpose of this thesis.

5.4. Requirement verification

At this stage of the thesis project, it is still premature to establish hard requirements and requirements verification processes. As mentioned, these high level requirements mostly perform a steering

function, improving the definition of the project, its challenges and novelty factors.

The thesis project will stay on the analysis level and, subsequently, so does the verification process. It is not expected to build a prototype or a complex computer model of the entire system. Still, it is expected that, at the end of the project, dependability figures related to the radiation challenge are achieved. Such analysis, complemented with literature resources, will provide a satisfactory verification process able to support the conclusions of the project for further development outside the scope of this document.

5.5. Conclusions

High level requirements were presented in this chapter. These represent the first definition of the system to be built following the research of the previous chapters. Analysis of the most important requirements was performed.

An highly integrated system is expected to be designed. One that is able to substitute other avionics units, becoming the center of the S/C system. The target of this system is 5 year EO missions in LEO, with launch masses between 50kg and 200kg. A target availability of 99.9%, or less than 8h 46min downtime per year, requires a certain level of autonomy which distinguishes this system from other COTS based systems.

The following step in the design process is the discovery and selection of concepts. A number of these concepts are presented and discusses. It shall advise on functional allocation and ability to meet non-functional requirements.

6

Concepts

The previous chapters focused on the initial definition of the project including its relevance, market positioning and basic requirements. Now, the first steps into the actual design of the avionics suite are taken. The first design possibilities will be presented and at the end a clearer vision of what to achieve will be formed.

The first section of this chapter is an high level discovery of avionics architecture concepts. With the use of a discovery tree, multiple concepts will be explored, described and exemplified using satellite missions, COTS products or research papers. Visuals will help better understand the differences between each concept which is necessary for the following step: a trade-off. An in-depth analysis of each concept with respect to a selected number of parameters will assist the aforementioned trade-off to select the most adequate concept. After this selection takes place, it is possible to dwell deeper into the concept, better map functions and high-level requirements into an initial design.

At the end of this chapter, these issues shall be handled, to generate a rough definition of the architecture along with supporting technologies required. This shall make it possible for the next chapter to define more concrete system requirements that will further define the avionics suite.

6.1. High level design option tree

A design option tree is commonly used as a brainstorming tool to identify all possibilities for a design without overlooking possible solutions. By hiding details of the implementation it avoids distractions at the same time it allows for organized decision making [17]. Hence, it is used as the first step towards selecting a baseline conceptual idea of the avionics architecture.

The tree in figure 6.1, is divided into three main branches according to the distribution of functionalities behind each concept. The left branch contains all concepts where functions are mostly centralized in a specific unit. The center branches represents the antagonistic idea, where all functions are dispersed inside the system as deemed necessary. Finally, the right branch combines both ideas into a set of concepts that include a centralized piece in the avionics although de-centralization of functions is also accomplished.

Each of these three branches is represented by a letter, A, B and C, and each concept within those branches is identified by a number. Exemplary implementations are mentioned and used as a visual description. Major advantages and disadvantages are mentioned briefly, as they will be further explored in the following section.

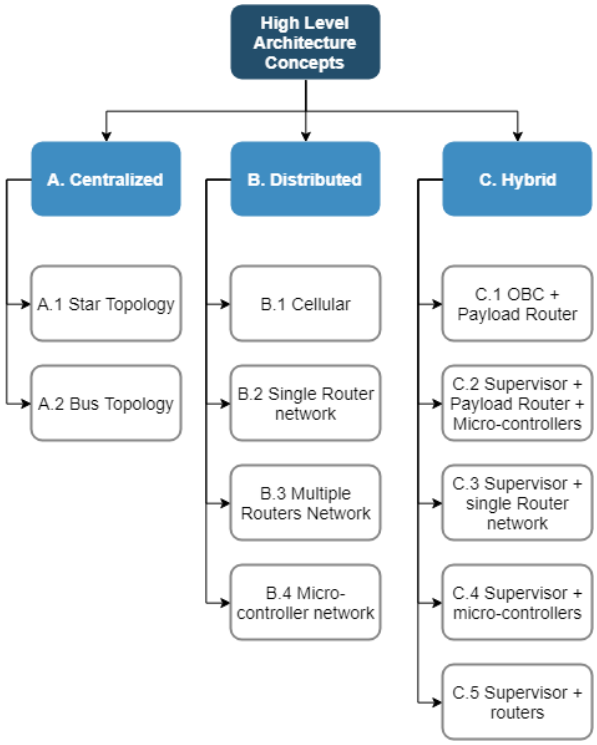


Figure 6.1: High Level Design Discovery Tree

6.1.1. Centralized

For centralized concepts, there is a unit that handles all or most of the systems functions. It is adequate when functionality and interface requirements are reduced. However, when multiple concurrent functions and interfaces are required, a single unit is often not the most adequate implementation due to size constraints.

A.1 - Star topology

In a star topology such as the one of figure 6.2, peripherals are connected to a central unit via point-to-point interfaces. All the functionalities are provided by this unit so it enables high integration and small form factor. Due to those factors, it is the most common topology for nano- and pico-satellites. However, it also brings some disadvantages, most noticeably the limitations in achievable computational power and also the large number of point-to-point interfaces required as the S/C size increases [82].

A.2 - Bus topology

A variant of the star topology that still retains centralized functionality is the bus topology. In this concept, one or multiple data buses connect the electronic equipment to the OBC. This characteristic contributes to a reduction in number of interfaces although it has an extra disadvantage. In this topology, the bus might become overloaded with simultaneous communicating peripherals. In this case, a fast data bus is required with adequate data control to allow priority packets to be sent expeditiously. This topology can be seen on the 10kg Nano-JASMINE, based on the PRISM project from the University of Tokyo [83], in figure 6.3.

6.1.2. Distributed

The distributed branch include concepts where functions are distributed across different units. A particular case is referred to as subsystem intelligence as this usually translates into processing power, in the form of microcontroller or FPGA within each sub-system to enable a certain level of autonomy. Nevertheless, this category also includes concepts where functions that do not require dedicated processing power, such as I/O interfaces or data storage are distributed across dedicated units. This division allows individual units to adapt to specific mission requirements.

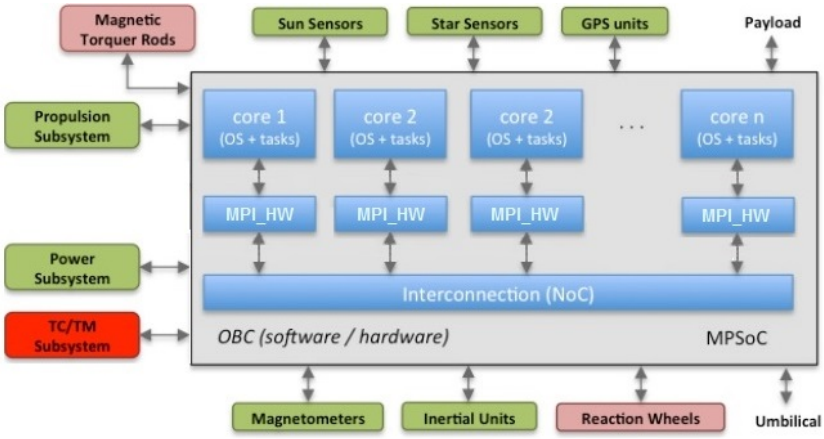


Figure 6.2: **Concept A.1:** Example of a star topology architecture. Notice how each subsystem or component is individually connected to the SoC. Credits: Innovative FPGA

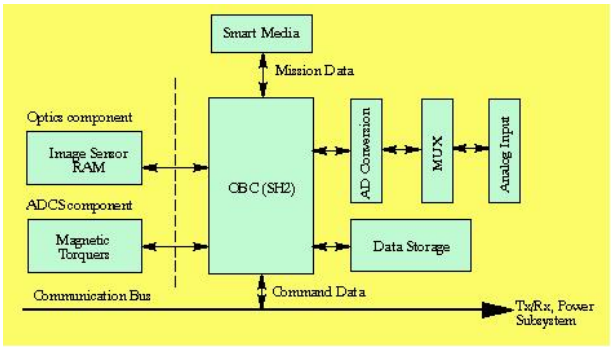


Figure 6.3: **Concept A.2:** In this example of a bus topology, there is a command data bus towards the communications and power subsystems. Credits: Intelligent Space Systems Laboratory at the University of Tokyo, Japan

B.1 - Cellular

Inspired by biological organisms, the multicellullar architecture is a concept put forward by Erlank et al from the Surrey Space Center of the University of Surrey [6]. The research proposes to solve the reliability issue of small satellites by designing identical, fault tolerant hardware blocks that behave and interact as electronic counterparts to multicellular living organisms.

The proposed artificial cell (figures 6.4 e 6.5) is composed of a MCU, the counterpart of a cell macromolecular machinery, FPGAs as proteins for interacting with external devices and a non-volatile memory as the DNA. This 'cell' has internal buses that enable the reconfiguration of the block if an FPGA is faulty, reprogramming the surrounding FPGAs from the non-volatile memory. This method is thought to increase reliability as functionality is recovered when a fault occurs.

An advantage of this innovative concept is the possibility to distribute functions across 'cells' as needed. Since the entire system is composed of identical interconnected cells, it is entirely reconfigurable to fit the requirements at each epoch of the mission. Nevertheless, such concept requires an immense validation effort, although its feasibility as an ADCS controller for CubeSats was demonstrated. Despite the increased reliability in lower operating modes (with the possibility to be further improved by adding 'cells'), it was found to consume approximately 77% more power than an integrated, COTS ADCS solution and predicted to be 30% less reliable than the COTS competitor in its full operating mode after a year of operation [7].

B.2 - Single router network

In order to avoid overloading the data bus(es) and expedite data transfers, a router can be employed to interconnect modules with high speed data transmission requirements. As Jiang et al suggested [82], payloads, storage modules, processing modules and others could benefit from having a centerpiece router as dedicated interface between them (figure 6.6).

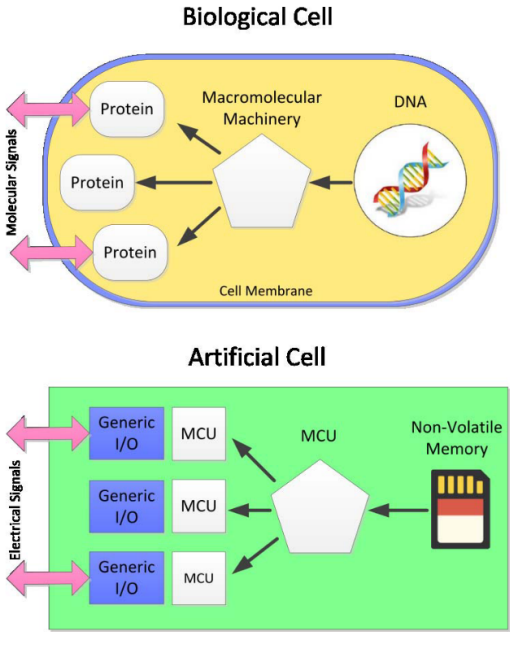


Figure 6.4: Comparison between a conceptual artificial cell (bottom) and a biological cell (top). [6]

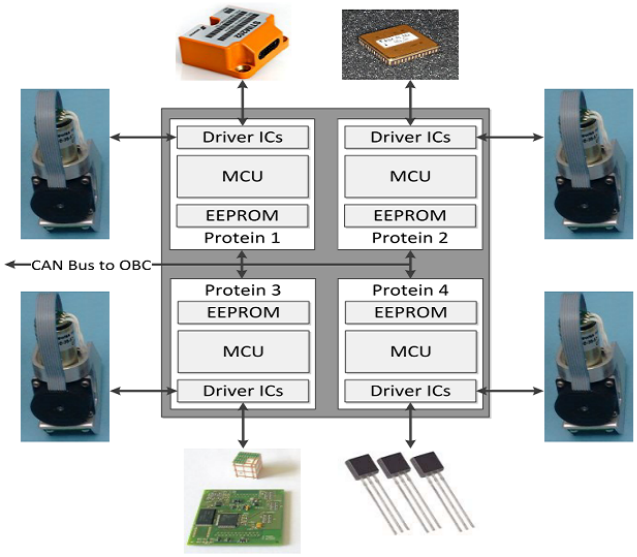


Figure 6.5: **Concept B.1:** Representation of an artificial cell composed of four proteins used on the 3U SME-SAT as an ADCS controller connected to an array of individual components. Credits: Surrey Space Center [7].

This concept adds a layer of complexity, in comparison to a centralized architecture, as a router network is harder to implement and test with limited experiences in space applications [84]. However, it can achieve high data transfer efficiencies as all elements are interconnected via the router.

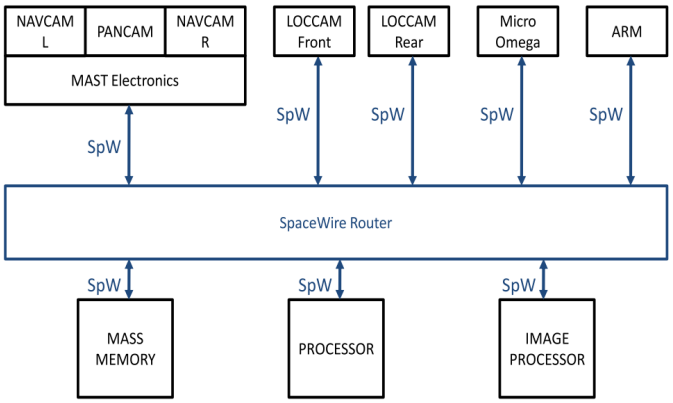


Figure 6.6: **Concept B.2:** ExoMars SpaceWire Data-Handling Architecture composed of a central router that connects all instruments and camera to the processing units and mass memory [8].

B.3 - Multiple routers network

Similarly to concept B.2, it is possible to imagine a concept that utilizes more than a single router [82]. This enables more than one network to be designed according to the needs of the S/C and for those networks to be reconfigured during mission lifetime or in the case of a failure. It also makes it possible to segment subsystems and create a network inside each subsystem, isolating it from a shared bus or network. Such concept is shown in figure 6.7.

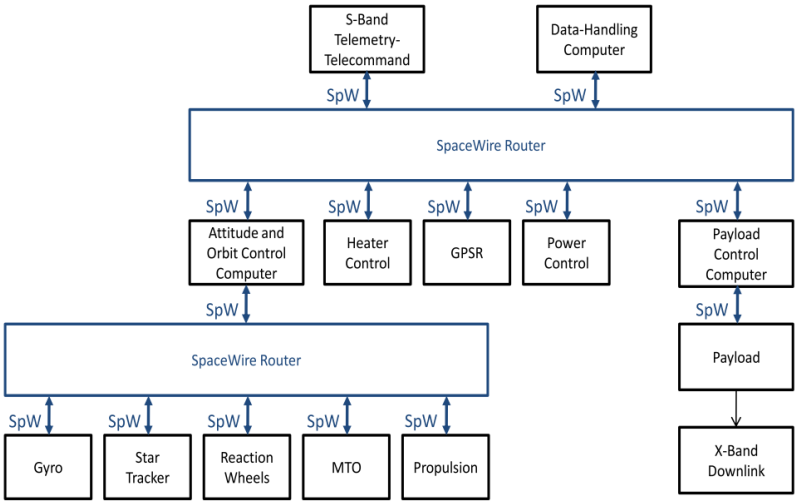


Figure 6.7: **Concept B.3:** ASNARO SpaceWire Data-Handling Architecture. A router connects all the platform electronics whilst a separate SpaceWire network connects the AOCS sensors and actuators to the AOCS computer [8].

B.4 - Micro-controller network

The last distributed concept relies on the use of micro-controllers to provide functionality and interface control between components and sub-systems. Bus or point-to-point connections can be established to and across MCU in order to spread functions and redundancies as required. In this concept, seen in figure 6.8, each MCU is the focal point of the architecture. It enables the design to be similar across subsystems. An example for this architecture is seen on the LUMIO satellite, a 20kg, 12U Cubesat to "observe, quantify, and characterize the meteoroid impacts by detecting their flashes on the lunar farside" [85]. The mission has an AAC Microtec Sirius C&DH unit has central OBC, in addition to two GomSpace processors based on the Zynq 7000 SoC, one as PLIU and the other as AOCS controller.

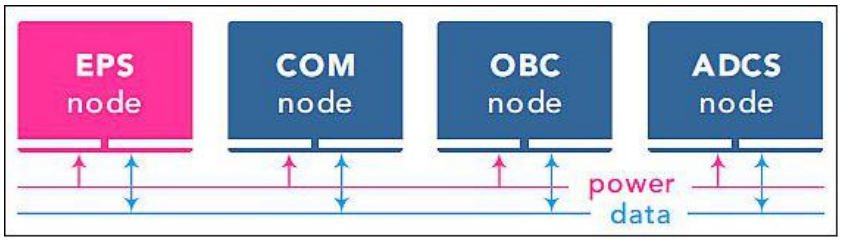


Figure 6.8: **Concept B.4:** Illustration of the main nodes of the TUBiX20 bus. Each node has its own processing power in the form of a μcontroller. Image credit: TU Berlin.

6.1.3. Hybrid

The definition of an hybrid concept is that where functions are not totally distributed across subsystems. Some overarching functions may be concentrated in a unit, namely those functions related to supervisory roles. In this context, a supervisor implements functionalities that directly affect multiple other functions and/or systems such as functional monitoring, reconfiguration, active control of units and/or components.

C.1 - OBC + payload router

For S/C that have multiple payloads generating data, a hybrid architecture might be an interesting possibility. It consists in an added router that creates a network between those payloads and other relevant functional units for faster data exchanges. In the architecture of figure 6.9 for example, a SpaceWire router is used to connect two payloads to a mass memory, computational and communications units. The payload system is therefore isolated from other systems and does not share the same data paths, minimizing its impact on other units. Besides the increase complexity in the design,

it improves efficiency in handling payload data as this is only shared between relevant units. Low and high speed data buses can therefore be created.

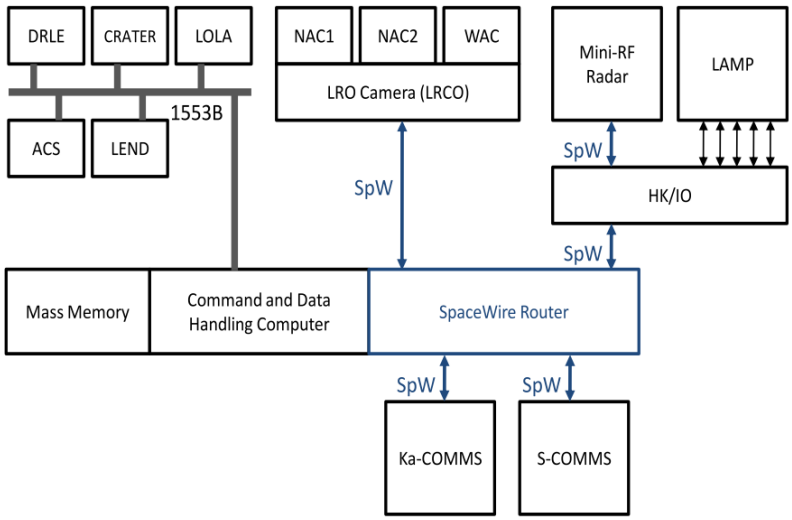


Figure 6.9: **Concept C.1:** Lunar Reconnaissance Orbiter data-handling architecture. In this architecture a router is used to connects the payloads to the command and data handling computer and to the communications systems [8].

C.2 - OBC + payload router + micro-controllers

For those mission where a complex network of systems and payloads are implemented, concept C.2 is a possible architectural solution. A main OBC provides support and control over PLIU. This PLIU has its own computational power and router capabilities in order to interface with a large number of heterogeneous payloads. BepiColombo mission implemented such a concept as seen in figure 6.10.

The benefits of this implementation are more obvious for highly complex scientific missions. In these cases, a router supports and manages digital interfaces to many payloads thus reducing the complexity of a point-to-point interface. However, with I/O capabilities of modern MCU and SoC, a router is unnecessary if the expected number of elements is reduced. Additionally, the variety of interface protocols of COTS AOCS peripherals preclude the use of routers, namely the ones based on SpaceWire, for these functions.

C.3 - Supervisor + single router network

Similarly to B.2, there is a single router has centerpiece of the architecture. It connects both discrete peripherals as well as entire subsystems and units. There is an additional functionality that assures system reliability, mentioned as a supervisor. Although it adds some complexity to the architecture described in concept B.2, this architecture, as put forward by Maqbool [86], is aimed at mitigating SEFIs at a system level. The implementation of this concept, as described by Maqbool is shown in figure 6.11.

C.4 - Supervisor + micro-controllers

Comparable to the previous concept, C.4 is an variant of B.4 where each subsystem has one or multiple MCUs and a central unit has a supervisory role. This can be seen in the system architecture of the KySat-2, where a ”heartbeat monitor” function in the central unit is able to perform hard-resets of the multiple MCUs as a fault tolerance and mitigation strategy, as seen in figure 6.12.

C.5 - Supervisor + multiple routers network

The final concept, C.5 is described as a distributed architecture, with multiple units connected via an array of routers and controlled by a supervisor unit. This allows satellites with a large number of sensors and components to be connected without a significant cabling and mass overhead. An example is seen in the BepiColombo Mercury polar orbiter data-handling as seen in figure 6.13.

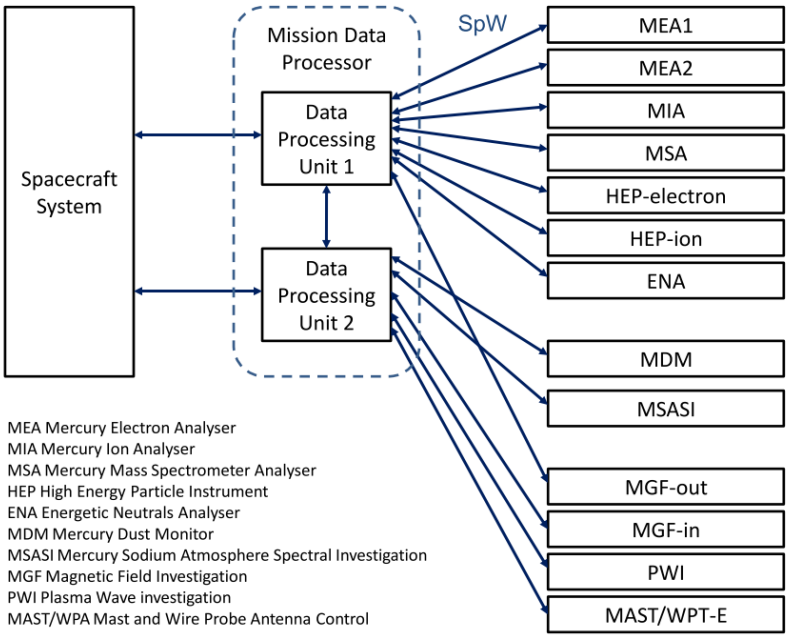


Figure 6.10: **Concept C.2:** BepiColombo Mercury magnetospheric orbiter data-handling architecture. "Each instrument is connected using a point-to-point link to the mission data processor, which contains two data-handling units, each of which contains a central processing unit and a SpaceWire router" [8].

6.2. Concepts trade-off

The aforementioned concepts are a good starting point for the system design. It is necessary to further select a general architecture in order to move on with the design. In this section this selection will be performed by means of direct eliminations and trade-offs, all fully justified. A number of parameters for analysis and trade-off were considered in order to guide the discussion. At the end of this section, the multiple concepts will be reduced to a single most interesting one to be further developed.

6.2.1. Trade-off parameters

The following parameters were considered as the most important ones for this trade-off. The definition and reasoning behind the selection of these parameters is as follows:

- **Innovation:** A thesis project must provide some new information and/or innovation to the field, in this case aerospace, so innovation is an important factor. In particular, a new approach to satellite avionics is to be formulated. Just applying the same concept and design a new avionics system will not suffice. A high score in this parameter is related to a high innovation factor.
- **Innate fault tolerance:** This parameter is related to the level of fault tolerance that can be expected from the architecture. Since high dependability, most concretely availability, is one of the major drivers of the system, it is important to determine from early on if the design concept supports fault tolerance and reconfiguration techniques. A high score in this parameter is indicative of a concept that enables the introduction of elements to increase dependability figures.
- **Complexity:** The complexity of the concept and predicted implementation. An avionics system is, by nature, complex. However, features that increase complexity with minimal benefit make the design more prone to faults and shall be avoided. A high score is indicative of low complexity to benefit ratio.
- **Performance:** It should be forecasted if a concept will be able to match the expected performance considering the usage of commercial technologies. A concept which is thought to

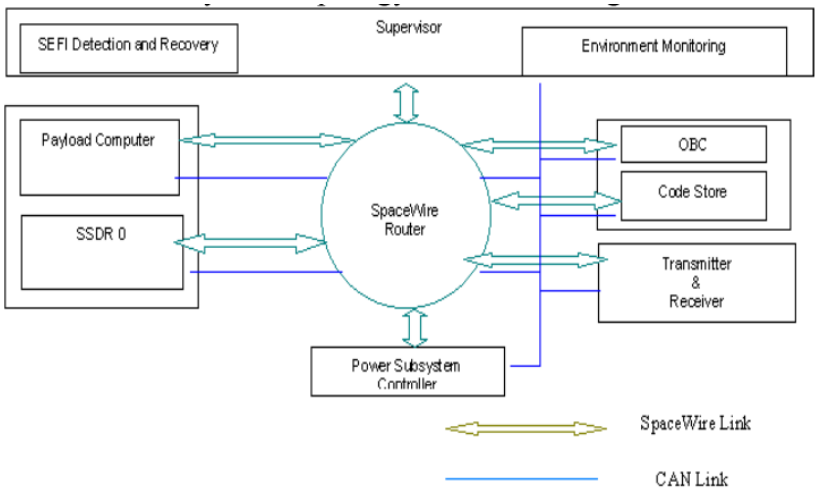


Figure 6.11: **Concept C.3:** System topology where a center router is used to link all units together in addition to a supervisor unit that provides SEFI detection and recovery amongst other functions [9].

negatively affect the overall performance of the system (for example: processing power, data bandwidth, power consumption) will have a lower score.

- **Cost:** This parameter encompasses all costs related to the system. It is mainly affected by the complexity of the system and consequent increased design costs and the level of commercial or space-grade components it requires. A high score in this parameter is a consequence of lower expected costs.
- **Power:** The reference S/C for this system is expected to have either body mounted solar panels or ”wings”. In both cases, available power is restricted so the avionics suite must have a reduced power consumption. A high score in this parameter is related to low power consumption.

6.2.2. Concept analysis

Section 6.1 presented eleven different concepts, organized into three categories. This large set of concepts was compiled with the goal to acquire as enough information to propel the following phases of the project. However, some of these concepts are not useful to be considered in later stages as they do not fulfill the paradigm of the project. Taking that into consideration, seven concepts were promptly eliminated prior to the trade-off process. This signifies that these concepts are thought to be inadequate as main design form-factors. However, some of their principals or ideas can still be applied.

Category A of figure 6.1 presents two concepts based on a centralized architecture. Widely used in CubeSats, where distributed architecture are hard to apply due to the innate SWaP restrictions of the form-factor, centralized architectures are deemed to be inadequate to handle larger, more complex S/C. In particular, a centralized architecture naturally represents a single point of failure which would negatively affect the dependability figures of the avionics suite. A fault of the central OBC has the possibility to cause catastrophic failure of the entire S/C. Not withstanding, the hard performance, dependability and functional requirements imposed in that central unit by this design are against the fundamental ideas and project objective. It is thought that such a design would require a large number of qualified components which would preclude a COTS-based system.

Concept B.1 ’Cellular’ is a futuristic concept from Surrey Space Center. The distributed architecture is inspired in the resilience of nature, from which one is expected to learn a lot on highly reliable systems. The results presented so far are mixed, showing some increase of reliability at the expense of increased power consumption and complexity [7]. This original idea should, therefore, continue to be pursued by the same researchers as any work performed by this thesis would hardly add any significant contribution to the scientific community. For those reasons it was decided to not pursue this concept.

Concepts considering the use of routers as design centerpiece were eliminated due to a number of factors. First, the lack of heritage in small satellites. This would make it difficult to perform any validation by similarity and would require an entire new approach as a thesis project. Second, the use of

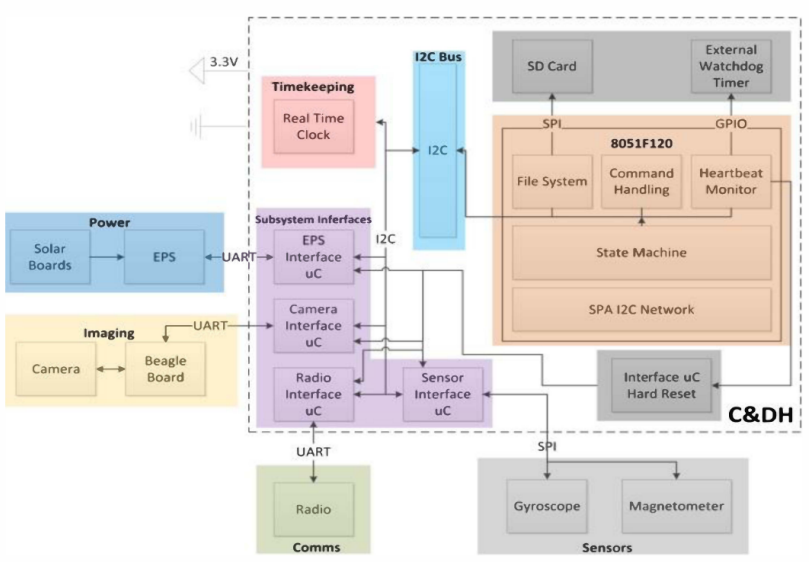


Figure 6.12: **Concept C.4:** A distributed architecture where a supervisor function is incorporated. The architecture of Cubesat KySat-2 seen in the figure applies this concept through a "heartbeat monitor" function [10].

routers requires additional hardware and software design in addition to becoming single points of failure of the design. SpaceWire routers are the most common application of routers in space applications. However, multiple interfaces besides SpaceWire, including analog signals, are to be expected, which are not compatible with router networks. Hence, concepts B.2, B.3, C.3 and C.5 were eliminated.

Following these considerations, four concepts remained, B.4, C.1, C.2 and C.4. These will be trade-off against each other in order to identify the most promising concepts and ideas for further development. The following paragraphs present the most noticeable upsides and downsides of each concept.

B.4 - Micro-controller network

- **Upsides:** This approach allows for all modules to be interconnected via one or more buses. It is a rather simple implementation where functions are distributed so SPOF are not so remarkably present. Component costs are also reduced due to the wide variety of commercial products to choose from.

- **Downsides:** Designing a data bus with a large number of nodes poses hard implementation problems related to signal propagation, line reactance, clock jitter besides other issues.

C.1 - OBC + payload router

- **Upsides:** From a high level perspective, this concept is a payload focused one, where the avionics is design around a central payload and its needs. The dedicated network for payload data allows easy flow of large amounts of data.

- **Downsides:** In addition to the cost inherent to router networks for space, more complexity is expected in order to design the other data connections for non-payload related functions.

C.2 - OBC + payload router + micro-controllers

- **Upsides:** As the central unit of concept C.1 is replaced by a supervisor and micro-controllers, some benefits are introduced and downsides removed. In particular, the benefits of the distributed architecture are brought back from concepts B with the addition of a centralized supervision that supports fault tolerance and handling.

- **Downsides:** Following the analysis of concept C.1, the SPOF in the router and "chicken and egg" problems are maintained. However, the SPOF in the OBC is eliminated. Adding the supervisor as an extra node in the system may also contribute to complexity and cost parameters.

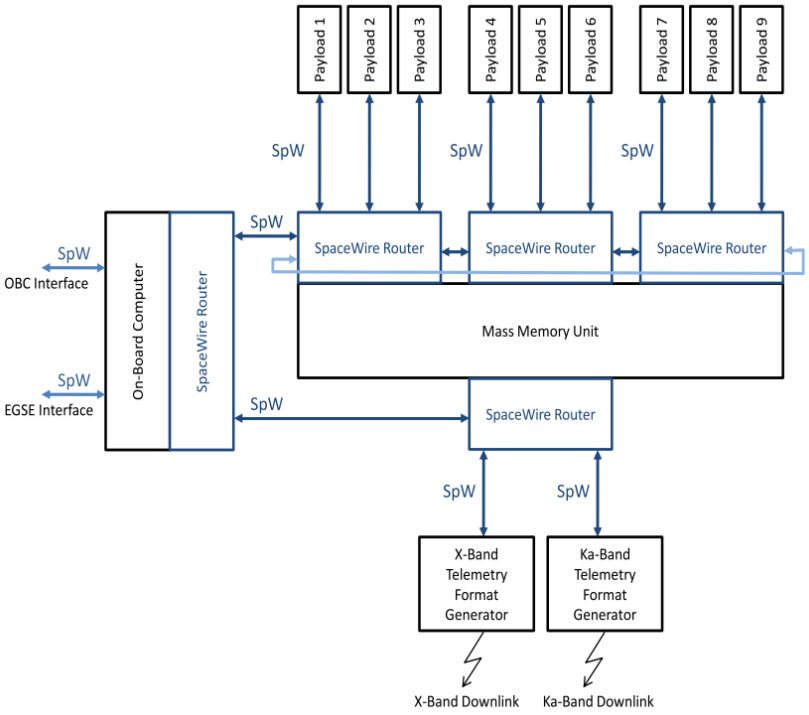


Figure 6.13: **Concept C.5:** BepiColombo Mercury polar orbiter data-handling. A shared memory unit is linked to 9 payloads and two downlink systems via 4 routers. Additionally, an OBC commands and supervises the operation of the payloads. [8].

C.4 - Supervisor + micro-controllers

- **Upsides:** Supervised micro controllers allows distribution of functions across multiple components and interconnection between them. A centralized supervisor can also improve dependability without major overhead.

- **Downsides:** A dependable supervisor is required in order to improve the dependability of its adjacent systems. Hence, qualified components are to be expected which add significant cost penalties.

6.2.3. Pugh matrix

A Pugh matrix was selected as an effective tool to visualize and review the analysis described in the previous paragraphs. As seen in figure 6.14, the parameters/criteria described in 6.2.1 are placed on the left side and a weight factor from least important, 0, to most important, 10, is attributed to each one. For each concept/criteria combination, a rating from 0 to 10 is given, with lower scores representative of negative contributions and higher score positive contributions as explained in 6.2.1. The rating multiplied by the weight factor gives the 'weighted' score which, summed with all other 'weighted' scores of each concept gives a final score. The final scores are seen on the bottom of the figure. A higher score is therefore representative of a more adequate concept. A color scale for the 'weighted' score and another for the total score is also implemented to quickly visualize the upsides and downsides of each concept and also the most and least adequate concepts. Red represents low scores and green higher scores, with intermediate values in shades of yellow and orange.

From figure 6.14 it is seen that concept C.4 'Supervisor + Micro-controllers' is the one with the highest score on the Pugh matrix. Despite the low score on complexity due to the fact that it integrates multiple micro-controllers and an additional supervisor, which poses design and qualification overheads, it is expected to have good performance and innate fault tolerance. The use of multiple controllers allows wide functional allocation to improve performance and efficiency at the same time that a supervisor ensures dependability. Therefore, this concept will be used as a basis for the proposed high level design in the following section.

Pugh Matrix									
Criteria	Concepts	B.4 - Micro-controller Network		C.1 - OBC + Payload Router		C.2 - Supervisor + Payload Router + Micro-controller		C.4 - Supervisor + Micro-controllers	
	Weight factor	Rating	Weighted	Rating	Weighted	Rating	Weighted	Rating	Weighted
Innovation	6	4	24	5	30	8	48	6	36
Innate Fault tolerance	6	6	36	3	18	7	42	8	48
Complexity	2	6	12	6	12	4	8	4	8
Performance	7	9	63	8	56	7	49	8,5	59,5
Cost	6	5	30	4	24	2	12	3	18
Power	5	3	15	7	35	3	15	4	20
	Total Score		180		175		174		189,5

Figure 6.14: Pugh Matrix for high level concept trade-off. Notice that concept C.4 is the one with the highest score, followed by B.4, similar concept but without a supervisor. The highest contribution for the trade-off is in the form of the performance parameter, since it has a high weight and high score for this concept.

6.3. Proposed high level concept

Following the results of the Pugh matrix (figure 6.14), a decision to pursue concept C.4 was made. The high level analysis, high level requirements and a preliminary FMECA analysis (see annex B) guided the design of the proposed concept. Visible in figure 6.15, this is the baseline design that will guide the creation of more specific requirements and the detailed design of the system.

The proposed concept is based on a distributed architecture. It is constituted by a power supply and distribution unit, a supervisor and redundant OBC and PLIU boards. The PSDU is responsible for supplying the avionics suite and connected peripherals with regulated power lines, derived from an unregulated 28V supply from the main S/C power unit. Embedded in the PSDU is a supervisor, based on a reasonably priced rad-hard microcontroller [1], that oversees the status of nominal and redundant OBC and PLIU. From the preliminary FMECA analysis it was concluded that functional monitoring of the avionics was required in order to achieve the dependability goals. For that reason, a supervisor unit inside the PSDU is considered in order to implement FDIR solutions. At the highest level, the supervisor is able to detect anomalies in the behavior of the system and provide, besides other actions, timely activation and contextualization of the redundant units. In addition, redundant units for the OBC and PLIU were selected as fault recovery methods in both first and lower levels procedures.

The OBC unit provides three functions: C&DH, TM/TC and AOCS. The nature of these functions allows them to be clustered in a single unit, possibly powered by a single SoC. The unit also provides the necessary interfaces for these functions.

The PLIU is responsible for handling of the payload(s) via the required interfaces. It controls the payload, pre-processess the observation data and stores it in a non-volatile memory. One or a combination of data processing chips (SoC, DSP or ASIC) are expected to be utilized. The OBC and PLIU units can be connected (blue line) if deemed necessary in later stages of the design . [2]

6.4. Conclusions

In this chapter, a number of high level concepts for the avionics system were described, traded-off and finally one was selected. The research put into compiling multiple concepts allowed for an overview of the existing solutions employed in satellites and also concepts proposed for the future. Some concepts, such as the ones involving routers were concluded to be too expensive both in terms of complexity and component cost to be adequate to this paradigm. Additionally, a supervisor unit was found to be required to achieve the high availability whilst maintaining the COTS, cost-effective paradigm. For the completion of the Pugh matrix, a thorough reflection of each concept was required,

[1] At this stage of the design process, the intent is to use one of the microcontrollers in A.4.

[2] From this point onward, the multiple functions of the avionics (C&DH, AOCS, PLIU, Supervisor, PSDU, TM/TC) are mentioned as *avionics subsystems* for clarity. Note that this is an internal sub-division of the avionics and it is distinct from S/C subsystems.

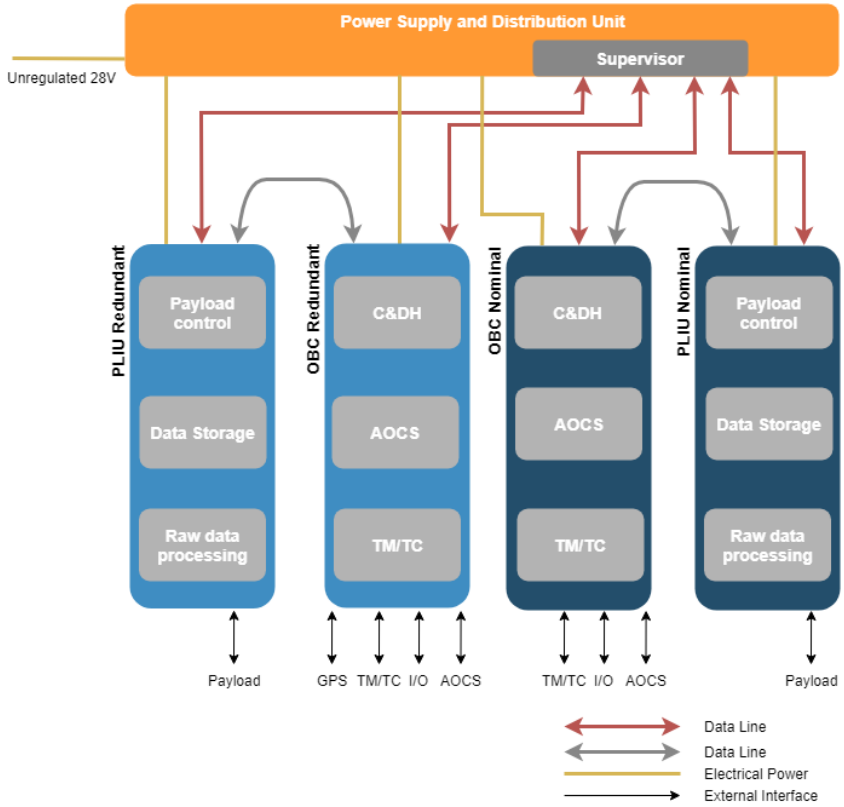


Figure 6.15: Proposed high level architecture.

which gives confidence on the suitability of the proposed concept. This proposed concept sets a baseline design to build upon on the following chapters and will be followed until the end of the thesis.

Innovation in the concept of figure 6.15 is related to the integration of all the mentioned functions inside a single avionics suite. The concept derives ideas and functionalities from larger, more expensive spacecraft, such as reconfigurable redundant units and powerful payload interface unit, whilst empowering solutions utilized in CubeSats namely the condensation of functions in a single MCU with all the required connectors under a single casing. To the aware of the author, such a system target at 50kg to 200kg satellites is not yet available.

7

System requirements

This chapter is dedicated to the definition of system requirements. This will be accomplished with the help of functional flow block diagrams and interface control documents for peripherals when necessary. These requirements will improve the understanding of the system to be designed and allow for verification at the end of the project.

The chapter is divided into sections that represent the subsystem for better readability. A description of the requirements for each section is given whilst a full requirements list is provided in annex C.3. Said requirements are analyzed to determine key, driving and killer requirements.

At the end of this chapter, the reader shall understand the requirements of the avionics unit and their impact on the system design. This represents the last phase before the actual design process begins.

7.1. AOCS

The AOCS subsystem interfaces with a selection of mission dependent peripherals according to their specificities, by converting their output data into a signal readable by a micro-controller and producing a control signal according to the available interfaces of the peripheral. Additionally, for some devices it is also necessary to supply power although the design of this functionality is out of scope for this thesis. The most relevant AOCS high level function to be further analyzed is related to the control of peripherals as in requirement HLR-A02. The functional flow diagram is seen in 7.1.

An analysis of the AOCS subsystems in representative spacecraft (n=10) was performed in order to support the requirement definition process (see annex A.3).It presents the type, number and interfaces options of AOCS peripherals expected for EO applications. The variety of interface protocols is noticeable both inside and between spacecraft. The proposed system is expected to cope with this variety with low recurrent engineering efforts. For that end, a variety of AOCS peripherals was compiled and analyzed (see annex A.2) in order to improve understanding of these issues. Peripherals from A.2 were selected in the basis of their applicability and availability of interface control documents (ICD) as use-cases. The selected components are:

Sun sensor

Solar MEMS SSOC-A60

The 'Sun Sensor on a Chip A60' from Solar MEMS is a two-axis, low-cost analog sun sensor for high precision applications. It consists of four photodiodes, each generating an analog output, plus a ground line. A digital version with RS-485 outputs is also available. It was selected for being a flight-proven COTS device targeted at cost-effective small satellite applications with available documentation online. Each satellite is expected to have four of these devices [87]. As seen in A.2, analog sun sensors are still common, posing particular signal conditioning requirements.

Star tracker

TERMA T1

The T1 optical heads and electronics units are star trackers designed under ESA contract for high

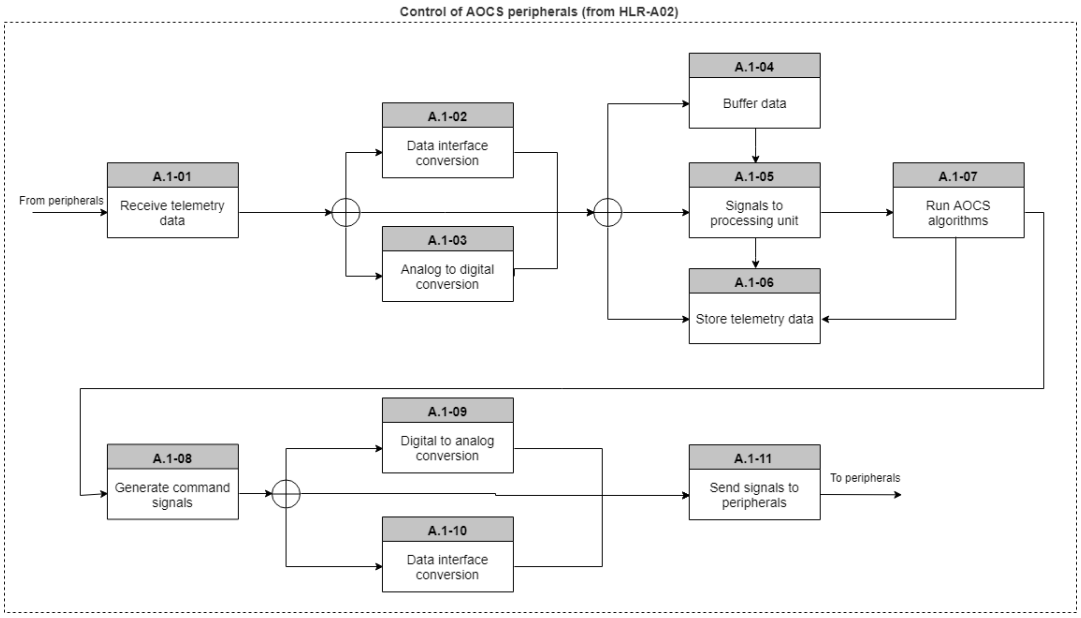


Figure 7.1: Function flow of the control of AOCS peripherals. The circle with cross symbol in the diagrams represents a logical "OR".

reliability and low recurrent costs. The two devices offer SpaceWire interfaces to the S/C platform. If only the optical head is installed, captured images are directly sent to the S/C's OBC. The electronic unit, when installed, makes use of a LEON3-FT processor for autonomous attitude determination. The T1 star tracker suite was selected since it provides SpW interfaces and due to the fact that it represents the possibility of the S/C owner to select either autonomous or non-autonomous star trackers thus requiring star tracking at the OBC [88]. It is expected that two star trackers heads are present in the S/C.

Reaction wheels

Sinclair Interplanetary RW3

A reaction wheel for small satellites with built-in speed, torque or current control can be found in the RW3. It has flight heritage with 44 units in orbit since 2016. Its ICD provides valuable information for the definition of requirements for general reaction wheels. The device can be found with two RS-485 pairs which may be used as two half-duplex 2-wire buses, or used together as a 4-wire bus. One of the RS-485 pair may be exchanged by a CAN bus. The device as an operating range between 20V and 36V [89]. It is common to use four reactions wheels per satellite, using similar RS-485, RS-422 or CAN interfaces, as seen in A.2.

GNSS

GPS-601

GNSS modules are utilized for navigation purposes in LEO satellites handling the RF-front end before outputing position, velocity, time and PPS signals. The GPS-601 GNSS receiver from SpaceQuest is a flight proven design that tracks GPS, GLONASS, Galileo and BeiDou constellations to provide such outputs. Data interface is via serial RS-422 or CAN ports, and sync and reset signals via LVTTL I/Os. The expected data rate is below 1Mbps [90]. Other devices in A.2 were found to have similar functionality and interface options.

Magnetorquers

Sinclair Interplanetary TQ-40

A generic magnetorquer consists in a copper wire coil around an open or ferromagnetic core that produces a magnetic dipole varying with the flowing current. In the case of the TQ-40, a $40Am^2$ dipole can be achieved. To control the current, a driving circuit taking a pulse-width-modulation (PWM) signal is employed. Sinclair Interplanetary offers the TQ-40 with H-bridge or current control circuits controlled

over a CAN or RS-485 bus, or without any driving electronics [91], much like other manufacturers. Both options shall be supported. Three magnetorquers are expected.

Magnetometers

New Space System NMRM

This magnetometers provides x, y and z-axis magnetic field component measurements. It contains all sensing, analog to digital conversion and processing features required to produce an digital measurements of these components over a RS-485 output. It is powered by regulated 5V DC supply. Analog outputs are also a possibility to be considered.

Fiber optic gyroscopes

Honeywell GG1320AN

Fiber optic gyroscopes are used in space applications for their reduced sized and high accuracy. The GG1320AN from Honeywell is a ring laser gyro that returns a frame of data containing gyro status and angle when it receives a sampling pulse. This rate of sampling is, therefore, determined by the user and, according to its ICD, the maximum guaranteed sample sample frequency is 1.6 kHz for the GG1320AN1X gyros and 5 kHz for the GG1320AN2X gyros. When not pulled, the serial output port is set on tri-state, allowing a pseudo-multipoint configuration on RS-422. The data is then provided at 1 Megabaud which is similar to competitors. The instrument is powered by a 15V and 5V regulated power supplies [92].

7.2. TM/TC

The TM/TC functions of the avionics are responsible to provide the interface between the RF front-end equipment and the satellite (data link layer or layer 2 of the OSI model [93]). A survey of satellite RF-units (transceivers, transmitters and receivers) concluded that these units work on the physical layer which includes signal modulation/demodulation, signal generation, mixing/demixing and power amplification. Although some units, in particular for micro-satellites, include layer 2 features, such as data packetization and encoding, the avionics system is focused on these data link layer processes.

Two functional diagrams were created to better understand the requirements applicable for this functions. In figures 7.2 and 7.3 the functions related to telecommand and telemetry are described, respectively. For clarity, a distinction is made between data before and after data link layer protocols have been applied. Data flowing from the RF unit is transformed from uplink data into telecommands as it is processed in the avionics. For outflowing data, it is transformed from telemetry data into downlink data as layer 2 protocols are applied. In the cases where layer 2 protocols are applied in the RF front-end, telemetry can flow directly to the RF unit. The inverse happens for telecommands.

7.3. Payload interface

The interfaces and functions related to the payload(s) are extremely important in the context of this system since it is directed to EO applications. For that reason, two high level functions were selected to be further analyzed in order to establish requirements. In figure 7.4, the gathering of payload telemetry is distilled into multiple functions that need to be accomplished namely receiving, processing and storing of data of multiple formats. Additionally, the control of the payload(s) is also reviewed since it involves multiple steps related to the generation of commands, storage of those commands as housekeeping data and correctly interfacing with the payload's data input lines (figure 7.5).

There are two payloads to be considered. Both require one or more LVDS interfaces for high speed data transfer. There shall be at least 3 LVDS interfaces in the system for payload data. This raw data shall then be pre-processed or stored in non-volatile memory. The level of pre-processing, either by applying compression algorithms, clever image processing techniques or others shall be supported and is mission-dependent. Non-volatile memory size is also mission dependent and shall be at least 64GB. The system shall also control the payloads and this is expected to be achieved via a CAN bus and two discrete commands. It shall be possible to substitute the CAN bus by other serial interface without much overhead.

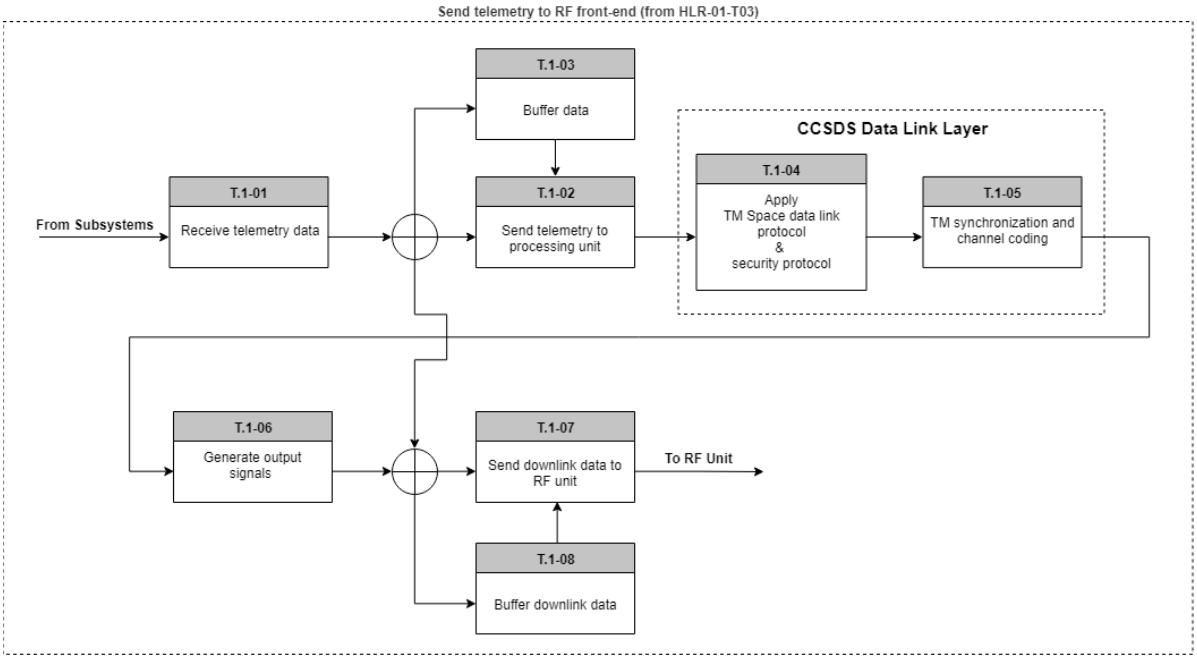


Figure 7.2: Functional flow for telemetry data.

7.4. C&DH

The command and data handling subsystem is responsible for the general operation of the satellite and schedule on-board tasks. Since its tasks are more easily defined, no functional diagram was deemed necessary to complement the requirement definition. It is however important to stand out that the C&DH is also responsible for handling general I/O's that do not fit the other subsystems and also for the collection of relevant telemetry to operate the S/C operating system.

7.5. Supervisor

As mentioned in the previous chapter, a supervisor subsystem, embedded inside the PSDU is expected in this avionics architecture. This subsystem implements FDIR policies for dependability assurance so it requires functional and fault mode analyzes in order to be correctly designed. A functional diagram (figure 7.6) visualizes some of the supervisor functions. This will help to understand how it operates, what interfaces to establish and support some requirement definition. Since the supervisor functions are complex and highly dependent on the general architecture of the avionics, it is expected that this subsystem will gradually evolve as the avionics is developed.

7.6. Non-functional

Non-functional requirements were kept constant to the ones defined in 5. The ones that are expected to have a greatest impact on the system design are the ones related to RAMS. Interface number and protocol were consolidated.

The consolidation of system interfaces shows what are the peripherals connected to the avionics. It hints at the positioning of the avionics as the core of S/C. Figure 7.7 is the result of this exercise.

7.7. Requirement analysis

Following the definition of system requirements it is clear by this point the functions and main characteristics of each subsystem. A reflection on the written requirements enables a better understanding of the system as a whole and subsystems in particular. Moreover, the identification of critical requirements provides guidance for the design stage of the next chapter.

A selection of system requirements will be presented as the key, killer, and driving requirements, much like previously performed for high level requirements.

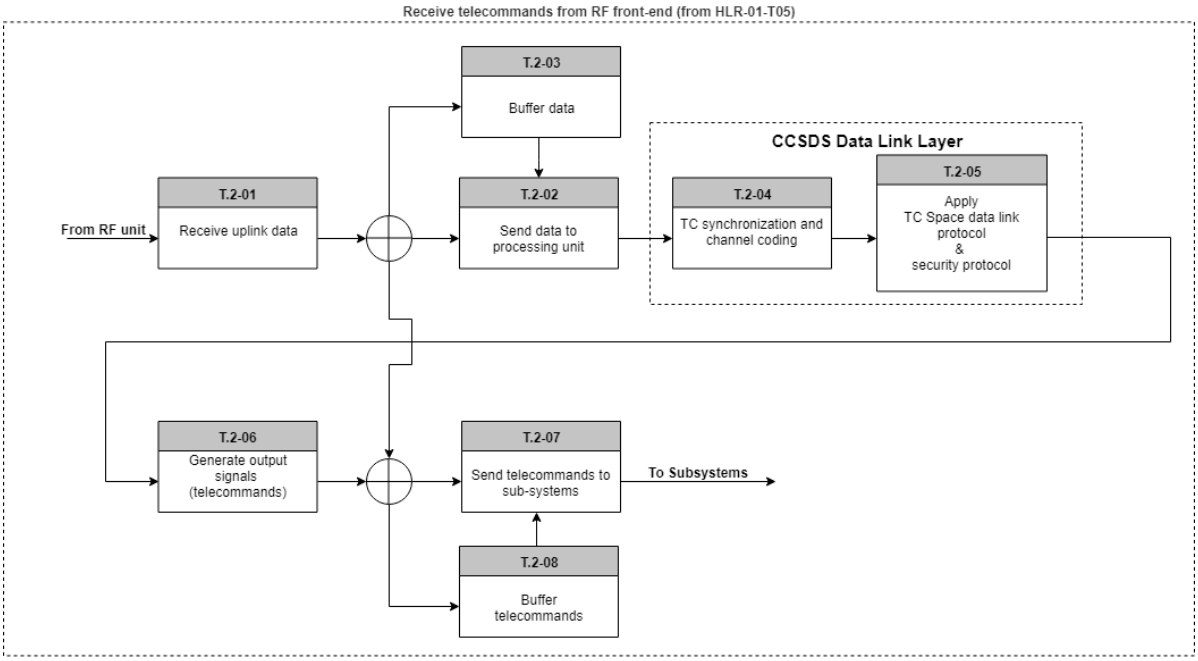


Figure 7.3: Functional flow for telecommands.

The **key requirements** identified and their reasoning are:

- **SR-O01:** The combination of PLIU for EO payloads, TM/TC, C&DH, I/O and AOCS functions in a single system is the answer to research question 1.
- **SR-O11:** By designing an avionics system tailored to EO small satellite missions, recurrent engineering costs and integration efforts are reduced. (Research question 2)
- **SR-SP01:** One of the protections that was found to achieve availability was the supervisor. (Research question 3A)
- **SR-O02:** To add to the supervisor, redundant boards will allow functional redundancy and enable high availability. (Research question 3A)
- **SR-SP02:** The use of space qualified components in the supervisor is necessary to achieve the RAMS figures. (Research question 3B and 3C)
- **SR-O12:** Using COTS parts outside the supervisor functions allow for cost savings whilst maintaining high availability. (Research question 3B and 3C)
- **SR-R04:** The availability goal is 99.9% throughout the mission lifetime of five years. (Research question 4)

In turn, the **driving requirements** are:

- **SR-A01:** A large number of peripherals impose design challenges in the number of interfaces.
- **SR-T02:** As the downlink data is expected to be large, this can be a resource consuming feature.
- **SR-P06:** Since the system is targeting EO missions, the payloads will generate large amounts of data which demand unique computational resources.
- **SR-SP12:** The ability to supervise and control each board requires dedicated internal interfaces and components.
- **SR-R04:** The goal of 99.9% availability is driving every design choice.

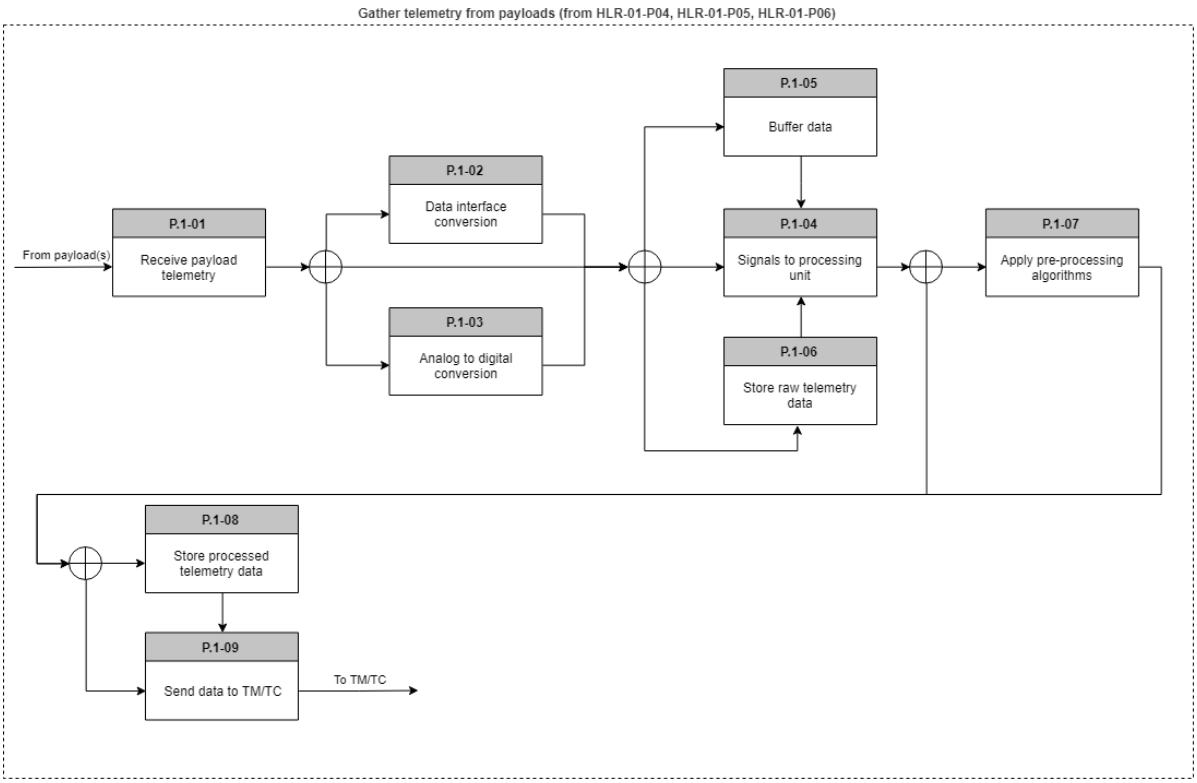


Figure 7.4: Functional flow of payload telemetry collection.

- **SR-O07:** All design choices and safety features should always consider fault containment.

Finally, no particular **killer requirements** were identified as it is thought that current technology and appropriate design methods are able to meet all requirements.

7.8. Requirement verification

At this stage of the project, it is expected that review of the design is the preferred verification process. Other designs and literature will be utilized to verify the design by similarity. Radiation analysis is another method employed to verify non-functional requirements.

7.9. Conclusions

The chapter presented the reader the process utilized to generate more detailed system requirements and the results of that process. Functional flow diagrams were extensively used to better understand the expected functions. Further research into AOCS peripherals lead to particular understanding on the commonalities and differences between components. It shows that the avionics shall support multiple configurations according to the selected interfaces for AOCS peripherals. A variety of functions were found for the supervisor unit which improve its contribution to the entire system.

Non-functional requirements did not suffer any alterations from the previously defined High level requirements of chapter 5. Nevertheless, a consolidation of the system interfaces was performed, leading to a visual representation which guides further developments.

Key, driving and killer requirements were also identified. The key requirements are largely related to the suitability of the avionics to multiple LEO missions and availability whilst employing COTS components. The most significant driving requirements are related to the challenges associated with the complexity of interfaces the system provides. No killer requirements were determined. Verification of requirements is expected to be performed via verification of the design, similarity with literature or other products or analysis of radiation effects.

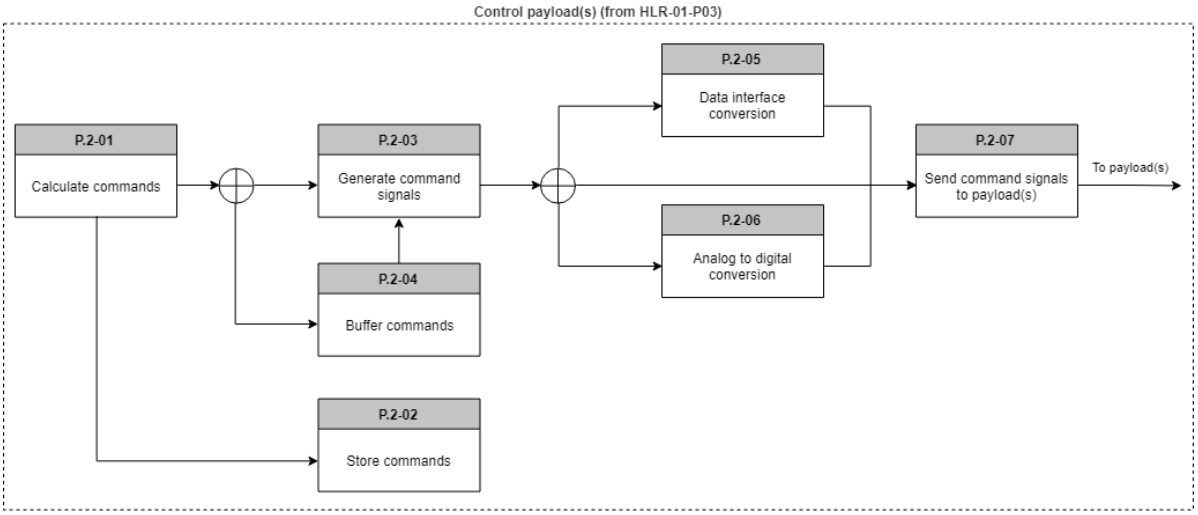


Figure 7.5: Functional flow diagram of payload control.

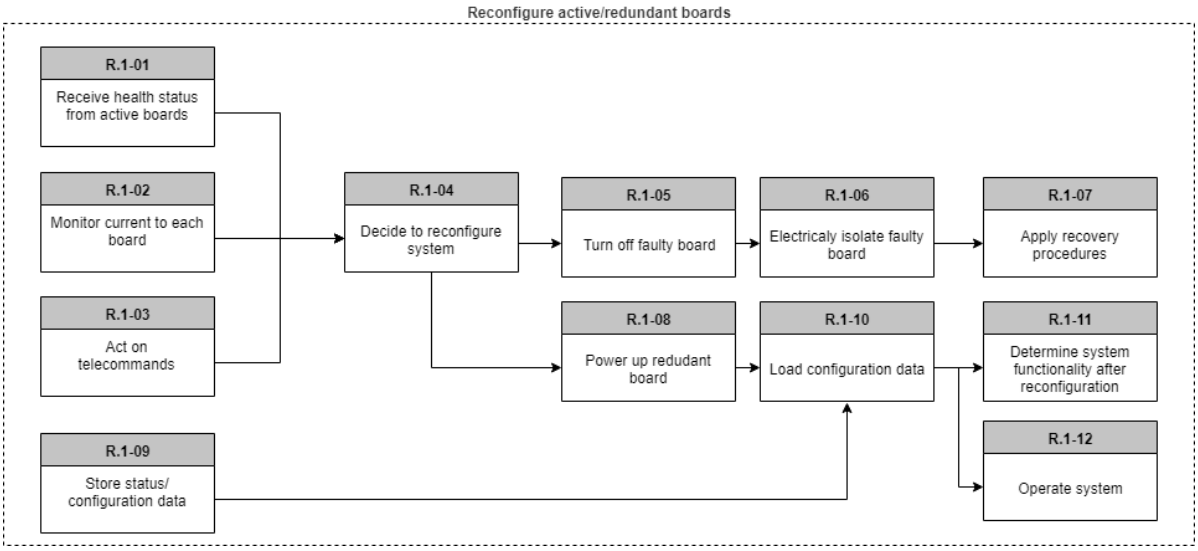


Figure 7.6: Functional flow diagram for the supervisor subsystem.

Following this last project definition stage, the design process can begin. The functional architecture is presented in the next chapter.

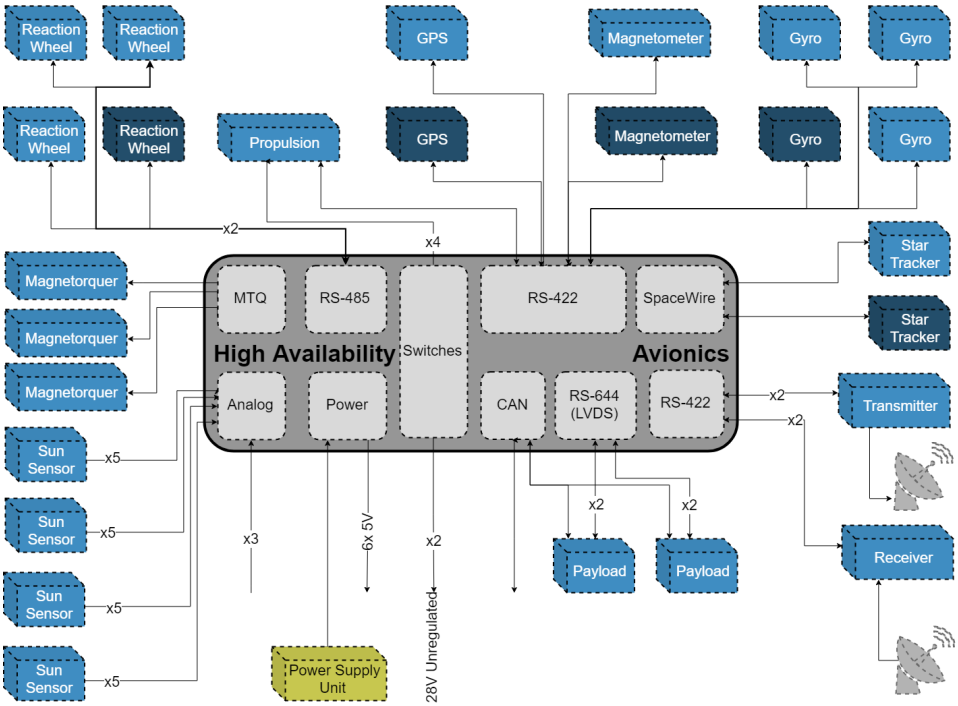


Figure 7.7: Interfaces between the proposed avionics system and other S/C peripherals.

8

Functional Architecture

The definition of the functional architecture is an important step in the design process with particular implications in hardware allocation and dependability issues. This chapter presents a functional architecture that strives to maximize the systems dependability figures and modularity by means of linked functional blocks.

In order to improve the overall quality of this exercise, the SAVOIR reference architecture was used. This guided the definition of functional blocks whilst standardizing the design, improving readability and clarity when comparing the proposed system with other systems. A basic introduction to the SAVOIR reference architecture is made, followed by three possible configurations for the avionics systems. These are compared and traded-off to reach a final configuration which becomes the basis from which a physical design can be developed. The implications of said choice are discussed.

This chapter is the first step into the design of the avionics units. It presents the first detailed internal view of the system architecture at a functional level. At the end of the chapter, the reader is expected to understand the functional configuration of the avionics units and its implications.

8.1. SAVOIR reference architecture

SAVOIR stands for Space Avionics Open Interface aRchitecture and its an initiative to improve the quality of European space avionics systems by agreeing on a set of well defined specifications based on a reference architecture. The functional reference architecture is supported by an overall view of avionics functions and their interconnections, redundancy schemes, and possible hardware allocations. It covers both platform avionics as well as payload interface units. The SAVOIR advisory group includes some of the most important names of the European space avionics communities such as ESA, CNES, DLR, Airbus Defense and Space, RUAG amongst others. System designers are expected to reduce recurrent engineering costs and associated schedule risks, improve the competitiveness of their products, improve interchangeability and interfacing with other systems by following the SAVOIR reference architecture and specifications. [94]

This reference provides guidance for this thesis project as it informs and guides the development of the functional architecture. Following the SAVOIR guidelines ensures the functional completeness of the project without compromising innovation therefore improving its quality. Furthermore, it improves readability and understanding between engineers since schematics are traceable to a standard. For these reasons, the ”SAVOIR Functional Reference Architecture” (document SAVOIR-TN-001) is used as a standard for the definition of functional blocks, data messages and development of schematics.

8.1.1. Functional blocks

It is essential that the functionalities of a system be clearly and thoughtfully described. SAVOIR defines a set of functions to be provided by the spacecraft avionics which are also considered for this project. These are more precisely divided and described than the previously mentioned functions (named AOCS, TM/TC, PLIU, C&DH and Supervisor) but represent the same functionalities. The following is an excerpt from SAVOIR-TN-001 and described the functional building blocks of SAVOIR:

- *Telecommand reception, decoding and distribution.*

- *Security function that protects the spacecraft from receiving unauthorized commands and that provides optional decryption and encryption of data sent on the TM/TC link. Optional function.*
- *Telemetry Transfer Frame generation and coding.*
- *Essential TM function, collecting essential data and generating data packets for the TM Encoder. Optional function.*
- *Essential TC function, distributing pulse commands to control vital spacecraft functions.*
- *Parallel I/O to support the acquisition of discrete essential spacecraft data.*
- *On-Board Time management, providing a time counter and generating synchronisation events.*
- *Platform Data Storage function for storage of data needed for the spacecraft operation.*
- *Safeguard Memory function for storage of vital spacecraft data that is needed by the processing function.*
- *Reconfiguration function that maintains the operation of the processing function even in case of errors.*
- *Processing capability to store and execute Execution Platform and Application software.*
- *Communication, separated into Mission Data and Cmd & Ctrl communication systems, allowing the processing function to communicate with platform sensors and actuators and with the spacecraft payload.*
- *Data Concentrator function for handling the monitoring of spacecraft sensors.*
- *Sensor and Actuator Interfaces for interfacing the physical sensors and actuators.*

The following payload functions described in SAVOIR are also considered in the design:

- *Payload data routing function for routing monitoring and control communication to and from payload units.*
- *Payload Data Storage function, for storage of payload TM data during periods of no ground station contact. Optional function.*

8.1.2. SAVOIR functional architecture

In figure 8.1 the SAVOIR functional diagram with typical hardware mapping is presented. It is seen how the OBC supports most of the functionality with a RTU supporting the interface between sensors, payload and platform. The diagram also presents the suggested redundancy schemes for each function. It is interesting to notice the separation between payload functions and platform functions. As it was seen in chapter 4.4, payloads for Earth observation are diverse in terms of functionality. Therefore, the diagram suggests an implementation of these functionalities outside of the OBC. Additionally, the RTU handling IOs is also developed outside the OBC for better adaption to each mission. The proposed avionics system shall incorporate all of these functions into a single product.

8.2. Proposed functional architecture

Following the presentation of the SAVOIR architecture and the main functions of satellite avionics systems, it is possible to design and iterate until a functional architecture of the system is achieved. This section presents possible configurations of these functions and a final configuration is presented as the building block from which the physical architecture will be designed.

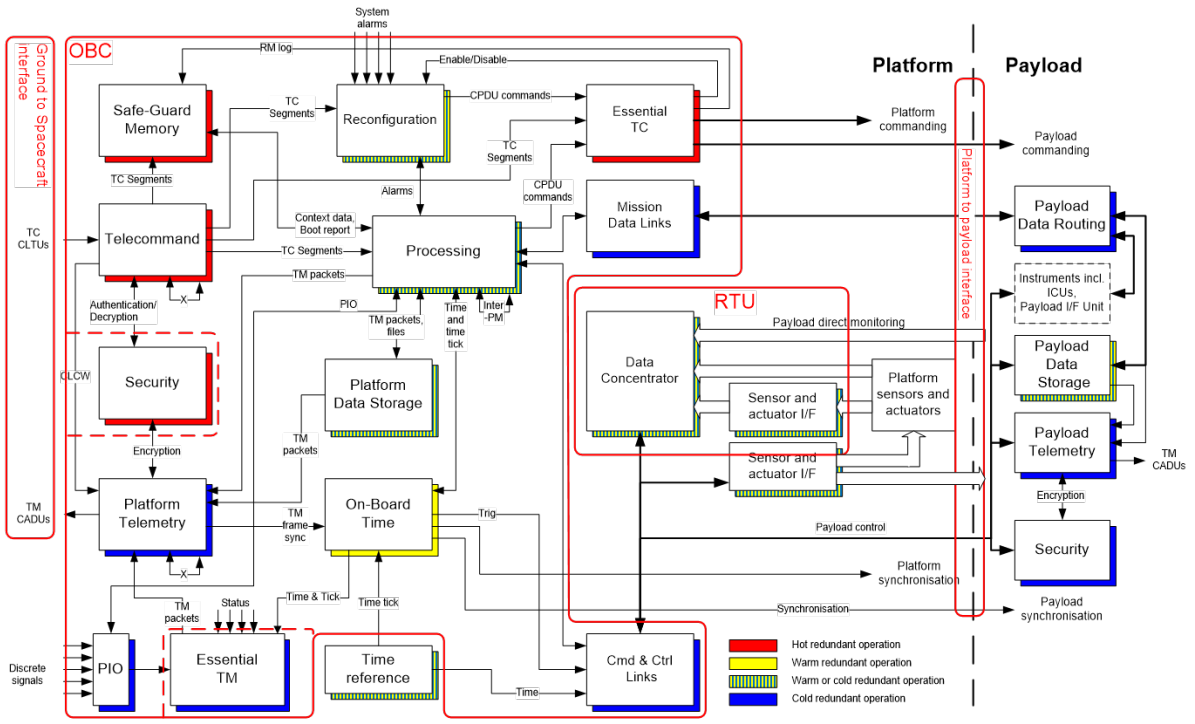


Figure 8.1: SAVOIR functional architecture as seen in the SAVOIR Data Handling Handbook.

8.2.1. Possible configurations

In chapter 6.3, a high level concept for the system was described. It consisted in the the division of functions between a Supervisor, an OBC and a PLIU. That idea is further developed into three concepts which mostly diverge in the placement of TM/TC functions in the Supervisor unit. This exercise shows how functional allocation plays a major role in the reduction of recurrent engineering costs in order for this architecture to adapt to a large arena of missions.

The functions provided by the PLIU are similar for all versions. It receives payload data which is routed for storage or processing by a dedicated processing unit. Another processor provides payload control via a dedicated control link. The payload also receives synchronization signals from the Supervisor. The main processor of the PLIU and the payload data processor share interprocessor messages (inter PM), boot report from the payload data processor to the main processor and context data in the opposite way. This main processor also develops similar links to the other units. Additionally it receives telecommand segments from the telecommand function. Payload data storage is linked to the telemetry function to be downlinked.

There are a number of functions attributed to the Supervisor unit which are immutable between versions of the architecture. These are thought to be indispensable parts of a supervisor unit, being divided into three categories: on-board time; reconfiguration and essential TM/TC. The first ensures the synchronization of all units and accurate knowledge of time. Hence, these signals are distributed to all units and platform. The reconfiguration function requires a safeguard memory from which to receive and store context and boot data. Alarms from the avionics and other units are also concentrated in this unit. Essential telecommands are controlled from the reconfiguration functions as well, which are then transformed into high priority commands (HPC) to be send to components or power supply units. Status of the avionics and S/C are compiled in the Essential TM functions. The parallel IO function provides the interface to the exterior.

The OBC contains, in all versions, functions required to provide processing, storage and control of peripherals. The general processing function is the centerpiece of this unit, managing the links and interfaces to peripherals such as sensors and actuators. It is supported by platform storage functions. Much like the main processor of the PLIU, it receives context data and alarms from the supervisor. Telemetry packets are sent and telecommands received. The OBC is also able to control the Essential TC function, much like the Supervisor.

In the telemetry function, all data to be downlinked is concentrated. It receives packets from platform data storage, payload data and essential telemetries. Command link control words (CLCW) are received from the telecommand function, to report the acceptance and reassembly of TC frames. After assemble, telemetry packets are sent to the RF transmitter via a dedicated interface.

The telecommand function is the symmetric of the telemetry function. It receives telecommands from an external receiver unit and then routes the segments inside the system. Essential TC segments are routed to the respective function, whilst other non essential segments are routed to the processing units of each unit.

Most of these functional allocations are immutable between options. This is related to already described high level features which guided the design. The distinction is reserved to the functions related to telemetry and telecommand. It is believed that these functions are extremely important as ground commands are the last resort to recover the spacecraft in case of unrecoverable failure. Also, handling of CCSDS communication protocol at hardware level imposes hard requirements at later stages of the design, therefore requiring attention early on. The following paragraphs describe the main differences in these aspects between versions.

Version 1

Option 1, figure 8.2, features a separation of essential and non-essential TM/TC between the OBC and Supervisor. Interface with RF units is performed at the OBC however handling and acting of essential TM and TC messages is performed at the supervisor. Hence, the essential functions are allocated to the Supervisor whilst the nominal TM/TC operations occur on the OBC.

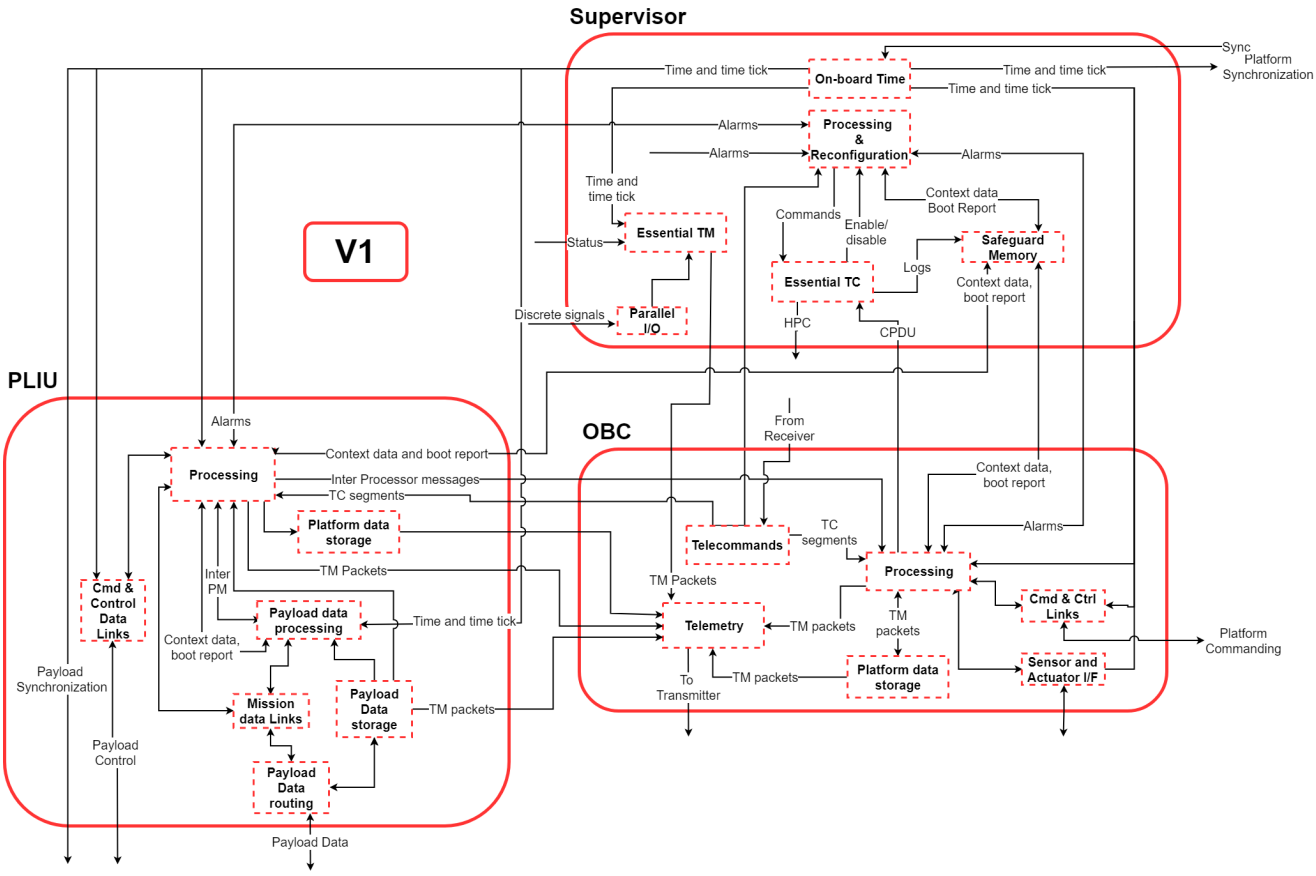


Figure 8.2: Functional architecture for Version 1

Version 2

In this version, figure 8.3, an additional receiver can be connected to the Supervisor unit for ground access for fault recovery. It is considered a secondary source of telecommands. It is, in essence, a

backdoor to the system during safe-mode operation whilst maintaining the nominal radio interfaces in the OBC.

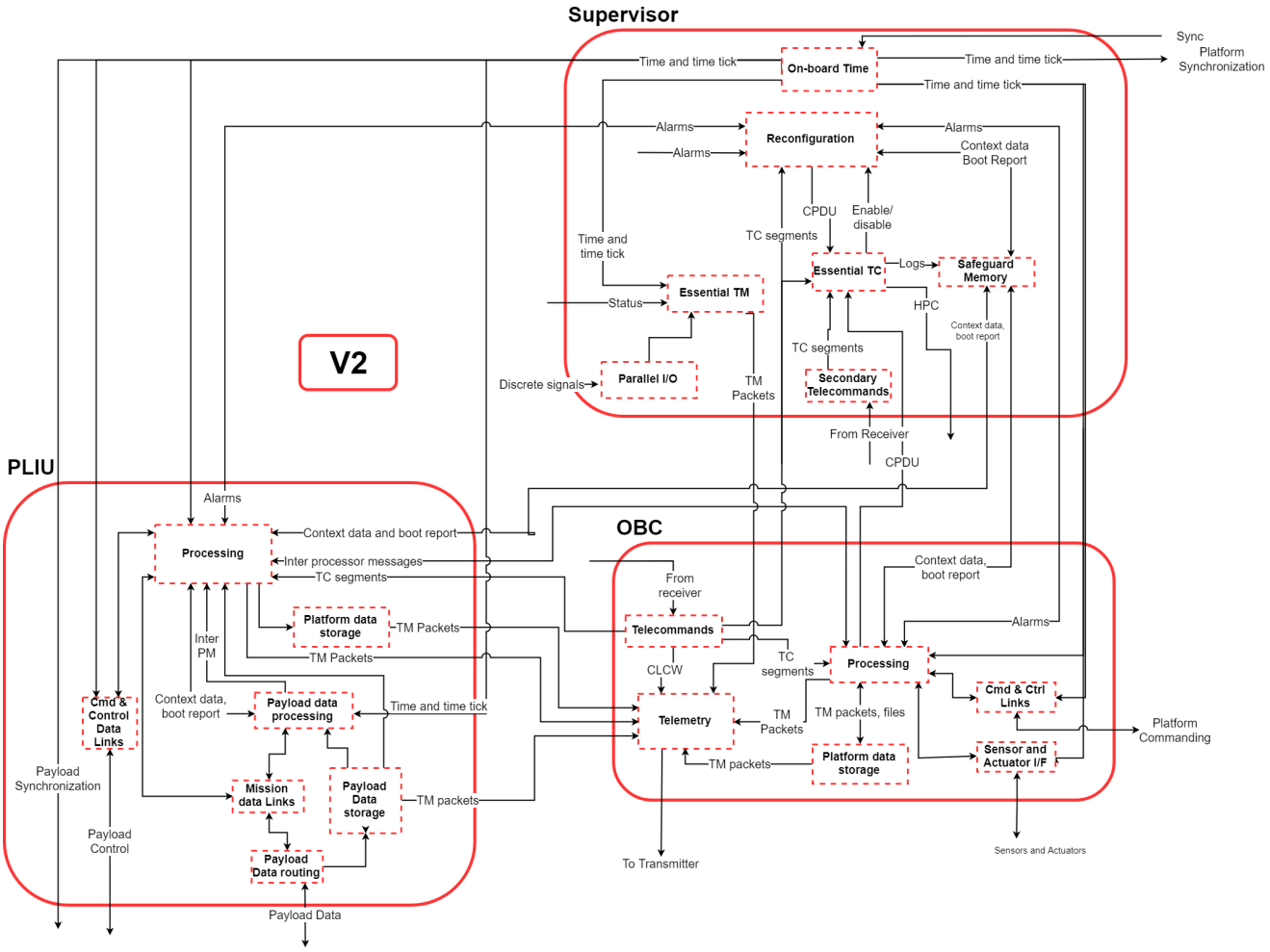


Figure 8.3: Functional architecture for Version 2

Version 3

This option, figure 8.4, is marked by the allocation of all essential and non-essential TM/TC to the supervisor in contrast with the previous options. Such concept minimizes requirements for the physical design by concentrating functions in one unit. Additionally, it assumes that the dependability figures of the Supervisor system support communication and control of the avionics in all scenarios.

Trade-off

From the previously presented options one was selected via an elimination process. First, option 1 is eliminated due to the lack of direct access to telecommands by the Supervisor. In the event of functional interruption of the OBC, the Supervisor is unable to receive and act on essential TC since it depends on the telecommand function, therefore impeding the resolution of faults. The second option is also disregarded. That configuration requires the implementation of hardware capable of handling CCSDS in both the OBC and Supervisor. This increases the complexity of the system by having two sources of telecommands without significant benefits compared to the third version of the architecture. Therefore, version 3 was selected as the one which better serves the requirements of this design. The design is further discussed in the following section.

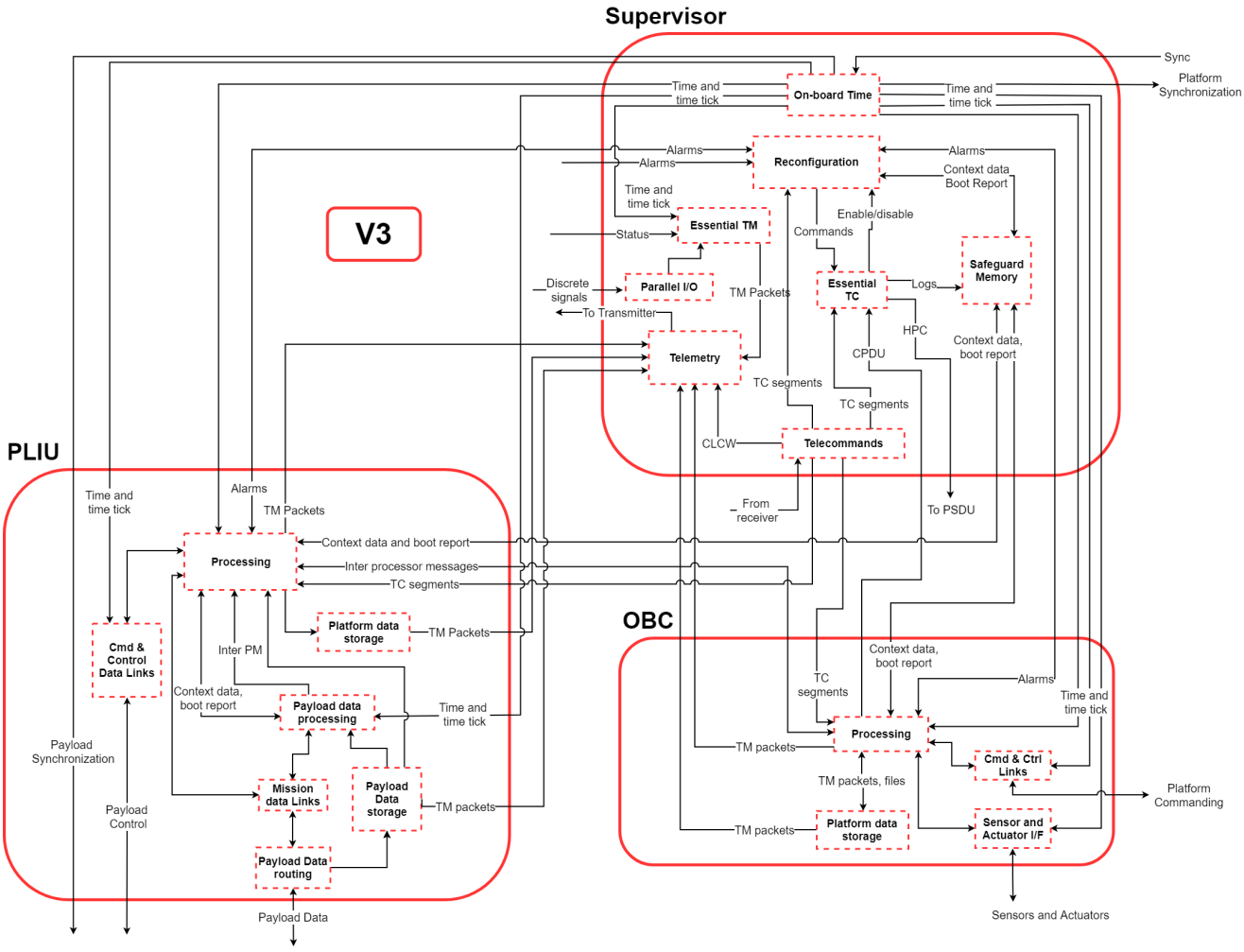


Figure 8.4: Functional architecture for Version 3

8.3. Discussion

Increasing dependability figures comes at a cost both monetary as well as complexity-wise. The goal of this thesis to achieve high dependability figures whilst maintaining the cost-effectiveness of the avionics is achieved, to a large extent, by the allocation of functions in the Supervisor unit.

There are two aspect thought to be paramount for this goal: the ability to communicate and control the S/C at all times, in particular during safe-mode operation; second, the ability to autonomously reconfigure the S/C following fault detection. When these two requirements are combined in a single unit, named the Supervisor, it is thought that dependability requirements on other units, OBC and PLIU, are relaxed thus enabling the introduction of COTS components. These two functions, usually not seen in COTS-based satellites (eg. CubeSats), can be implemented in small satellites by properly mixing COTS and rad-hard components.

The suggested functional architecture is in essence divided into two segments, the supervisor or rad-hard unit, and the OBC and PLIU or COTS units. The Supervisor implements the functions required to ensure the integrity and availability of the system by developing hardware coding/decoding of TM/TC segments, reconfiguration functionality, clock distribution and certain interfaces with the exterior. Thus, this unit provides minimum functionality to the avionics. These can be expanded by the addition of other units such as OBC and PLIU.

The modularity of the design is the distinctive factor of this concept. The Supervisor is by definition a rad-hard unit, an 'old-space' implementation in its design and selection of hardware. However, when coupled with the OBC and PLIU, the supervisor is a unit which allows the OBC and PLIU to be implemented using COTS components without compromising the dependability of the entire system. Major

cost reductions can be achieved since the most expensive, rad-hard components, are implemented in a single unit. Furthermore, the low component cost of the COTS units allow for redundant implementations without incurring in major cost penalties. The redundancy of these units is managed by the supervisor. Additionally, the supervisor, by performing reconfiguration functions is able to implement recovery images in the redundant unit which reduce the mean time to recover from a fault.

Upgrades to the OBC and PLIU hardware can be performed following the improvements of COTS products without requiring an extensive qualification process. The uncertainty is managed by the Supervisor which manages eventual faults as they occur and minimizes downtime. Additionally, flexibility in the redundancy of OBC and PLIU is achieved as the supervisor is able to implementation cold, warm or hot redundancy schemes. Additionally, if no redundancy of OBC and PLIU is employed, the supervisor is still able to reconfigure the unit with a recovery image and minimize downtime. Another feature is the ability for the supervisor unit to become the basis of other use-cases. Additional boards, tailored to a particular use-case can be developed with COTS components relying on the Supervisor to ensure dependability. As the supervisor is only designed once, recurrent engineering costs are reduced.
To the authors knowledge no other system employs this view to support the use of COTS components. Reconfiguration units in larger satellites are not used to reduced hardness requirements on other units. Reconfiguration in smaller satellites such as CubeSats is either not available or not supported by a dedicated space-qualified unit.

8.4. Conclusions

This chapter dwell on the functional architecture for the system. The SAVOIR reference architecture was introduced since it was used as a basis from which this particular architecture was built. This reduced development risks as functions and links between functions suggested by the SAVOIR were followed. Three options for the architecture were considered and traded-off with a final solution presented in figure 8.4. The benefits of this architecture were discussed in the last section.

The division of functions per unit and suggested qualification levels of their components are the key distinctive factors of this architecture. The segregation of rad-hard components into a Supervisor board, implementing reconfiguration, TM/TC and clock distribution functions is thought to minimize reliability and radiation hardness requirements on adjacent units. It is expected that the Supervisor unit incurs in significant component costs as a results of the required space-grade qualification of its components. However, the basic functionalities it supports, allow for it to become a baseline for future use-cases. This increases the design and selection freedom for adjacent units leading to lower recurrent costs. Redundancy of this additional units is possible with a small component cost penalty, as they are mostly composed of COTS components, reducing overall system costs.

At this stage of the report, the reader is expected to have a deep understanding on the system's functional architecture, the reasoning for that design and its impact on dependability. This chapter is the basis for the following chapter which develops the physical architecture and allocates functions to components. The procurement of components is guided by the considerations presented in this chapter.

9

Physical Architecture

In this chapter, the physical architecture for the avionics is presented. First, the methodology for the design process is explained, followed by an overview of the design. Sections dedicated to particular features of the design complement this overview improving the understanding of some its design challenges and innovation factors.

Iteration and research are two of the most important aspects of the methodology employed to develop this architecture. This is described in the first section. Secondly, an overview of the design is provided. In particular, the cross-strapping scheme and suggested backplane design, a distinct factor of this architecture that reduces integration costs, is presented. Each unit of the system is also described with the help of visual representations. The following section describe some trade-offs, most noticeably related to processing units and memory technologies. A design feature that provides the ability to change the type of serial outputs, thus reducing recurrent engineering costs, is described in section 9.5. The design of internal and external interfaces is also considered. The former, demonstrates how to support a large number of I/Os which are required according to the functional architecture. The latter, concludes on the impact of small size connectors in the overall system size and the ability to adapt this architecture into a single-board computer. Finally, a review of the entire design is given.

In combination, these sections present the function to component mapping for the architecture. The reader shall be able to, at the end of this chapter, understand the design features that distinguish this architecture from others and make it possible to reduce component, integration and recurrent engineering costs. Additionally, it shall understand the flexibility of the design to be implemented in multiple configurations of interfaces, functionally and performance.

9.1. Methodology

The design of the physical architecture builds on the functional design defined in the previous chapter. The chapter provided some clues and guidance to the design of the physical architecture although this is an iterative process. This process begun with considering the Zynq-7000 SoC as a candidate technology as described and explored in the literature study [16]. Despite the fact the other SoCs and MCUs were also considered, this device was the basis from which the physical architecture was developed. The methodology to develop the physical architecture was the following:

1. Analysis of candidate processing system, interfaces and their effects on the system.
2. Trade-off and selection of candidate processing systems.
3. Function to component mapping.
4. Candidate technologies for integrated circuits (transceivers and memories).
5. Research into the effect of different IC packages and functions on the system specifications.
6. Interface definition between processing systems and ICs (allocation of pins).
7. Compilation of physical dimensions of devices (ICs, connectors, PCBs).

8. Effects of candidate technologies in system dimensions.

Following this iterative process, a design was consolidated which is presented in the following sections. This design is found to be realizable particularly in terms of interfaces between devices, physical dimensions, radiation harness assurance and verification of requirements. This issues are discussed in the following chapters.

9.2. Overview

The system is envisioned has being composed of multiple PCB boards staked inside a structural casing. A baseline system consists of a Supervisor board, a PSDU, complemented with OBC and PLIU units with or without redundancy. Interfaces to the exterior are available on a single plane of the structural casing providing a single output scheme independent of the internal redundancies. Furthermore, the functional allocations and size advantage of using COTS components allows each unit to be implemented as single board computer if such a demand occurs.

Internally, the layout of the PCB has not only structural implications as well as cable harnessing and radiation effects assurance implications. Due to radiation, there is a benefit from physical separation of these units. Adjacent boards are prone to simultaneous ion strikes and similar TID levels as calculated by [95] and shown in figure 9.1. As a result of these factors, the redundant set of boards are expected to be placed in the middle of the assembly. In the case of an high energy ion penetrating the casing, the probability that the ion strikes multiple active boards is reduced. Additionally, the redundant boards benefit from additional shielding and absorb less radiation if some sort of hot or warm standby is employed.

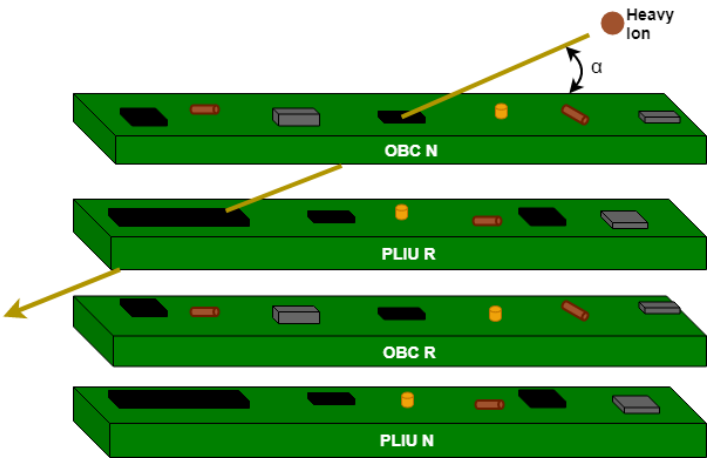


Figure 9.1: The trajectory of an high energy ion penetrating through the avionics at an angle. Notice that depending on the incidence location and angle, the ion will strike multiple PCB's as its energy is much larger than the stopping power of the silicon. Positioning the nominal systems as the outer boards minimizes the probability of multiple ion strikes in nominal systems and shieldings redundant systems.

At this stage of the design, no selection of backplane technology is made although some considerations on internal cross-strapping are made. Either backplane or cables are expected to carry a variety of data buses, control and power signals in-between boards. In particular, this choice has an implication on the cross-strapping scheme that enables internal cross-strapping hence minimizing the number of external connectors. A proposed backplane is presented in the following paragraphs.

Cross-strapping

A wide variety of cross-strapping schemes are seen in space avionics. From total absence of redundancy to totally redundant, cross-strapped systems, the trade-off and design of these features is of major importance to the behaviour of the system.

An analysis of cross-strapping models, as presented in the SAVOIR architecture, has revealed some potential improvement points, in particular for applications in small satellites. Figure 9.2 represent how peripherals and subsystems of a spacecraft are connected to the avionics system in legacy systems.

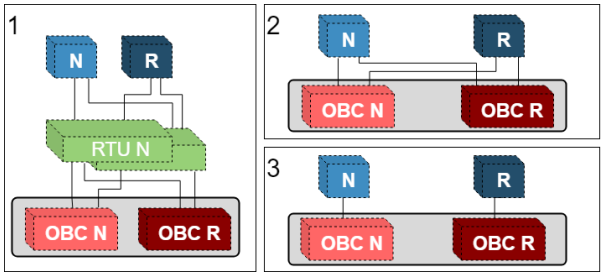


Figure 9.2: Three types of legacy cross-strapping methods as seen in SAVOIR data handling handbook.

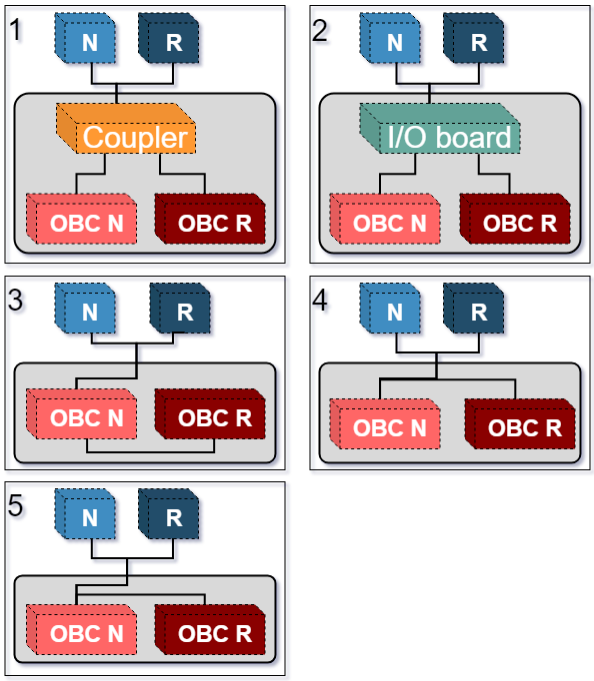


Figure 9.3: A variety of internal cross-strapping schemes.

Schemes 1 and 2 of figure 9.2 show two arrangements of nominal and redundant units which increase harnessing mass and complexity by requiring separate wires from the peripheral to each OBC. Additionally not all peripherals, in particular COTS ones, offer redundant interfaces. Scheme 3 does not require redundant outputs in the peripheral, however each OBC has its own peripheral set which imposes harder requirements for the rest of the S/C design. In order to improve mass and cost of wire harnessing from the peripherals to the avionics, and to relax requirements on peripheral selection (targeting COTS components), other concepts were developed. The goal is for the avionics unit to provide a single interface for a particular peripheral bus, thus simplifying the design of the entire spacecraft. Internally, that bus is then cross-strapped to the multiple boards as seen in figure 9.3.

The options displayed in figure 9.3 allow for redundant control of a single data bus which is connected to a number of redundant and nominal peripherals. It was concluded, from the analysis of the ICDs of the AOCS peripherals presented in annex A.2, that these devices are fail-safe which means that if the device is not powered or a latch-up is detected by its internal electronics that their outputs are set to a high impedance state, also known as tri-state or floating. From this, one can argue that after a peripheral fault has been timely detected and the device has been turned off, that the bus it is connected to will not be further affected by said fault. This allows for more flexible designs and redundancy schemes which will benefit from this internal cross-strapping of the avionics system.

The trade-off between the options of figure 9.3 is mostly based on signal integrity, dependability and development aspects. Options 1 and 2 are eliminated since they require the design of additional hardware. Options 3 and 5 are eliminated based on the fact that stub length shall be minimized and

equal for both nominal and redundant units in order to minimize reflections [96]. Therefore, option 4 is the selected option.

Backplane

It is envisioned that I/O signals are passively divided for interfacing nominal and redundant units. This routing is achieved via a solid PCB, supporting the external connectors and signal routing along with flexible PCB sides which, using connectors at their tips connect to nominal and redundant units. Such an implementation, besides allowing for internal cross-strapping has low design and product cost as it consists of a passive PCB. Additionally, impedance matching of the vias in the solid and flexible parts of the PCB has been demonstrated in literature [96] [97], allowing for good signal integrity. The use of flexible PCB, besides signal integrity considerations, also minimizes integration complexity, as a flexible PCB is easier to manipulated compared to a large array of cables and connectors. An example implementation of this concept is seen in figures 9.4 and 9.5. The first one is an exploded view. The second one is an assembled view which shows the small form factor achieved by using flex PCBs.

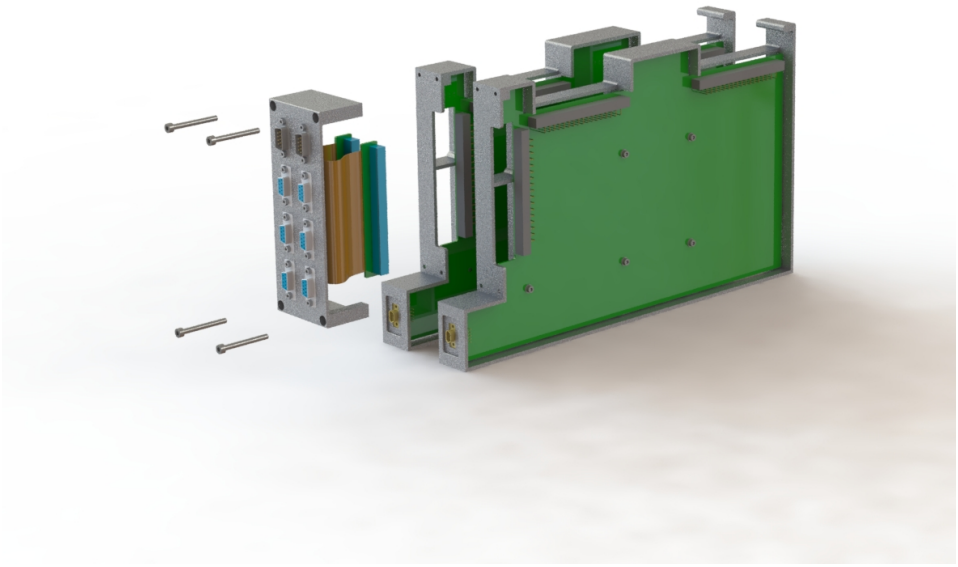


Figure 9.4: Exploded view of redundant board crossstraped to the same output pins via a PCB with flexible sides. Courtesy of Evoleo Technologies.

9.2.1. OBC

Figure 9.6 represents the proposed physical architecture of the OBC board. It develops six connectors for data interfacing with external units and an additional JTAG connection for debugging and programming purposes. Furthermore, it interfaces with the other boards via the proposed backplane. This interface not only exchanges data but also provides regulated power for all components in the PCB.

A major guideline during the design process is to maximize the potential of each physical device, in particular the chosen microcontrollers. This is accomplished by prioritizing the design around the microcontroller, in particular by utilizing its native I/Os and features. This reduces the complexity and cost of the design since less components are required and the advantages of microcontrollers are enhanced.

Therefore, the design of the OBC board is centered around a SoC, complemented with an array of components to support its functions and also to provide the interfaces to external devices. Despite the

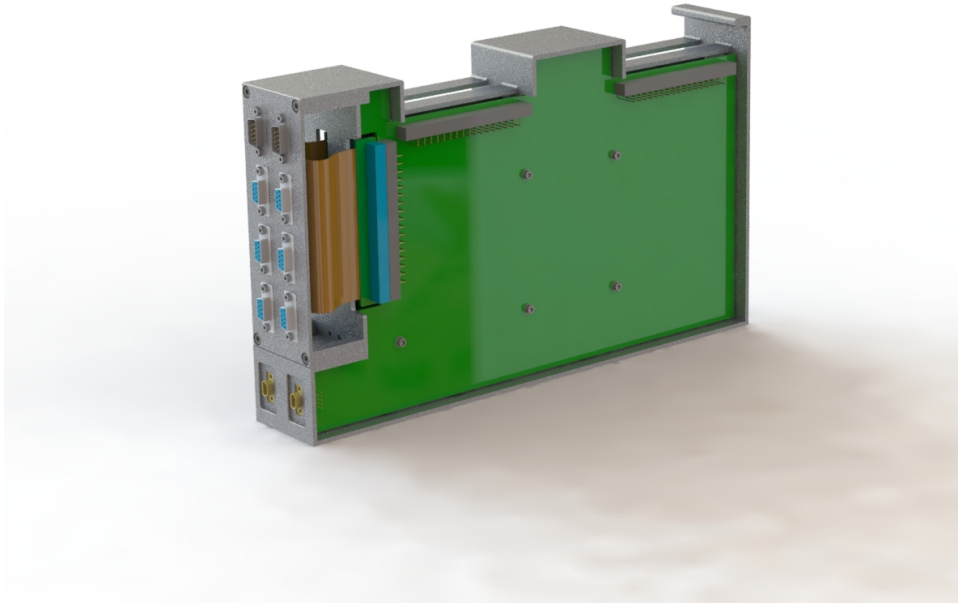


Figure 9.5: Assembled view of redundant board crossstraped to the same output pins via a PCB with flexible sides. Courtesy of Evoleo Technologies.

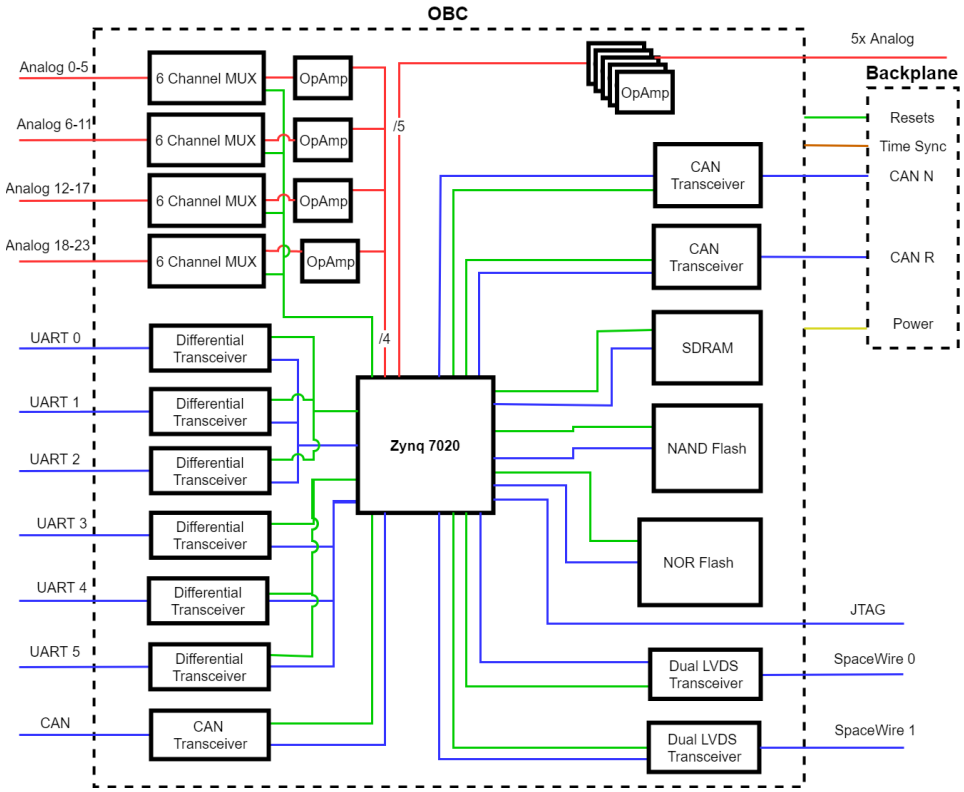


Figure 9.6: Physical architecture for the OBC unit. Not to scale. Blue lines: digital data; green lines: control; yellow lines: power; red lines: analog; brown lines: time and sync.

fact that no particular selection of components is realized at this point of the design (besides the SoC), representative allocation of interfaces and functions to components is achieved.

The processing function is developed by the Zynq-7000 series SoC, supported by volatile memories (SDRAM), first stage boot memory (NOR Flash) and NAND flash acting as platform data storage. Command and control links and data interfacing with other boards is achieving by means of discrete signals for time, resets and redundant CAN transceivers connected to one of the two CAN controllers of the SoC. External sensors and actuators are connected to the SoC with the physical layers of the data protocols and conditioning of analog signals supported by a variety of ICs. Analog signals from the sun sensors are multiplexed and amplified before being sampled by one of the Zynq's internal ADC. The use of six-channel multiplexers in combination with the internally multiplexed inputs of the ADC allow for tailoring of the sampling procedure according to the mission. The second ADC is utilized to sample additional external signals allocated by the end-user. The implementation of the physical layer of the RS-422, RS-485, SpaceWire and CAN protocols is assured by a set of transceivers which, due to their characteristics make it possible to adjust the number and type of protocols provided to external units without major redesigns. This ability to adapt the external interfaces with low recurrent engineering costs is further explained in 9.5.

9.2.2. PLIU

The design of the PLIU, see figure 9.7, differs from the OBC in particular since it employs a processing unit, the Zynq-7000 and a dedicated payload data processor. Similarly to the OBC, these functions are aided by volatile memories (SDRAM) and first stage boot memories (NOR Flash and EEPROM). Payload data storage is based on an array of NAND flash memories, controlled by the programmable side of the Zynq. The payload data interface is based on LVDS transceivers connected to the data engine which routes this data to programmable logic of the Zynq for further routing or storage. A memory bus is developed for sharing of payload data between units. Control and synchronization of the payload is made by the general processing unit via discrete signals and a payload CAN bus.

The data engine is programmed by the Zynq SoC. Due to its programmable logic capabilities, it is possible to personalize this link between both units according to the chosen data engine, for instance via parallel or serial interfaces. As an example, a Spacewire link can be established supported by physical layer LVDS transceivers. This implementation would allow the Zynq SoC to program and control the data engine as well as supporting data transfers. The selection of data engines is discussed in 9.3.2.

9.2.3. Supervisor

The centerpiece of the Supervisor board is a rad-hard FPGA aided by other rad-hard ICs. Volatile memory is in the form of SDRAM whilst its boot memory is an EEPROM. Second stage boot images for the OBC and PLIU boards are stored in a NOR flash.

Interface with other boards is via redundant CAN buses along with the distribution of reset and time sync signals. The supervisor also measures currents from the PDSU which are sensed, amplified, multiplexed and then converted with digital signals. External interfaces consist of 5 full duplex differential signal pairs which are expected to support redundant interfaces to receiving and transmitting radio units. Additionally, 6 switches are developed for control of external units. The design is seen in figure 9.8.

9.3. Processing units

At the heart of an embedded system there usually is a processing unit. In the form of an FPGA, SoC, MCU or processor, these provide not only processing power as well as interface with peripherals and memories. In this system, three types of processing units are expected. On the OBC unit, a SoC, on the PLIU the same SoC with an additional data engine, and in the supervisor an FPGA.

In this section, technology candidates and important trade-off parameters are presented. These strive to provide a state-of-the-art overview of the available technologies and their benefits if implemented on the design. For the SoC, a target device is selected on the basis of the literature study findings. Multiple options for the data engine are given based on current developments in the European space industry. Rad-hard FPGAs for the supervisor are discussed and some suggestions presented.

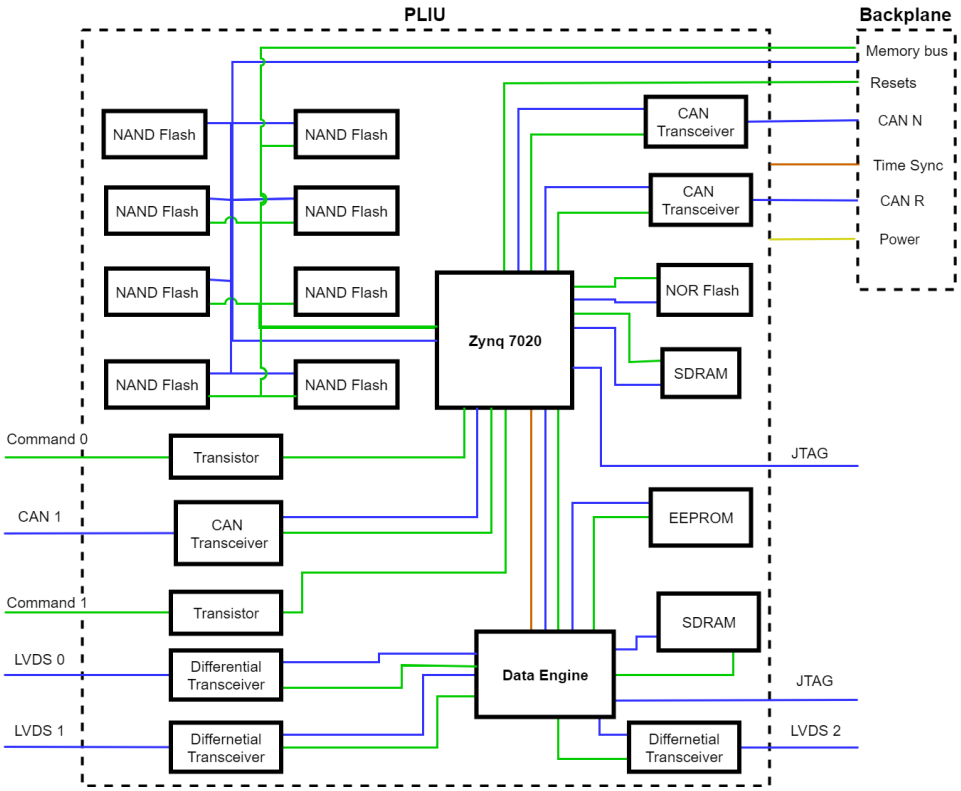


Figure 9.7: Physical architecture of PLIU unit. Not to scale. Blue lines: digital data; green lines: control; yellow lines: power; red lines: analog; brown lines: time and sync.

9.3.1. SoC

The SoC for the OBC and PLIU must perform complex tasks related to the real-time control of the S/C and its peripherals. A large number and variety of peripherals are expected to be operated simultaneously, in particular in the OBC. Therefore, a device with high processing power and I/O possibilities is to be found whilst maintaining the cost low by using commercial devices.

Previously, a literature study focused on the state-of-the-art in processing units for small satellites. It concluded that significant performance improvements are achievable with COTS devices, despite some consequences on the radiation hardness. Most noticeably, the Zynq-7020 SoC was found to be particularly suited to this use-case as a consequence of the combination of programmable logic (Artix FPGA) and embedded processing cores (dual-core ARM Cortex-A9). Additionally, a variety of peripherals are available as seen in figure 9.9. Its radiation harness, studied in chapter 11 further justifies the use of this SoC as the central core of the OBC and PLIU.

Other micro-controllers were also considered for completeness. These were selected based on the findings of the literature study and evidences of chapter 3. Listed in annex A.5, it is possible to conclude that despite the much lower cost of the Zynq, it is capable around 10 times more DMIPS than the popular rad-hard GR712RC LEON-3FT MCU [1]. In fact, the cost parameter is a major decision factor. The differences between COTS controllers and space qualified devices is also seen in the maximum power consumption and radiation hardness with qualified devices assuring lower power consumption and improved hardness.

9.3.2. Data processor

The choice of a suitable data processor is based on the needs for the system to support the increasingly demanding requirements of EO payloads with flexibility and low power consumption. For these applications, very long instruction words (VLIW) digital signal processors (DSP) and FPGAs are the most adequate devices due to their efficiency in applying complex operations in large data sets

[1] DMIPS: Dhrystone Millions of instructions per second . A popular benchmark program to assess the relative performance of a processing architecture [98].

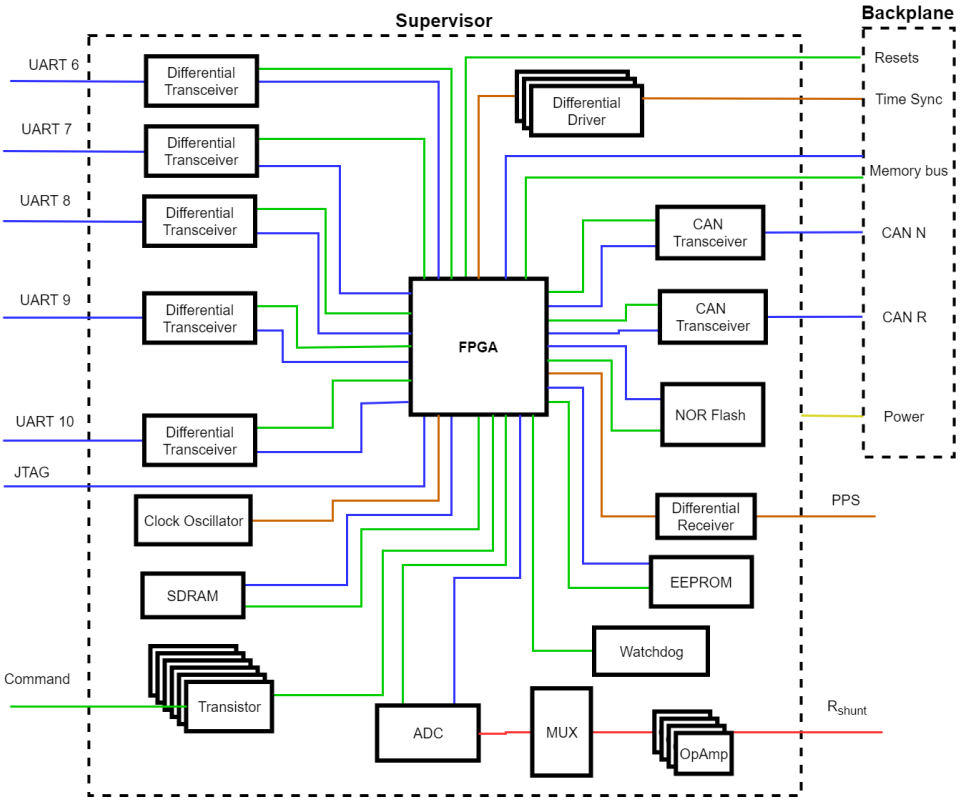


Figure 9.8: Physical architecture of the supervisor unit. Not to scale. Blue lines: digital data; green lines: control; yellow lines: power; red lines: analog; brown lines: time and sync.

[39] [99].

There are a number of differences inherent to FPGAs and ASIC implemented DSPs that affect the choice of technology for a certain application. For example, ASICs allow faster clocks at lower power consumption whilst FPGAs allow better parallelism and flexibility. Additionally, the memory technologies employed in each device affect its radiation harness, namely the sensitivity of SRAM based FPGAs [100].

Selection of a data engine for the architecture is a complex process. The ESA 2007 Round Table on "Next Generation Processor for On-board Payload Data Processing Applications" [78] provides guidance and background for this selection. It is possible at this stage to point out promising devices worth considering based on current developments and heritage. The two presented data processors are being considered for future ESA missions and are not COTS products [101] [78]. Besides these rad-hard devices, one can also consider high-end commercial FPGAs such as the UltraScale devices from Xilinx.

The first option is the High Performance Data Processor (HPDP) from Airbus seen in figure 9.10. The HPDP "has been initiated by the European Space Agency (ESA) and DLR to address the need for a flexible and re-programmable high performance data processor". It is implemented on a 65nm technology from ST Microelectronics which provides radiation robustness along with low power consumption. With 40 Arithmetic and logic units (ALU) running at 250MHz and 2 VLIW cores at 1250MHz it provides 40 giga operations per second through parallelism via four 1.1Gbps streaming ports. A SpaceWire interface enables control and cascading by using multiple devices. It has 4MB internal SRAM memory, watchdog circuitry and controllers for DDR3 memory [102].

Another possibility is a 65nm CMOS DSP from RAMONChips, the RC64. Targeted to space applications, it is a rad-hard implementation of 64 single-precision floating point units (FPU) cores at 130MHz. The peak performance is as high as 65Gops for 16-bit fixed-point multiply and add operations. There is a variety of interfaces, including 12 high-speed serial links, supporting SpaceWire for control and configuration and 48 LVDs links. It has also 4MB of internal memory and DDR3 and NAND flash controllers [103].

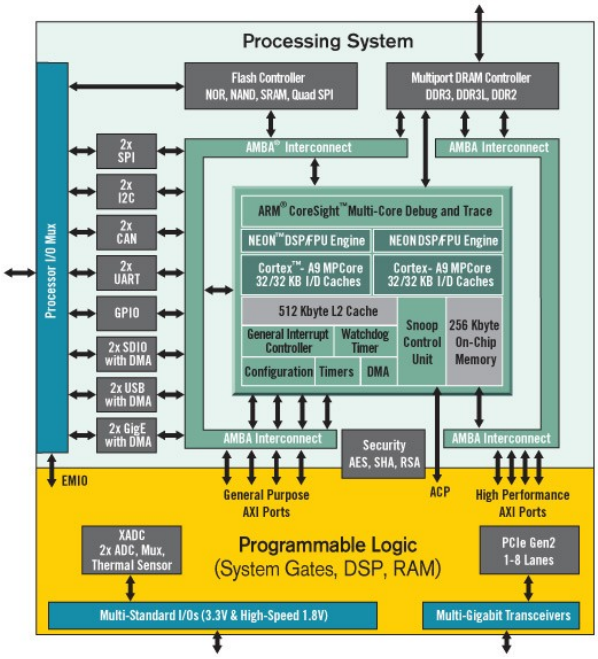


Figure 9.9: Internal architecture of the Zynq-7000 series SoC. Courtesy: Xilinx

9.3.3. Supervisor FPGA

There are three types of FPGAs based on the technology used to store the configuration bitstreams [104]. Radiation response, power consumption and other factors vary among these technologies which requires careful analysis before selecting a technology for a certain application. Recent advances in commercial FPGAs are complicating the trade-off process for engineers. [105] FPGAs are widely used in the space industry for their flexibility in implementing complex digital circuits. SRAM-based FPGAs store configuration data in SRAM which is volatile thus requiring an external non-volatile memory when powering up. They also require correction of upset bits in configuration memory, known as scrubbing. In contrast, Flash-based FPGs are non-volatile, consume less power and are more tolerant to radiation [104]. These have become more resourceful than the SRAM variant with the recent advances in Flash memory technology. Lastly, antifuse FPGAs can only be configured once and were, for a period, the only radiation tolerant FPGA technology [43].

Recently, commercial FPGAs have gained the attention of the space industry for their tolerance to radiation. In combination with considerable higher performance at lower power consumption, com-

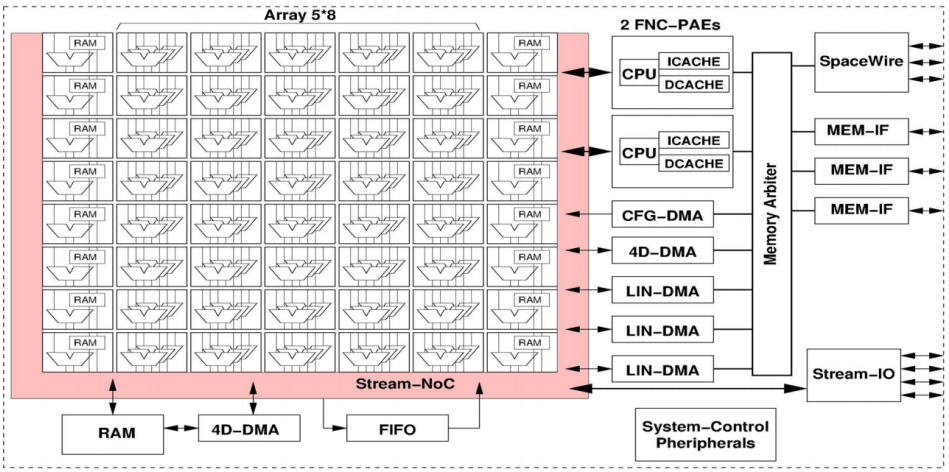


Figure 9.10: Architecture of the HPDP data processor. Obtained from [11]

mercial FPGAs are now considered appropriate for many LEO missions. Most significant issues are related to the more frequent scrubbing required to mitigate SEU, as described by Glein et al [106], which predict similar reliability levels between a space grade Xilinx Virtex-5QV and commercial Xilinx Kintex-7 devices in N modular redundancy.

Despite these promising results, the proposed architecture predicts a single space-grade FPGA to assure high reliability and availability levels. This is based on the argument that the implementation of NMR incurs on a unnecessary design and validation effort. Additionally, the feature to update the configuration of the FPGA mid-flight is required. This eliminates anti-fuse based devices from the selection process leaving Flash and SRAM as two possible solutions. The aforementioned differences between technologies are to be considered for a trade-off. However, the two most important aspects to consider are the unit cost and SEL threshold LET.

Space grade FPGAs are extremely specialized, expensive products. The cost of a single FPGA ranges from a few tens of thousands of euros to close to a hundred thousand euros, a major difference from the couple thousands euros for high performing commercial devices. In the context of this system, the supervisor FPGA easily outshines the COTS based OBC and PLIU units in terms of cost, as it will be described in chapter 12. In order to maintain cost-effectiveness it is therefore important to further analyze the requirements for this device and avoid unwise choices. Popular devices are the flash-based RTG4 or RT ProASIC3 FPGAs from Microsemi or SRAM-based Virtex-4QV and Virtex-5QV devices from Xilinx.

Furthermore, the variable radiation hardness of space qualified FPGAs requires attention when selecting a technology. The presupposition that the Supervisor is an always available unit requires that its components are SEL immune. Hence, the procurement of components for the Supervisor, in particular the FPGA, shall eliminate all devices which, besides being space-grade are not SEL immune. As will be presented in chapter 11, the threshold LET for SEL shall be higher than 100 $MeVcm^2/mg$.

9.4. Memories

The memory technologies selected for this application can be divided into two main categories, volatile and non-volatile. For each main categories, distinctions are also possible depending on the particular functions they fulfill, which are described in the following paragraphs.

9.4.1. Volatile

Regular operation of an embedded system requires fast access memories to temporally hold relevant information such as executable code and variable data. This is typically performed by volatile random access memories (RAM) which are able to store information whilst powered and have much better write/read times than non-volatile memories such as EEPROM or FLASH [107].

There are two types of RAM, dynamic (DRAM) or static (SRAM), if the stored bit needs to be refreshed or not, respectively. Although SRAM is faster, its density is also reduced so it is commonly used as cache memory whilst DRAM is used as system memory, despite its higher power consumption. Dynamic RAM can be synchronous (SDRAM) or asynchronous to an external clock signal. Due to this synchronicity, the flow of instructions to the memory is more efficient and therefore, SDRAM operates at much higher speeds. Beyond SDRAM one can also have DDR memory, for double-data-rate, where both rising and falling edges of the clock are considered, doubling the transfer rate, and clock frequency is increased from 100MHz in first generation DDR to 400MHz in DDR4 [108]. DDR memories also allow very large densities and advanced error correction features. These state-of-the-art DDR SDRAMs are the target technologies of interest for this application .

Both commercial and radiation hardened components can be found for DDR, DDR2 and DDR3 SDRAM and used in space applications. For the case of DDR4, testing from NASA's Electronics Parts and Packaging (NEPP) is underway, preparing for the use of these products in satellites. For now, DDR3 is still the most advanced technology to be flown with well studied components on both commercial and space qualified sides of the spectrum [109]. For these reasons, DDR3 SDRAM is the targeted technology for volatile memory in this context.

9.4.2. Non-volatile

The use of non-volatile memories in this system is further explored in the following paragraphs. In particular, payload and platform data storage, as well as boot memory were consider the most

important trade-offs for this architecture. The outcome of this process is the selection of NAND flash devices for payload and platform data storage and NOR flash storing boot and reconfiguration data.

Payload and platform data storage

The increasing storage demands of modern spacecraft are pushing new designs. In the situations where viable space qualified parts do not exist, COTS NAND Flash devices are a viable solution, even for harsh radiation environments like in the JUICE mission, as long as component screening and system level mitigation techniques such as EDAC and recovery methods are employed. For those reasons, interest in COTS memory devices from the industry is increasing. In particular, high density Flash memory provides the required densities for payload and platform data storage without the volatility and power consumption of DDR SDRAM [110].

NAND Flash density is increased by increasing the number of voltage bands in each cell, effectively increasing the number of bits per cell, as seen in figure 9.11. In consequence, SLC (single level cell) technology maps one bit per cell whilst MLC (multi level cell) maps 2 bits per cell and TLC (triple level cell), 3 bits per cell. The increase in density reduces cost per bit at expense of poorer access times and endurance. Most importantly, reliability in radiation environment is reduced with increased SEU susceptibility of TLC and MLC Flash compared to SLC [111]. As a consequence, a careful trade-off is required when individual component procurement is performed, trading the radiation behaviour of SLC and MLC technologies against capacity and performance requirements. Furthermore, technologies are evolving from planar to 3D layouts for even higher densities [112].

Non-volatile memory supports platform and payload data storage functions in the OBC and PLIU units, respectively. Since the storage requirements for these two functions are distinct, considering the much larger capacity for payload data, it is possible to combine SLC and MLC technologies with ECC as necessary to fulfill error rates requirements. Considerations on this subject are made with radiation analysis results in chapter 11.

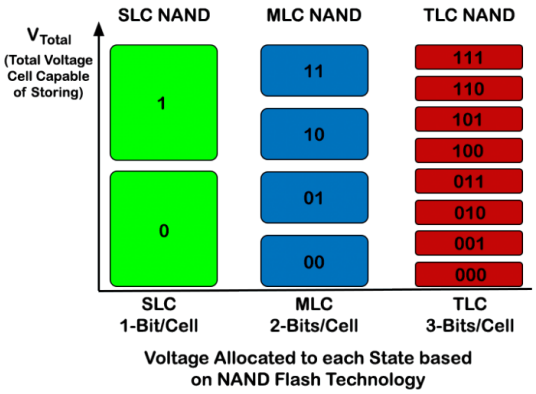


Figure 9.11: Voltage allocation in SLC, MLC and TLC NAND flash technologies.

Boot memory

The selection of boot memory technology and the design of the booting process are extremely important as this procedure is key to achieve high availability and reconfigurability. In the following paragraphs the selection process of memory technology employed in the first stage boot loader is described with the booting process itself being described in 10.2.3.

A number of particularities were identified related to the use-case for the boot memory. First, it shall be a space qualified non-volatile memory since a faulty first stage boot loader would impede the configuration of that board, thus reducing reliability and availability. Second, it should be supported as a source of fast boot data by the microcontroller in the OBC and PLIU and its read time shall be as small as possible. Finally, the chosen component shall support the expected size of installed boot memory. For reference, the target Zynq-7000 series SoC supports NOR, NAND, Quad-SPI, SD and JTAG as primary boot devices.

Four technologies were identified as candidates for this application: NOR Flash, SLC NAND Flash, EEPROM and FRAM. Despite the innate tolerance to radiation by FRAM memories, large read/write endurance, low power consumption and fast read times, it was eliminated as a candidate technology since it is not supported by the Soc. Also, it has low capacity and there is a lack of space qualified parts [113]. On the other hand, SLC NAND flash is a technology that presents very large memory capacity. However, its large memory capacity has low read speeds which is a disadvantage when high availability, and therefore fast reconfiguration, is the goal [114] [115].

In order to select between the remaining options, NOR Flash or EEPROM, focus was put into gathering metrics that could help the trade-off process. In particular, radiation tolerance, capacity, endurance and access times were metrics obtained from manufacturers of both products. Despite the better radiation tolerance of EEPROM, NOR flash is available in higher capacities, available in serial or parallel interface options and has a faster access time [113]. In addition, these conclusions are based on recovered metrics of available rad-hard memories from vendors such as 3D Plus, Renesas, Micron and Maxwell Technologies presented in table 9.1. Due to these reasons, a NOR Flash will be used as boot and configuration memory in the system.

Manufacturer	3D PLUS		Maxwell	DDC	Aeroflex	Atmel
Technology	**NOR**	**EEPROM**	**NOR**	**EEPROM**	**NOR**	**EEPROM**
Capacities	64Mb to 2Gb	1Mb to 8Mb	1Mb to 20Mb	4Mb to 20Mb	64Mb	4Mb
Endurance	1 Million	10K	100K	10K	10K	50K
Interface	Parallel, QSPI	Parallel, Serial	Parallel	Parallel	Parallel	Serial
Access Time [ns]	90	150 to 250	120 to 200	150 to 200	60	∆
TID [krad]	20	80	100	>100	10	20
SEL $L_0[MeVcm^2/mg]$	51,2	80	60	>120 (device)	80	95
SEU $L_0[MeVcm^2/mg]$	10	80	∆	>90 (memory cells) >18 (write mode)	102	∆

Table 9.1: Specifications for a variety of NOR and EEPROM devices as seen in the manufacturers websites. Maximum TID values are under bias conditions. Endurance in number of write/erase cycles. ∆: No data

9.5. Transceivers

Transceivers, or transmitters-receivers, are paramount in a system required to interface with other units. These manage the physical implementation of a communications protocol, interfacing with exterior peripherals in one side and a MCU on the other. In this implementation based on differential signals, the exterior signals are a differential pair and the internal signals are a certain digital logic, such as TTL or CMOS.

The choice of communication protocols and physical layers is case dependent and varies from spacecraft to spacecraft. As it was discussed before, differential signals are the preferred communication medium in space applications namely as RS-485, RS-422 or CAN networks. Therefore, as a means to reduced recurrent engineering costs, it would be beneficial that these physical layers could be implemented as per case basis without requiring major redesigns of the PCB tracks.

The reduction of recurrent engineering costs is effectively achieved by making use of the characteristics of the Zynq-7000 SoC and the packaging of transceivers into discrete ICs. Like other system-on-chip, it develops a number of multiplexed I/Os (MIO) in the processing system segment which means that the large array of supported interface protocols are multiplexed into a smaller number of pins. Most importantly, the similarities in packing for RS-485, RS-422 and CAN transceivers allow the design of the PCB to easily adapt to each of these by means of specially designed vias and the use of 0Ω resistors. Depending on the application a certain transceiver would be soldered into the PCB holes with the resistors adapting the PCB for that particular configuration. In figure 9.12, the design of a PCB able to accommodate these 3 standards is shown.

The design is oversized to allow full-duplex communications. With such configuration, RS-485 and CAN networks which only require two lines are also possible with the rest of the lines not internally connected. In the OBC, the 6 UART outputs, prepared for full duplex signals allow 28 possible combinations of RS-485, RS-422 and CAN interfaces.

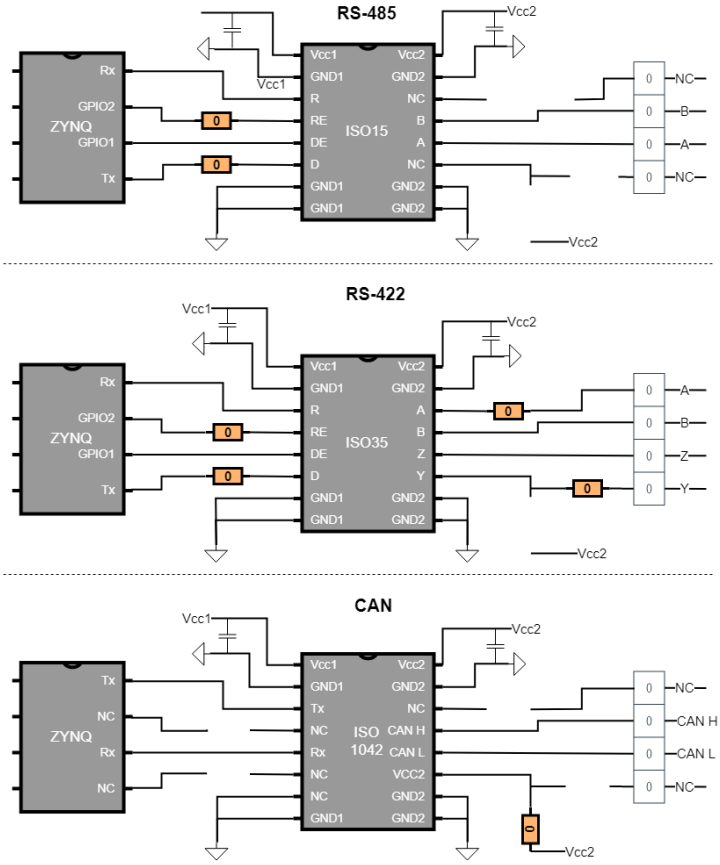


Figure 9.12: An example design to accommodate ISO15, ISO35 and ISO1042 transceivers from Texas Instruments which share the same SOIC-16 package. In theory this design principal can be use to prepare the PCB for whatever transceivers that share some of its pinouts. Note that the pin allocation on the SoC can be configured. The pinouts were obtained in the transceivers datasheets available in Texas Instruments website. NC: Not-connected

9.6. Interfaces

The design of interfaces, both internally between individual ICs and externally with peripherals is paramount not only for the system performance but also in terms of its suitability for the intended application. This section is divided into these two categories.

9.6.1. Internal interfaces

In this sub-section, attention is given to demonstrate the compatibility of the previously described technologies and their ability to integrate in a system. First, the pin allocations for the Zynq SoC are presented for the OBC and PLIU, supporting the diagrams in 9.2.1 and 9.2.2. Then, the connections running through the backplane are explained including the internal CAN bus. Finally, considerations on the impact of different size connectors on the systems and possible SBC implementations are made.

OBC

It is around the SoC that the design of the subsystems revolve. Therefore, it is important to assure that the SoC is compatible with the intended ICs it is connected to, both in terms of number of pins as well as data protocols.

The Zynq SoC is divided into a processing and programmable logic segments with different interface options. The MIO feature of the Zynq-7000 allow its pins to be assign as needed. In the case of the Zynq-7020, 50 pins are available as MIO. However, some protocols are only allowed in a subset of these pins therefore constricting the design. For example, interfacing with NAND flash in MIO, which occupies 22 of the 50 pins, precludes the use of Quad-SPI, Ethernet, NOR and SRAM. Detailed information regarding the use of MIO is available Zynq-7000 SoC technical reference manual [116]. Dedicated pins are provided for SDRAM interfacing.

The 200 pins connected to the FPGA side of the Zynq-7020 are divided in 4 banks of 50 pins. Additionally, a central interconnect fabric allows pins from processing and programmable sides to be accessed by both units. This architecture is seen in figure 9.9. An iterative process was used to map the intended ICs to the available pins. The availability of interface controllers and minimization of IP-core based controllers were the main drivers of this process. The following table 9.2 presents the suggested implementation.

Pin Type	Pin Numbers	Protocol / Peripheral
Processor System	0-39	NOR Flash
Processor System	40-41	CAN 0
Processor System	42-43	CAN 1
Processor System	44-45	UART 0
Processor System	46-47	UART 1
DDR	-	SDRAM
Programmable logic	Bank 1	SpaceWire 0 + SpaceWire 1
Programmable logic	Bank 2	UART 2 to UART 5 + GPIOs
Programmable logic	Bank 3	NAND Flash
Programmable logic	Bank 4	ADC (4 Mux outputs + 5 platform inputs)

Table 9.2: Assignment of Zynq pins in the OBC unit.

The processor system MIO is connected to the NOR flash, the two internal CAN buses, and two UART ports, therefore making use of the native protocols supported by the SoC. The dedicated DDR pins are assigned to the DDR3 SDRAM selected as candidate technology. The PL segment handles, besides the rest of the required UARTs, particular protocols not natively supported by the system and implemented as IP cores. In the case of the UART ports, the flexibility of the FPGA code supporting these ports, in addition to the findings in 9.5, allow for RS-422, RS-485 or CAN networks to be implemented without major redesigns of the PCB. The system develops two SpaceWire networks in pin bank 1 and a NAND controller in bank 3. By implementing the NAND controller in the PL segment, the design not only frees up pins in the PS segment but also allows custom hardware based memory management and EDAC algorithms to be developed according to the customer requirements. The last pin bank is assigned to the inputs of the internal ADC.

PLIU

Similarly to what was mentioned in the previous paragraphs, the allocations of the pins for the PLIU segment builds on the native strengths of this particular SoC. The MIO and DDR pins are assigned similarly to the previous case. The PL pins are assigned to the link between the Zynq and the data engine. Bank 1 is expected to support the chosen protocol for communication between processors, for example Spacewire. Bank 2 is expected to support fast payload data transfers as LVDS or as a parallel interface. Bank 3 supports the NAND flash array used to store payload data. The allocation of the Zynq pins in the PLIU is seen in table 9.3.

Pin Type	Pin Numbers	Protocol / Peripheral
Processor System	0-39	NOR Flash
Processor System	40-41	CAN 0
Processor System	42-43	CAN 1
DDR	-	SDRAM
Programmable logic	Bank 1	Link to data engine
Programable logic	Bank 2	Payload data transfer
Programmable logic	Bank 3	NAND Flash

Table 9.3: Assignment of Zynq pins in the PLIU.

Backplane signals

The backplane transports a variety of signals between the system's units. These are divided into four categories, power, time sync, digital data and control lines.

Regulated power from the PSDU is transported via the backplane. There is a yet to be determined number of power and ground vias, which are dependent on the particular design of the PSDU and power requirements of each board.

The internal data bus connecting all boards is a redundant CAN bus. The differential pair and ground signals for each bus leads to 6 lines running through the backplane. A variety of resets signals, for the processing units and other ICs are also transported over the backplane.

In the case of the PLIU, it is expected that payload data is transported from this board into the supervisor for encoding prior to downlink. Hence, a memory bus is established over the backplane so that the supervisor unit has direct access to the memory array.

Synchronization signals are generated in the supervisor and run via the backplane to each board. The particular configuration and number of these signals is dependent on more detailed design.

Most notoriously, the backplane supports all external connectors and, thus, the corresponding electrical lines. External interfaces are compiled in table 9.4. It is important to notice that there is a considerable number of lines required to support all this interfaces. The PCB tracks shall then be designed in order to avoid cross-talks and with special attention to signal integrity.

CAN network

Traditionally, spacecraft avionic systems have relied on data buses to connect multiple modules with a reduced number of wires. The most common ones are the MIL-STD-1553B and SpaceWires buses. In the case of smaller platforms, such as CubeSats, other solutions are common such as I2C, RS-232, SPI, USB, CAN, in descending order of popularity [117].

There is a number of important aspects to consider when selecting the data bus protocol to be implemented, in particular:

- **Robustness**: Resistance to noise and other errors, in the form of differential signals or error detection and correction mechanisms;
- **Costs**: In the form of component or implementation costs. For the former it is mostly related to the cost of acquiring IP cores and discrete components. For the latter, it is attributed to the physical layer protocols which might increase design and V&V complexity;
- **Procurability**: The level of difficult associated with procuring components (eg. transceivers) with the required specifications and qualification levels. It is also related to the ability of the processing units to support said protocol.
- **Flexibility**: The ability of the protocol to support multiple masters and nodes.
- **Heritage**: The confidence in the suitability of such data bus based on its utilization on previous missions.

The chosen internal data is the CAN bus. CAN was first developed by Bosch GmbH in 1983 as a solution to the then increasing number of wires required to connect subsystems in automobiles. It is a multi-master, low power consumption, two-wire differential signal protocol with robust error detection and correction mechanisms at the transfer layer [118].

Widely used in terrestrial applications it has caught the interest of the space industry and ESA, employing the protocol in missions such as ExoMars, NeoSat, the OneWeb Constellation to name some. Due to these benefits and its popularity, most microcontrollers now provide one or multiple CAN controllers, at all qualification levels including space grade. The physical layer is also supported by a large variety of transceivers, interface converters and controllers, also at all qualification levels (although selection variety is lower at higher qualification levels) [119].

Despite the relatively low data rates (up to 1Mbps) and lack of de-facto high layer standards for space applications, CAN is an appropriate choice for this avionics system which requires parts at different qualification levels. The differential signal is also favorable to signal integrity, allowing for the implementation of a robust connection between all microcontrollers. It supports the transmissions of the following messages between boards and the supervisor: on-board time, TM packets, TC segments, context data and boot report.

The SoC of the OBC and PLIU has one of the two native CAN 2.0 controller connected to nominal and redundant transceivers and subsequent CAN networks. The intent is to assure communication between the microcontrollers in the system in the event of a fault of a transceiver. In these cases, the redundant controller and lines are activated to ensure communications.

9.6.2. External interfaces

The large integration achieved with this design, translates into a significant number of pins in the external interfaces. Not considering the ones required for the PSDU and configuration of the system (JTAG), there are an estimated 148 pins in external interfaces. From these, the largest percentage is for the OBC, 82 pins, followed by the supervisor, 48 pins, and the PLIU, 18 pins.

Table 9.4 contains a suggested allocation of pins to connectors according to signal type and originating PCB. These connectors, described below, were selected in order to optimize their number and footprint. For that, high density connectors are employed except for cases where separation of signals is required or beneficial, for example, Spacewire buses. These connector are implemented in the structural casing of the avionics. However, as it will be seen, their small footprint enables their implementation in each PCB, leading to multiple SBC configurations for other use-cases.

Board	Connector ID	Outputs
OBC	nanoD51_OBC_1	UART_0-5, CAN_0, Analogs 0-4
	MicroD9_OBC_1	SpaceWire_0
	MicroD9_OBC_2	SpaceWire_1
	nanoD25_OBC_1	Analog 5 - 24
PLIU	MicroD9_PLIU_1	LVDS_0, LVDS_1, Command_0
	MicroD9_PLIU_2	LVDS_3, CAN_1, Command_1
SUP	nanoD15_SUP_1	UART_6, UART_7, UART_8
	nanoD15_SUP_2	Commands_2-7
	nanoD9_SUP_1	UART_9, UART_10
	nanoD9_SUP_2	PPS_0 (Rx+Tx)

Table 9.4: Allocation of external interfaces to connectors. The connector ID is formed my amalgamation of the connector type (NanoD or MicroD) and number of pins with and identification the originating unit.

Connectors

The physical interface to the avionics is provided by a number of connectors. Currently, the vast majority of satellites utilize D-subminiature connectors, named after their D-shape metal shield. These connectors are extremely common in computer systems, normally known as being the blue external display connectors [120]. The number and type of pins per connector is customizable with options ranging from a few pins to up to 100 pins.

Other solutions are also offered to replace the bulky D-Sub connectors. For mass and volume saving purposes, Micro-D and Nano-D connectors were also developed. These offer surface reductions of 2.8 and 14 times, compared to the D-Sub standard respectively, with similar ratios for mass reductions. In the space segment, these considerations are relevant in particular when designing highly integrated solutions for small spacecraft [120].

Some standards, such as SpaceWire's ECSS-ST- 50-12, predict the use of Micro-D connectors, although interest into Nano-D connectors is also evident [120] [121]. Nevertheless, the designer is free to implement the connectors it wishes considering size and weight, electrical specifications and cost.

A study was performed to determine the effect of the use of these three types of connectors in the physical architecture. For that end, four different configurations of connectors for the OBC were identified [2]. Configuration 1, 2 and 3 expect only Nano-D, Micro-D or sub-D connectors respectively whilst configuration 4 follows the standard usage of Micro-D for SpaceWire and reduces size by employing the highest density Nano-D avaialble for the rest. The dimensions shown in figure 9.13 were used to calculate surface area along with specifications from cable producer Glenair, obtained from their website.

In table 9.5, the percentage surface area of a 3U size A PCB board required by each configuration is shown, simulating a backplane or SBC. Nano-D configuration 1 leads to the smallest footprint, followed by configuration 4. This surface area gain is quite visible when comparing configurations 1, 2 and 3. This gain suggests that the use of smaller connector standards is paramount to enable the implementation of the many I/Os this system is envisioned to developed. Besides gains in PCB surface area, the use Nano-D connectors translates into mass savings in cable harnessing and increase in the volume density of I/Os provided by avionics.

[2]The OBC was selected as an adequate example since it produces a largest number of signals, 82.

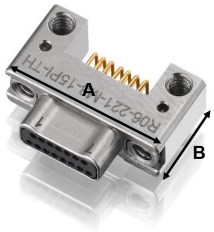


Figure 9.13: Example of NanoD connector with twist pins for termination on printed circuit board. Courtesy of Sunkye.

Despite these benefits, size and price of connectors is inversely proportional. Additionally, rated current is also reduced from up to 7.5A in the D-sub connectors to 1A in Nano-D. These and other factors related to electrical interface design are important to considered in later stages to avoid interface issues [120].

Configuration	Surface Area [mm^2]	Surface area usage
1	845.82	5.29%
2	1777.66	11.11%
3	4027.50	25.17%
4	1030.11	6.44%

Table 9.5: Configurations 1,2,3 consist of 3x 9 pin (2x SpaceWire + CAN + Analog) , 2x 15 pin (6UART) and 1x 25pin (Analogs). Configuration 4 pin allocation in table 9.4. Surface area of a 3U size A PCB is 16000 mm^2.

The outcome of this analysis is the selection of configuration 4 for the OBC connectors and the use of Nano-D elsewhere. The use of high density Nano-D connectors makes it possible to follow the standard Micro-D connectors for SpaceWire I/Os without compromising on surface area and adding some cost reductions compared to configuration 1. The suggest connector configuration for all boards and allocated I/Os is presented in table 9.4.

9.7. Review of design and conclusions

The proposed physical design consists on similar boards inside a structural casing, internally cross-strapped via a semi-rigid backplane with external connector mountings. The OBC unit design is centered around the Zynq-7020 SoC which, by making use of PS and PL pins is able to support a large number and variety of interface types. Similarly, the PLIU also contains a secondary processor for payload data which is controlled by another SoC. A NAND flash array stores the payload data and is managed by the PL of the SoC. The Supervisor is based on a rad-hard FPGA and assistant ICs for interface and sampling of analog signals. The units are connected via the backplane which, besides providing passive cross-strapping, carries reset and synchronization signals from the Supervisor, a memory bus for payload data, nominal and redundant CAN bus and power distribution lines. Volatile memories are based on Commercial DDR3 SDRAM with flight heritage. Platform and payload data storage is based on NAND flash. Boot memory is stored in space qualified NOR flash. A circuit design that supports RS-422, Rs-485 and CAN based on the placement of 0Ω resistors enables customization of interfaces with low engineering effort. Internal interfaces were mapped for the processing units and the pins of external connectors.

It is believed that this design potentiates the benefits of modern SoC in particular their interface flexibility and performance. Space-qualified components are restricted to the Supervisor unit and NOR flash memories to minimize component costs. Considerations for the selection of a data engine are based on recent developments of the European Space Industry and expected demand on on-board data processing. At this stage no selection of data engine was made. The interface and pin mapping suggest that this level of functional integration is possible in a system based on 3U size A PCBs or in similar sized SBC.

This chapter presented the proposed physical architecture. Promising technology candidates were presented and traded-off for some components. At this stage of the report the reader is expected to understand the functional and physical architectures for the system, including major design choices.

Additionally, it shall also be aware of the implications of said choices, in particular the use of commercial products. The following chapter, provides a more in-depth review of the design features which contribute to fault tolerance.

10

Protection Systems

In this chapter, the design features that protect and recover the hardware from undesirable faults are described. Following the description of the physical architecture, this chapter will provide a more in-depth analysis of the characteristics that allow the system to safely reconfigure itself and circumvent faults. This is only possible after understanding the major components of the design and their fault modes.

The methodology to find and select this protection systems is based on the study of the features of individual components as well as available literature. Similarly to what was mentioned before, this architecture strives to potentiate the benefits of COTS components whilst assuring the dependability of the overall system. This can be achieved by exploring the standard features of commercial devices which can often be utilized or adapted to space applications. Additionally, the wide variety of COTS products available allow the system designer to choose devices with characteristics which may contribute to its reliability and availability without significant design implications. For example, transceivers with galvanic isolation are available at similar prices as non-isolated counterparts whilst offering this additional protection.

At the end of this chapter, the reader is expected to understand how faults are handled and recovered, allowing the system to be built using COTS devices. It should also hint at the different FDIR policies to be implemented by the end-user and how these policies are supported by the basic architecture.

10.1. Fault masking

As mentioned in section 3.5, fault masking is any process that prevents a fault to propagate in the system and introduce errors that may lead to failure. In this design, it is achieved via latchup current limiters, galvanic isolation, fail-safe devices, ECC and scrubbing.

10.1.1. Latch-up current limiter

As it will be seen in the following chapter, COTS devices are susceptible to latchups. In these events, current limiters as the name implies, limit the maximum current flowing on an individual power line. These can be implemented on power supplies of individual components or on electrical bus lines, according to the requirements of the design. Although the design of the PSDU is out of scope for this thesis, some considerations on this subject are given.

There are multiple ways to implement current limiting circuits. A simple example consists of positive thermal coefficient resistors placed in series, which increase their resistance as their temperature increases. However their turn-off times are not quick enough to avoid damage. Other implementations, as reviewed by Selčan et al [122], are customizable in terms of autonomy, current thresholds and reset times. Autonomous implementations can be adapted to open the circuit at a certain current and reset it after a certain time. Others are controllable by an FPGA that receives a flag when such an event occurs. These circuits are based on current sensing resistors and, via transistors, open or close the circuit.

A particular aspect to consider when implementing current limiters are the type and number of loads on the power line. It is possible that latchups are not detected and mitigated by this implementation if the current threshold is incorrectly set or the latchup event does not induce a significant increase in power consumption. As it is the case for the Zynq SoC, micro-latchups of only 0.1A were observed [123] which suggests that if that electrical bus line is shared with other components, said event might go unnoticed. Hence, careful analysis of the latchup behavior of COTS components is required to determine their expected latchup current and event rate. Most susceptible devices shall be protected by their own current limiting circuits.

Protection of all power lines and some individual components is expected at this stage. The latchup behaviour of the Zynq SoC and other susceptible COTS build blocks must be particularly analysed in order to determine the proper current limiting implementation. The implementation shall also have the ability to flag and be reset by the Supervisor FPGA if an event occurs.

10.1.2. Galvanic isolation

Isolation of electrical systems is utilized in order to prevent unwanted effects such as ground loops, failure propagation due to over-voltages, electrical transients or electrostatic discharges. By precluding current flow over a barrier, it prevents over-voltages and transients from affecting the other end of the system. This is usually achieved by the use of transformers, capacitors or opto-isolators. Galvanic isolation is adopted in the space industry in signal lines based on the Mil-STD-1553B, which predicts the use of transformer coupling for each bus terminal [12] [124].

In the context of space applications, galvanic isolation plays a significant role in preventing faults to propagate within and in-between systems. This avionics system is connected to numerous peripherals which are themselves sources of faults. For example, peripherals exposed on the outside of the spacecraft, such as sun sensors are subjected to the space plasma environment which leads to voltage build up. When discharged, this voltage will propagate to the avionics unit, which, if not isolated, may lead to the destruction of internal circuitry [12].

In cross-strapped systems, failure propagation due to over-voltage may have catastrophic consequences, as depicted in 10.1. This compromises the entire premise of using redundancy to achieve reliability and availability. In this case, internally connected units, if not isolated, might all be subjected to high voltage states which can lead to the failure of multiple units from a single fault source [12].

Isolation for digital and analog signals paths is, for the above reasons, predicted in this design. It is expected to be employed when interfacing with peripherals outside the system and also in the the cross-strapping between boards. The same is said regarding operation amplifiers, providing isolation for analog signals. Optocouplers are a possible isolation method for other circuits.

10.1.3. Fail-safe transceivers

In a multiple node network, it is important to ensure that an inactive or faulty node does not affect the bus. If not, the entire system might become inoperable or unpredictable and degenerate into an error or failure state. The use of fail-safe transceivers is paramount to ensure that faults like these do not propagate.

To allow communication of multiple devices attached to the same network, signal drivers shall produce an high impedance state when not transmitting in order to not load the bus. Additionally, this shall be the default case when no data is being transmitted, power is removed from the driver or it is in low power mode.

Regarding the receiver side, fail safe is often associated with avoiding unpredictable outputs in the event of 'undefined' voltages at the receivers inputs [1]. This is the case in the event of: 1- all transmitters are in shutdown; 2- the receiver is disconnected from the bus; 3- the cable has an open; 4- the cable has a short. By applying a bias to the line pair, the receiver will then interpret these cases has a logic high, thus ensuring a known state. Additionally, transceiver with internal fail-safe mechanism interpret differential voltages around zero as logic highs, therefore not requiring external bias [125].

All transceivers in the system are expected to provide native fail-safe operation. This improves the dependability of the systems without significant overhead in terms of procurement cost and reducing design complexity.

[1] Undefined voltages are voltages within a certain range where logic high or logic low is not defined.

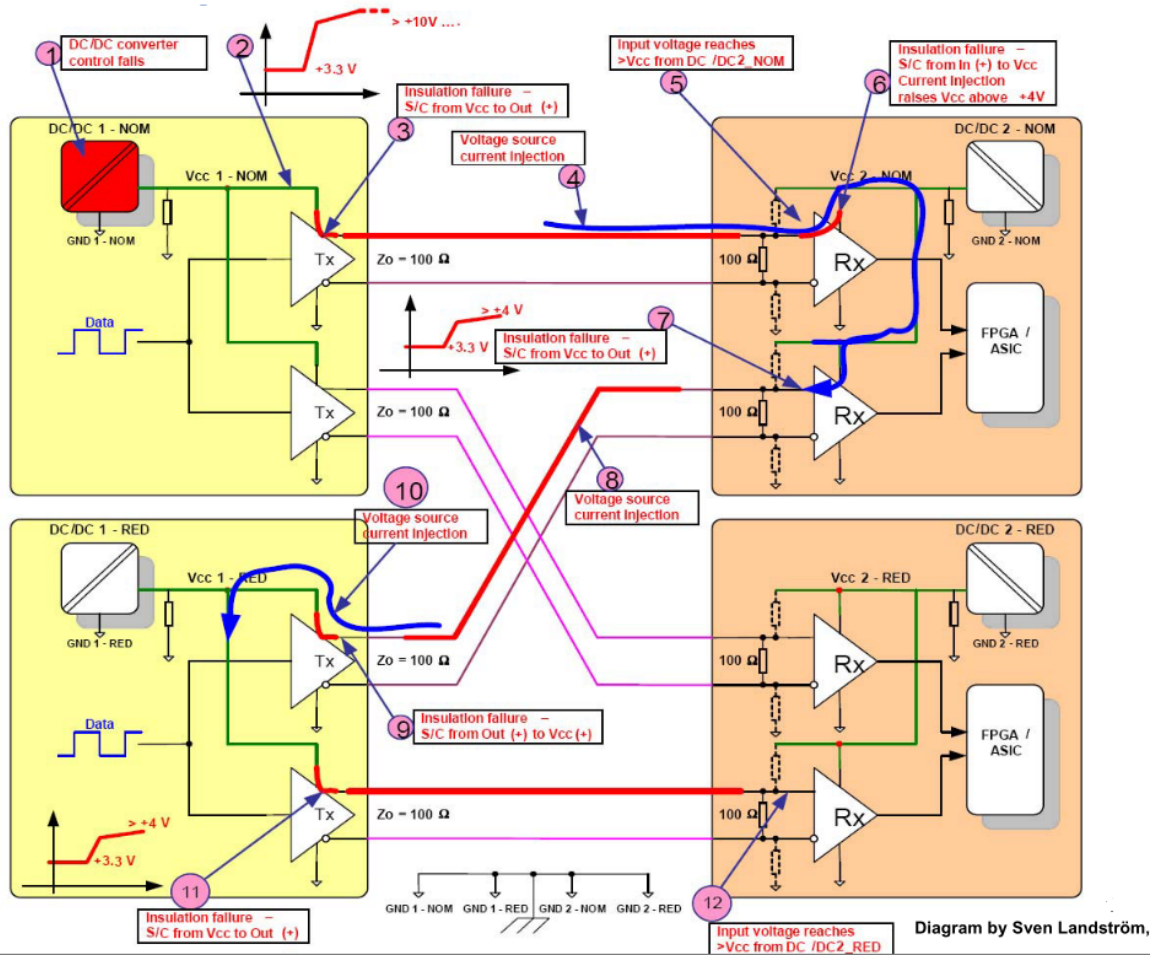


Figure 10.1: Failure propagation in cross-strapped systems due to over-voltage failure. Diagram by Sven Ladstrom as in [12].

10.1.4. ECC

Faults in memories, either arising during normal operating conditions or due to radiation effects, require error correction codes (ECC) to maintain the integrity of the stored data [126]. Depending on the memory technology and radiation environment, the number of corrupted bits varies and thus the requirements on the applied ECC.

According to the persistence of a fault it can be categorized as soft or hard fault. A soft fault is a flip in the state of a memory cell which can be corrected to restore its original value. An hard fault, is a permanent or semi-permanent one when the value of a faulty cell cannot be re-written and corrected. The fault behaviour is a characteristic of each individual memory technology and device [127].

The basic principal behind ECC is the addition of information in order to detect and, in some algorithms, correct the erroneous bit. These methods, in their simplest form, consist in the addition of a parity bit that ensure that the total number of 1-bits in a string is even or odd. This allows for simple error-detection but not correction. For error correcting codes, there is a multitude of techniques, each with their own benefits and downsides. The number of errors a code can detect and correct is dependent on the method and the number of redundant bits it adds compared to the number of data bits. Codes can be divided into binary ECCs, when data is treated as binary symbols, BCH and Hamming codes, or non-binary ECCs when data is divided into fixed size symbols, such as Reed-Solomon codes. Other divisions are also possible [127].

In this architecture, NAND flash, DDR3 SDRAM, NOR flash and EEPROM are expected to be used. For NAND flash, ECC requirements are often provided by the manufacturer since these devices are susceptible to memory corruption even at sea level. For example, the MLC MT29F32 from Micron requires 24-bit ECC per 1080 bytes of data [128] whilst the SLC MT29F16 from the same manufacturer requires only 4-bit ECC per 540 bytes of data [129]. As shown by Heidecker et al [130], it is important to

test these requirements in operating conditions in order to determine if the ECC overhead is acceptable and/or necessary. Additionally, the variety of orbits and radiation environments of the intended use-cases, requires choosing a particular ECC for each mission. This trade-off process is multi-dimensional and shall include the client in order to target a bit-error rate. [131].

It is interesting to point out the effects of artificial intelligence (AI) in ECC. Classical error correcting codes based on coding theory are now being challenged by AI which "achieve a comparable performance to the state-of-the-art ones. For certain cases, the learned codes may even outperform existing ones", according to Huang et al [132]. Furthermore, the impact of AI processing of downstream products, such as satellite imagery, could affect the error rate requirements of future payload data.

10.1.5. Scrubbing

One can distinguish two types of FPGAs based on their ability to be reconfigured. The first one are antifused-based FPGAs, which can only be programmed once and are seen in rad-hard applications. The second type are reconfigurable FPGAs, either based on SRAM or flash, popular in commercial applications and some rad-tolerant applications. These FPGAs, as opposed to antifuse ones, are known to be susceptible to upsets in configuration bits. The use of adequate mitigation solutions is then necessary to retain the intended functionality [104] [133] [134].

One suggested option to correct upsets in configuration bits of commercial FPGAs is by the use of scrubbing. Scrubbing is the process of reading the configuration memory, detecting any upsets and then partially rewrite that configuration memory, therefore eliminating the errors [135][133]. This process is usually performed automatically and can be implemented in multiple ways with both internal resources and/or additional hardware [135].

A particularity of the Zynq-7000 family is the ability of the ARM processors to assist in rapid scrubbing. Additionally, this family provides dedicated logic with the PL side for detection and correction of upset configuration bits. Stoddard et al [135] presented a hybrid technique which makes use of both these features to allow for faster scrubbing on a Zynq-7020 SoC. This implementation allows for software programmability of the scrubbing architecture whilst using the internal logic features for high speed detection and correction of errors. The scrubber, planned to be used in satellite missions, is able to scan the entire logic with a total scrubbing time of 8ms for SBU and 13.38ms for even MBUs. In the worst case scenario, the internal logic blocks responsible for checking the validity of the configuration bitstream suffers an upset. In this event, a full read-back and reconfiguration of all CRAM bits is required lasting 1.8 seconds.

In the following chapter, the upset rate for SBU in configuration RAM (CRAM) of the Zynq-7020 will be calculated. Radiation testing showed that 89.17% of events are SBU and that only 69 readbacks were required during the more than 42 hour test with 5563 corrected upsets [135]. These results, when compared with the aforementioned upset rate calculations, are key in calculating the system's availability.

10.2. Reconfiguration

Restoring and recovering the system's functionality following a fault or change in configuration is achieved by means of functional monitoring of the system, a watchdog and a particular design of the boot and configuration process.

10.2.1. Functional monitoring

The functional monitoring of the system allows the supervisor to acquire information on the status of the subsystems, information which is relevant to the implementation of FDIR policies. In this system, such perspective is achieved by means of continuous communication and current monitoring. These are able to inform the supervisor of functional interrupts, increases or irregularities in power consumption due to aging effects, SEL or other malfunctions, performance reports and upset rates in memories, to name some.

Continuous communication

The supervisor and adjacent units are connected via a redundant CAN bus. Since the CAN protocol is a multi-master one, it enables all nodes to initiate communication and report on urgent and/or periodic

messages. The content and periodicity of these messages can then be implemented for each mission, thus increasing the flexibility of this architecture.

In one side of the spectrum, the simplest messages exchanged between units and supervisor are a form of watchdog with a 'I am okay' message in-between tasks of the operating system. On the other end, special tasks designed to perform analysis of the unit can be designed. This, when run periodically, provide the supervisor with a better picture of the system status with information such as status of peripherals, usage of SoC resources, SoC temperatures, upset rate statistics, besides others [86].

Due to the configurable logic in the supervisor, an hardware-centric approach to FDIR is possible, further improving dependability. The FPGA can be configured and reconfigured in flight to implement detailed FDIR decision trees as a results of the contents of these communications.

Current monitoring

The current in the power distribution lines for each board are monitored through current sensing resistors and an ADC in the supervisor board. With such information it is possible to determine with greater precision the power sinks in each board and better monitor the performance of the avionics unit, possibly anticipating and preventing faults in certain components. The number of power lines to be measure is dependent on the PSDU design which is out of scope of this project.

The measuring principal is based on Ohm's Law. A resistor is placed in series with the system load and therefore produces a voltage drop across it proportional to the current flowing to the system load. A differential amplifier such as operational amplifier (opamp) translates this difference into a voltage level proportional to it. Such a voltage level can then be sampled by a analog to digital converter and interpreted by a processing unit. Figure 10.2 illustrates this procedure.

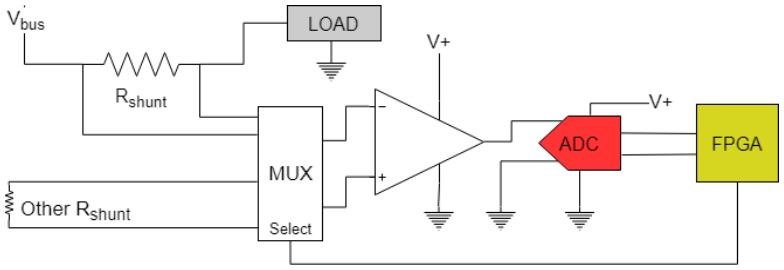


Figure 10.2: Example of a current sense implementation using multiplexing of currents.

10.2.2. Watchdog timer

The supervision of the PLIU and OBC boards is performed by the Supervisor board, which allows for the implementation of flexible FDIR policies. However, the FPGA supporting these functions is itself susceptible to faults. As a means to recover from functional faults affecting the FPGA and prevent overall system failure a watchdog timer is included in the design.

Watchdog timers are by nature simple but provide a valuable function to the system. It is based on the concept that a lack of action is an indication of a fault. A heartbeat signal from the FPGA is received by the watchdog periodically which resets a timer. If this heartbeat signal is not received before the end of the timer period a reset signal is sent to the FPGA. The reset leads to the recovery from said fault if this is not permanent. The timer's frequency can be adjusted according to the application [136]. An example of a typical watchdog timer application is seen in figure 10.3.

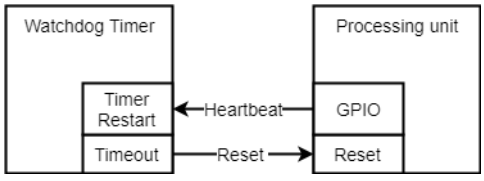


Figure 10.3: Basic implementation of a watchdog timer.

Watchdog timers and the heart beat signals can be implemented in multiple ways. In the case of the timer, this can be a single or multi-stage design depending on the number of timer stages. In a multistage design, successive timeouts trigger staged corrective actions. The generation of heartbeat signal by the processing unit is achievable via software or hardware. An hardware timer is independent on the correct software loop so an infinite program loop is not detect. A more effective method consists on generating this heartbeat at certain locations of the code or after the successful completion of each task [136].

This design considers the use of a single stage watchdog timer connected to the Supervisor's FPGA as a simple but effective method to overcome functional faults in that sub-unit. Without adding significant complexity to the system, it is also an inexpensive option at both component and design level. Watchdog timer circuits can be embedded in the processor or be external, based on capacitors/resistor circuit (RC circuit) or ICs with additional features such as low voltage detection.

10.2.3. Boot and configuration process

The boot and reconfiguration process is an important feature that enables the high availability of this architecture as described in the functional and physical architectures. The individual steps of this process are shown in figure 10.4.

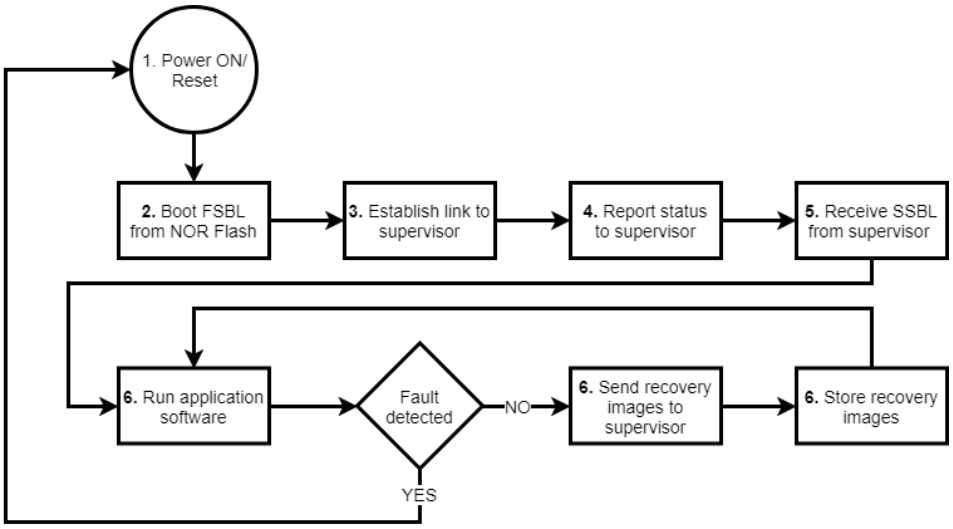


Figure 10.4: Boot and configuration process of the designed architecture.

The process starts with a power on or reset of the OBC or PLIU units (the process is identical for both). The NOR flash in each unit boots a first stage boot loader (FSBL) with basic functionality to enable communications with the supervisor. This is also the moment when status of the unit is provided in order to detect any active faults. With these checks performed, a second stage boot loader (SSBL) is sent over the CAN bus with an application image. This image, which can be either uploaded from the ground, a golden image of the flight software or a recovery image, is then loaded and run. As the application software is running, fault detection is active, depending on the FDIR policy of each mission. Until such a fault is detected, recovery images are sent and stored in the supervisor on a regular basis in order to minimize the downtime when a unit requires reset. In the event a fault requiring reset is detected, the process starts from point 1.

This process, predicted in the SAVOIR architecture, enables the COTS-based avionics unit to have a reliable and controllable booting process. Active faults that might be compromising functionality can be detected early in the booting process and their information stored for future downlink. Additionally, the supervisor unit, by means of FDIR algorithms or ground commands is able to select the most adequate software image for the situation.

10.3. Conclusions

In this chapter, the planned design features that ensure the dependability of the system were presented. This are divided into fault masking and reconfiguration methods.

Fault masking techniques were shown to be available in COTS components as galvanic isolated and fail-safe transceivers and as ECC codes for memory devices. Latchup current limiters based on discrete electrical components limit the impact of high current states before the supervisor is able to take recovery action. Scrubbing techniques for commercial FPGAs were shown to mask SEU in configuration RAM with low impact.

In order to reconfigure the system three methods were selected. First, the functional monitoring using continuous communication between units and supervisor is a method adaptable to each mission. Along with current monitoring, the supervisor acquires a complete view of system status. A watchdog timer in the supervisor is a last resort to reset the supervisor in the unlikely event of functional faults in that unit. To finalize, a boot and configuration process was designed to adapt to this architecture which provides better control of the booting process.

The aforementioned features lead to a dependable architecture which makes use of a reliable supervisor unit to support COTS-based units. The following chapter will analyze the effects of radiation on a variety of COTS technologies, further supporting this selection of protection systems.

11

Radiation Effects Analysis

The effects of radiation in COTS electronics is one of the first topics mentioned when debating the use of these devices in space. A large effort has been put by agencies such as NASA and ESA to test and characterize the behaviour of a number of devices in these environments.

Building on that knowledge, this chapter provides dependability figures that help better understand the suitability of target commercial devices in a number of orbits. This is achieved by using laboratory tests results from a pool of devices and then calculating the single event rates and total accumulated doses for selected orbits. First, these orbits are presented and characterized using ESA's SPENVIS tool. Then, event rates for SEL, SEFI, SEU and SET are given for susceptible devices as well as tolerance to accumulated doses.

At the end of this chapter, an overall picture of the effects of radiation in the target technologies is accomplished. It is demonstrated that the upset rate is tolerable and that destructive events are uncommon. This supports the calculation of the system specifications of the following chapter and premise that COTS components can be utilized in an avionics with high availability and reliability figures.

11.1. Radiation environment modelling

The first step to determine the consequences of radiation on electronics is to model the environment these will be subjected to. Since the radiation environment in space is constantly changing, both spatially as well as temporally, it is important to consider these aspects when performing analysis. In addition, the effective shielding provided by casings and the spacecraft is another essential variable affecting the experiments. The modelling of the radiation environment and its effects was performed with the assistance of the SPENVIS software, taking into consideration best and worst case scenarios of the space weather, shielding thicknesses and three reference orbits.

11.1.1. SPENVIS

SPENVIS is an ESA web-based software providing standardized access to models of the space environment. It was developed and maintained at BIRA-AISB since 1996 and it is usage is free of charge, although registration is required. Despite its ease of use, this tool generates valuable information for a system designer who wants to trade-off technologies or determine dependability figures [137].

Models for a variety of radiation sources are available in SPENVIS, such as the natural radiation belts, solar energetic particles and cosmic rays. The tool is used by scientists and engineers to perform quick analysis of the environment their spacecraft will be operating in, generating radiation fluxes and fluences and calculating radiation doses (ionising and non-ionising) for simple geometries. Most importantly, SPENVIS provides means to calculate upset rates in sensitive devices. For these reasons, it is used in this project to aid the radiation hardness assurance process.

11.1.2. Space weather scenarios

The cyclical activity of the Sun is paramount to correctly predict and model the radiation environment in our solar system. Its activity levels have an approximate 11 year cycle which are related to the number of sunspots visible on its surface. For solar maximums, lasting approximately 7 years, the

number of sunspots is higher and the flux of particles is increased. The following 4 years of solar minimum are characterized by low to non-existent sunspots and much lower flux [19]. This activity strongly influences the trapped electrons and protons in LEO, thus affecting the radiation environment closer to Earth. At solar minimum, trapped proton fluxes reach their maximum, similarly to what happens with electrons. Lastly, galactic cosmic ray fluxes are also maximized during solar minimum. [138]

Currently, the solar activity is declining and predicted to reach a minimum in late 2019 or 2020, according to NOAA, the National Oceanic and Atmospheric Administration. For the purpose of this analysis, a 2021 mission is modelled, considering a probable roll out of the proposed avionics. This puts the mission in between the current solar minimum and the expected solar maximum, occurring sometime between 2023 and 2026. For these reasons, and to better understand the response of COTS electronics to the space environment, best case and worst case conditions are taken into account, as described in the following paragraphs.

Best case scenario

During periods of reduced solar activity the flux of particles originated from the Sun heading towards the Earth is greatly reduced. The main sources of ionization are, therefore, only the trapped particles and galactic cosmic rays. In this scenario, the flux of particles with energies above the threshold to cause SEE in a device is low and one expects that the rate of this events is also low. Additionally, the dose of ionization radiation a device is subjected to is also at its lowest. The best case scenario generates optimistic results and an ideal case for the system.

Worst case scenario

In an opposite fashion, the worst case scenario is developed to represent the worst conditions one might find in orbit. It occurs during solar maximums where solar flares are responsible for bursts of high energy protons and heavy ions. Such high energy particles then lead to increased rates of SEE such as upsets and latchups and an increase in total accumulated dose. This pessimistic outlook provides a ceiling to the calculation and, in conjunction with the best case scenario, a range of expected SEE rates. The details on the models and respective configurations used for both scenarios in the SPENVIS tool are given in table 11.1.

11.1.3. Shielding

Multiple materials are used to shield sensitive spacecraft parts against harmful radiation or debris. In fact, this is a standalone research subject by itself, with particularly important results for human space exploration. The spacecraft structure, other subsystems, the avionics casing and even spot shielding shall be considered when performing radiation analysis. For standardization purposes, aluminum-equivalent thickness is used in most literature, in particular results are given considering a 100 mils thickness (which corresponds to approximately 2.5mm). Additionally, this is also a commonly used thickness in aluminum casings.

It is important to consider the cost/benefit ratio of increasing shielding as the reduction in SEE rate and total absorbed ionizing dose do not scale linearly with this increase. In particular, TID levels are known to plateau after a certain shielding thickness. Beyond this point, additional shielding will have a low impact on TID levels and SEE rates [139].

This effect is seen in figure 11.1, which shows the accumulated dose as a function of aluminum-equivalent absorber thickness for a 1200km orbit in best case conditions (corresponds to the High LEO orbit in 11.2). The graphic is also representative of all other orbits and weather scenarios. It is visible that at roughly 5.0mm aluminum absorber thickness, the total dose, represented by hollow squares, does not significantly decrease. Assuming a 2.5mm aluminum casing for the avionics, and depending on the shielding offered by the spacecraft structure and associated subsystems, a total of 5.0mm shielding is a meaningful representation of a possible use-case.

Following the observations mentioned above, two shielding thickness will be utilized in this study, 2.5mm and 5.0mm aluminum-equivalent.

11.1.4. Reference orbits

The study shall provide insightful results which correctly sample the heterogeneous radiation environments the avionics might be subjected to. Therefore, three reference orbits were selected for

Weather Scenario	Best-Case	Worst-Case
Trapped Protons Model	AP-8	AP-8
Model Version	Solar Minimum	Solar Maximum
Threshold flux (/cm^2/s)	1	1
Trapped Electrons Model	AE-8	AE-8
Model Version	Solar Minimum	Solar Maximum
Threshold flux (/cm^2/s)	1	1
Trapped Protons Anistropy	None	None
Solar Particle peak fluxes	—-	CREME96
Ion range	—-	H to U
Version	—-	Worst Week
Magnetic Shielding	—-	On, all directions, quiet, Stormer with eccentric dipole, unchanged
Solar particle mission fluences	ESP-PSYCHIC (total fluence)	ESP-PSYCHIC (total fluence)
Ion Range	H to U	H to U
Confidence Level	95%	195%
Magnetic Shielding	On, all directions, quiet, Stormer with eccentric dipole, unchanged	On, all directions, quiet, Stormer with eccentric dipole, unchanged
GCR Model	ISO 15390	ISO 15390
Ion Range	H to U	H to U
Model Version	ISO-15390 standard model	ISO-15390 standard model
Solar Activity data	Mission Epoch	Mission Epoch
Magnetic Shielding	On, all directions, quiet, Stormer with eccentric dipole, unchanged	On, all directions, quiet, Stormer with eccentric dipole, unchanged
Shieldied Flux	0,1 thickness	0,1 thickness
Ta to Al mass ratio	0	0

Table 11.1: Details on the configuration of SPENVIS and its radiation models for best-case and worst-case space weather scenarios .

this study. These follow not only from the findings of chapter 4 but also from the known geographical variations of trapped protons and electrons. The sample contains low altitude missions at medium and high inclinations, with the ISS and RapidEye2 (named SSO for sun-synchronous) orbits, and a high altitude LEO as the one expected for the future OneWeb constellation (named High LEO). The orbital elements are derived from `heavens-above.com`, a website hosted by the DLR Space Operations and Astronaut Training, dedicated to the tracking of known satellites. A mission duration of 5 years is selected following requirement SR-R02 in table C.8. A summary of the reference orbital parameters is given in table 11.2.

11.1.5. Limitations of the analysis

As with any experiment, this one has a set of limitations and uncertainties that affect the validity of its results. A number of these limitations were identified by the author and can be categorized into four main sources:

- **Accuracy of chosen radiation models**: A variety of factors affect the accuracy of the chosen models, including under-sampling and simplification of the environment. It is accepted that for most models orbit-averaged quantities are reliable within a factor of two [140].

- **Modelling of the environment**: The selection of parameters for this analysis follow the suggestions in literature and are thought to represent the best and worst case scenarios, thus providing a range of results. However, the changing space weather conditions and wide range of possible operating orbits, are a source of variance in the results.

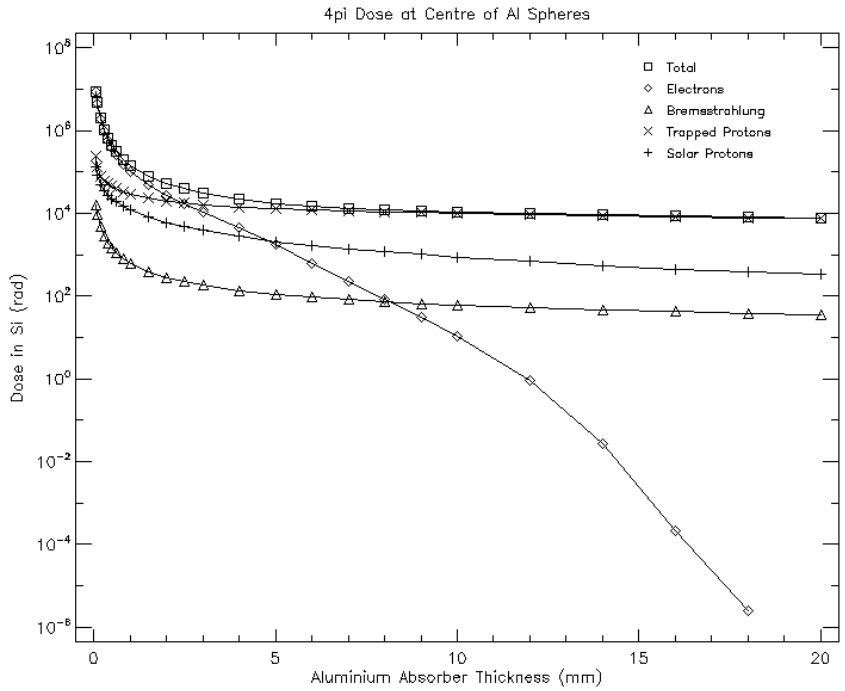


Figure 11.1: Total absorbed dose in Si (SRIM2008) at High LEO orbit in best case conditions. The target Si is modelled at the center of aluminum spheres for calculation purposes. Notice the contribution of trapped protons compared to other species. Generated with SPENVIS.

- **Quality of input data**: The accuracy of this analysis is highly dependent on the accuracy of its input data. This is retrieved from literature and is often incomplete or indirectly determined. Variations in fabrication process of COTS devices might affect the applicability of previously performed radiation tests. Additionally, assumptions in the sensitive dimensions of the devices, which have a great impact in the results, are made since these are not shared by the manufacturer.
- **Simplification of radiation effects**: The nature of radiation effects is complex and stochastic by nature, considered to follow a Poisson distribution. In the calculation of SEL, a binary view of the subject is employed, considering every particle above a certain threshold level to cause an event. Additionally, this analysis only considers heavy-ions when calculating SEE rates (direct ionization). This simplification is due to the lack of consistent data on proton sensitivity for multiple devices and also due to the much higher sensitivity to heavy ions. The analysis also does not consider the increase in cross section with temperature.

Despite these sources of uncertainty in the results, it is thought that by sampling best and worst

Orbit name	**ISS**	**High LEO**	**SSO**
Mission duration [years]	5		
Trajectory duration [days]	1		
Orbit start date	01/01/2021		
Perigee [km]	409	1200	612
Apogee [km]	419	1200	627
Inclination (i) [º]	51.64	86.40	97.74
Right ascension of ascending node [º]	270.59	0.00	254.1
Argument of perigee [º]	113.67	0.00	72.89
True anomaly [º]	246.52	0.00	287.36

Table 11.2: Orbital parameters for the chosen reference orbits. Data collected from heavens-above.com, 05/07/2019 at 08:45 ECT.

case conditions, it is possible to determine a range of event rates that support the conclusions.

11.2. Comparison of radiation environments

There are notable differences in the spectrum and flux of radiation particles in the three reference orbits. This section presents the radiation environments in each of these orbits, with attention to the differences in total accumulated doses, contribution of different species, particles fluxes and the effects of shielding in these parameters.

11.2.1. Total ionizing dose

The total ionizing dose accumulated for the reference orbits at best and worst case scenarios are shown in figure 11.2. In it, it is possible to see the amplitude of TID which might be encountered by the avionics. This amplitude is explained by the weather conditions and also the contribution of trapped protons and electrons. At higher inclinations, the High LEO and SSO orbits, are expected to cross regions with higher concentrations of trapped protons and electrons, the largest contributors to the accumulation of radiation. Additionally, the highest flux of electrons during solar storms is the greatest contributor to the higher TID in worst case conditions.

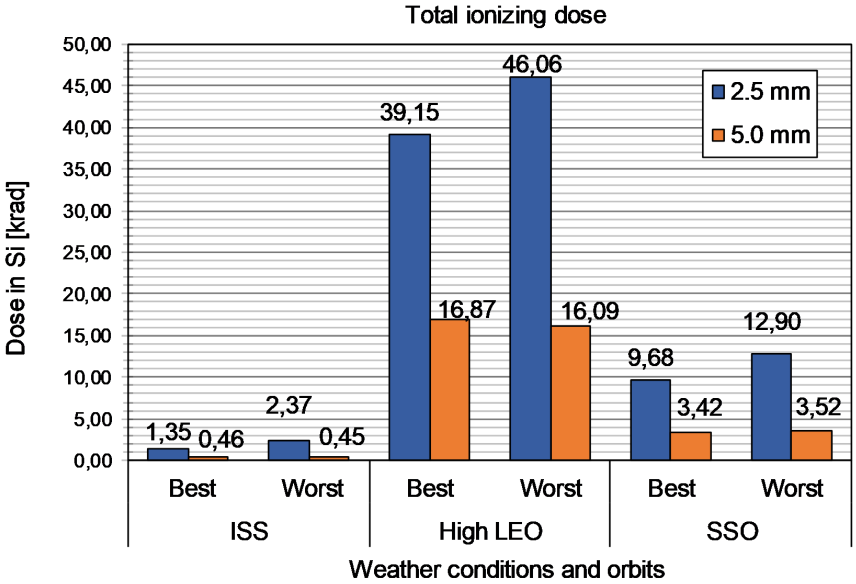


Figure 11.2: Total ionizing dose absorbed for all reference orbits and weather conditions. Notice the much higher dose for the High LEO orbit and the relative effect of shielding across orbits. The target silicon material is modelled at the center of aluminum spheres with 2.5mm and 5mm thicknesses. Calculated using the SHIELDOSE-2 model from SPENVIS.

Furthermore, figure 11.2 also displays the effects of the shielding thickness. As mentioned in 11.1.3 and seen in figure 11.2, there is a significant reduction in accumulated dose with an increase of shielding up to 5.0mm aluminum-equivalent thickness. For example, at the High LEO orbit in worst case conditions, TID can be reduced by 65% and set at a more acceptable level of 16 krad. This reduction translates into an effective increase in the number of commercial devices to choose from and a reduction in the risk of TID related effects such as increases in power consumption. However, it is important to consider the consequences of the application of this equivalent thickness for each particular spacecraft as different materials produce distinct secondary species and energy spectrums, some of which might be more sensitive to target device, as described in the literature study [16].

11.2.2. Shielded flux

A cocktail of ionizing particles hit target volumes in the space environment. This flux of particles is dependent on the orbital environment, shielding material and thickness it crosses before arriving at the sensitive volume. In order to determine the effects of radiation it is necessary to calculate the flux of particles with these variables. The results are presented in the following paragraphs.

In figure 11.3 it is possible to see the typical shielded flux, in this case, after a 2.5mm Al-equivalent shield at the SSO orbit in best case conditions. The graph presents both the differential flux, that is the number of particles with a certain LET crossing thought an area and time (solid line), and the integral flux, the cumulative number of particles above a certain LET crossing thought an area and time (dashed line). Both lines follow a similar trend, with values decreasing with an increase in LET. Most noticeably is the so-called "iron knee", the three decade reduction in integral flux from $25e4MeVcm^2/g$ to $35e4MeVcm^2/g$. This behaviour, similar in all orbits and conditions, translates into a much lower event rate for devices with an sensitivity threshold above that energy transfer level. Therefore, it is used as a rough parameter to assess the sensitivity of a device, with devices above the iron knee being considered radiation tolerant. Similarly, there is also a significant drop at around $60e4MeVcm^2/g$ with the plot ending at $1e5MeVcm^2/g$. Devices with onset values at or above $1e5MeVcm^2/g$ are usually known as radiation hardened devices due to the extremely low probability of encountering particles with LET above that threshold [141].

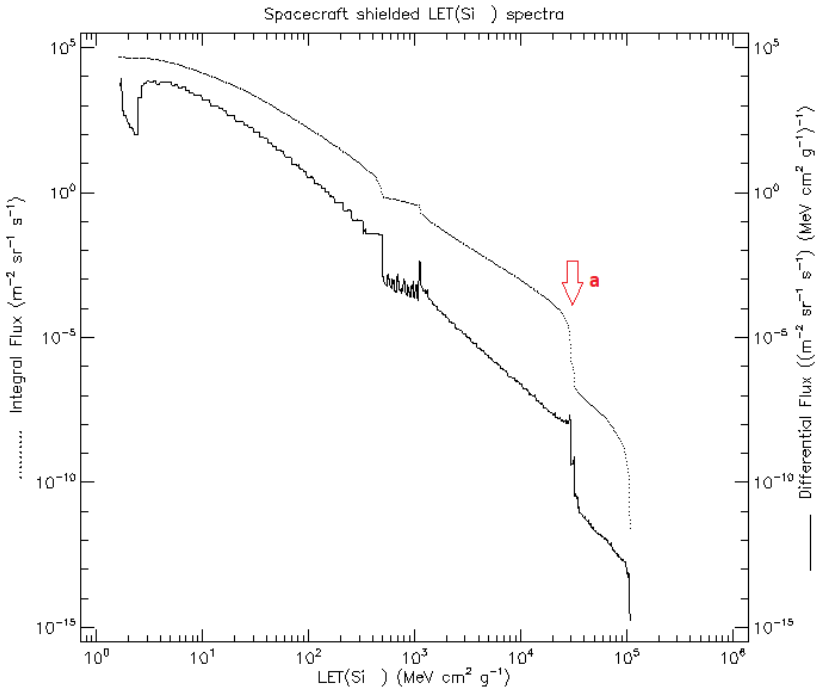


Figure 11.3: Shielded flux for SSO orbit in best-case conditions and 2.5mm Al-equivalent shielding. Notice iron knee market with red arrow. Calculated with SPENVIS' short-term SEU rate tool.

The effects of shielding in the shielded flux is a relevant parameter as a reduction in shielded flux translates into a reduction in event rate. The following plots, figure 11.4 and 11.5, represent the effects of shielding and orbital environments at three different LET levels in the integral flux. These energy levels were chosen to represent devices with thresholds around the iron knee and their applicability is noticeable by analysing the thresholds for latchup in table 11.5. The first value at $16e4MeVcm^2/g$ represents the Zynq-7000 SoC, $30e4MeVcm^2/g$ is right after the iron knee and $60MeVcm^2/g$ represents the standard threshold for space qualified NAND memories.

Four main conclusions can be draw for the above plots. The first one is that the High LEO and SSO orbits have similar fluxes which are higher by around an order of magnitude compared to the ISS orbit. The second is that the difference in flux from best case to worst case conditions is an increase of around two orders of magnitude. The third is the one order of magnitude reduction in flux when shielding is increased from 2.5mm to 5mm in worst case conditions. The final one is the inability of shielding to affect the integral flux in best case conditions with the particularity that for the ISS orbit increasing the shielding produces a slight increase in integral flux at lower LET levels.

The findings suggest that one shall expect significantly lower event rates at low altitude, low inclination orbits, compared to high inclination and/or higher orbits. Additionally, increased in shielding thickness is found to be most useful in reducing event rates in the event of high solar activity, similar

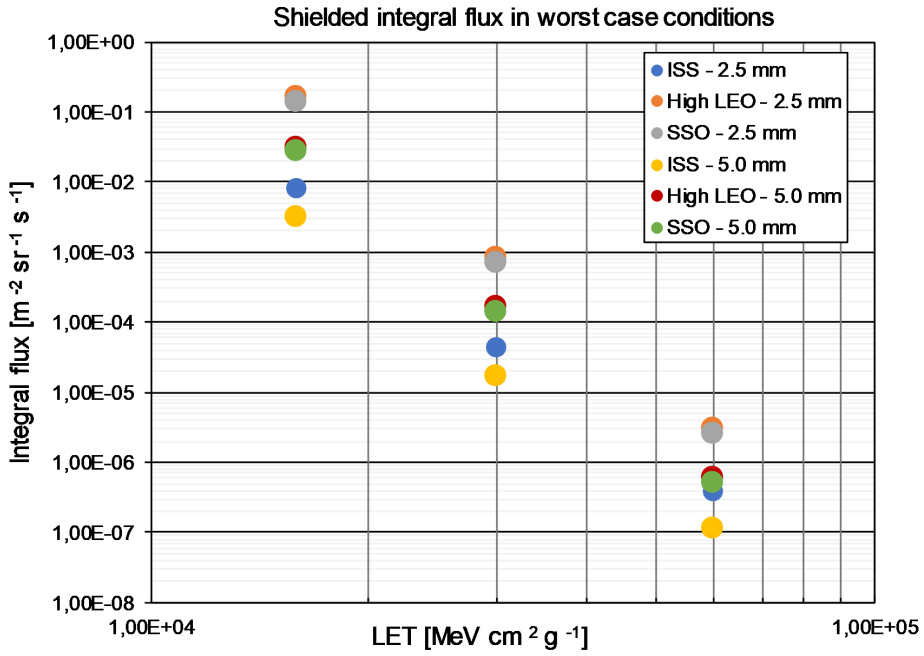


Figure 11.4: Shielded integral flux in worst case conditions. Notice that the points in the plot representing the following orbits are overlapping: SSO 5.0mm and High LEO 5.0mm. Also, SSO 2.5mm e High LEO 2.5mm are also overlaped.

to the conclusions for TID.

11.3. Radiation hardness assurance

Considering the radiation environments presented in the previous section, it is now possible to estimate the effects these will have on some susceptible devices. In this section, a number of commercial devices selected as meaningful building blocks of the avionics will be analyzed in comparison with counterparts qualified for use in space. Event rates for SEE (SEL, SEFI, SEU and SET) and total tolerable dose will be presented.

The successful and meaningful calculation of upset rates is dependent on a number of factors. In particular, the acquisition of a number of test results that characterize the response of each device to certain radiation energy levels as well as other characteristics dependent on the physical construction of said device are paramount. A review of these testing methods was already performed in the literature study [16]. For those reasons, it was soon established that a large research into scientific publications was required to gather this data. Additionally, this research provides guidance into what devices and technologies are currently in focus for the scientific and engineering communities.

The devices presented in the following subsections are thought to be representative of the state-of-the-art in COTS for space application at the same time it was possible to gather complete and meaningful test results to feed the calculations. Some comparisons between devices are provided both between COTS and their space-qualified counterparts and also between different technologies. In table 11.3, a division into different categories according to the radiation tolerance of each devices is presented.

Category	**TID [krad (Si)]**	SEE $L_{th}[MeVcm^2/mg]$	**Latch-up behaviour**
Commercial	2-20	<5	Not known
Rad-tolerant	20-100	20	Threshold above iron knee
Rad-hard	>100	>60	None

Table 11.3: Categories of radiation tolerance according to TID, SEE and SEL behaviour, as suggested by Furano et al [14]. The iron knee is the three decade drop in radiation integral flux usually between from 25 to 35 MeV.cm2 mg.

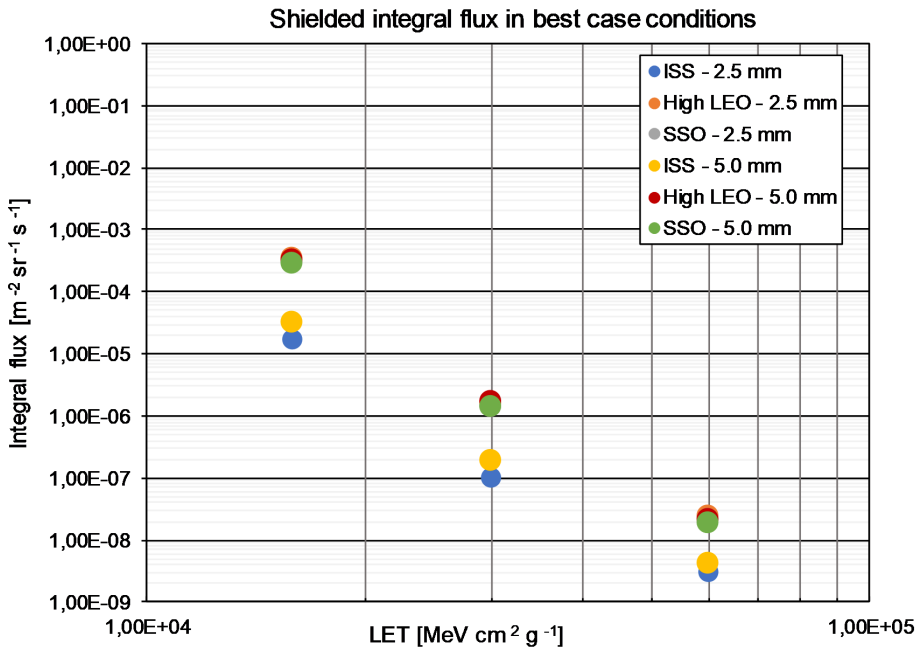


Figure 11.5: Shielded integral flux in best case conditions. Notice that the points in the plot representing the following orbits are overlapping: SSO-5.0mm, High LEO-5.0mm, SSO-2.5mm and High LEO-2.5mm.

11.3.1. Total ionizing dose

The tolerable dose for each device is a figure that represents the value at which the device loses some or all of its functionality due to the accumulated radiation. These figures are usually determined by exposing the device to radiation and testing it at certain dose levels. In table 11.4, a compilation of these values is presented for a variety of IC types.

Device	Function	Category	TID [krad (Si)]
Zynq [134]	Processing	Rad-hard	126
GR712 [142]	Processing	Rad-hard	300
SN55HVD233-SP [31]	CAN Transceiver	Rad-hard	>50
SN65HVD251 [143]	CAN Transceiver	Rad-tolerant	(few tens)
MT29F32 (MLC) [129]	NAND Flash	Rad-tolerant	22
MT29F16 (SLC) [128]	NAND Flash	Rad-tolerant	63
3DFN	NAND Flash	Rad-tolerant	60

Table 11.4: TID before appearance of faults for a selection of COTS and space qualified components. Although not found in literature, it is expected that the MT29F128 (MLC) has similar to better TID tolerance than the other Micron memories since it is built with a smaller feature size. Values for 3DFN from 3D Plus website (3d-plus.com) consulted in 25th July 2019.

As it is easily concluded by comparing the table above with figure 11.2, all devices are expected to work without issues with the end of life accumulated dose except for the SN65HVD251 and the MT29F32. These are prone to TID induced failure in low shielding High LEO orbits.

11.3.2. Single event latchup

In this subsection, research into the expected latchup rates for the most susceptible devices is presented. Evidence suggests that the danger of latchup events is reduced and tolerable for the target technologies.

The methodology to obtain the events rates is based on a simplification to allow the generation of meaningful results despite the lack of reliable information. In particular, it was observed that published test results provide a binary view of SEL, with the assumption that SEL occur above a certain threshold LET and not seen below this level. Also, cross-sections are often not provided for SEL. The assumption

of sensitive areas based on physical dimensions of the device are a large source of errors as the actual sensitive area for SEL is much smaller. Solely the SEL sensitive area for the Zynq-7000 VccAux power input was found in literature [30].

Considering these limitations, event rates for Zynq-7000 VccAux line (on FPGA side) were calculated as the product of the integral flux, in figures 11.4 and 11.5, at the threshold LET, in table 11.5, and the sensitive area, as used by Cruz-Colon et al [31]. This method, known as the RPP method, is conservative by nature as it assumes that all particles above the onset energy level lead to an event. For the other devices shown in the table, only comparisons of threshold LET is possible. Nevertheless, this comparison, alongside the integral fluxes in the above graphs, leads to some conclusions related to the radiation tolerance of these devices.

Device	**Function**	**Category**	$L_0[MeVcm^2/mg]$
Zynq [134]	Processing	Commercial	16*
GR712	Processing	Rad-hard	118
SN55HVD233-SP [31]	CAN Transceiver	Rad-hard	>90
SN65HVD251 [143]	CAN Transceiver	Rad-tolerant	>25
MT29F32 (MLC) [129]	NAND Flash	Rad-tolerant	>60
MT29F16 (SLC) [128]	NAND Flash	Rad-tolerant	>60
3DFN [1]	NAND Flash	Rad-tolerant	>62,5

Table 11.5: Threshold LET for SEL for a selection of COTS and space qualified components.Although not found in literature, it is expected that the MT29F18 (MLC) has similar latchup behaviour as the other MT29F memories. *: micro-latchup with steps of approximately 0.1A recovered only by power cycle.

In figure 11.6, it is possible to see the expected latchup rates for the Zynq-7000 VccAux power input for the reference orbits, in both best and worst-case scenarios and also for two distinct shielding configurations. The event rates are linked to the behaviour of the shielded flux as discussed in 11.2.2. One can see that the event rate for the most inclined orbits is substantially larger than at the ISS orbit. Also, the effect of shielding is most noticeable in worst case conditions. For the ISS orbit, as seen with the shielded flux, increasing the shielding leads to higher event rate due to the effects of secondary particles generation. Besides these variations it is also important to consider the magnitude of the event rate. Most noticeably, at the High LEO orbit, in worst cased conditions and low shielding the event rate is $5.12e-3$ events per day which translates into one event roughly every 195 days. Additionally, these are known to be micro-latchup events with steps of approximately 0.1A [123]. [2] The lowest calculated event rate is for the ISS orbit in best case conditions and 2.5mm shielding at $5.15e-7$ or more than five thousand years mean time between events.

The calculated results demonstrate the large influence of the space weather environment on the number estimated latchup events. Even the worst estimate is that latchups are to be expected around twice a year. The lower criticallity of the micro-latchup behaviour in addition the calculated event rates suggest that these faults are tolerable and correctable if detection and recovery mechanisms are available [144].

As seen in table 11.5, the threshold for latchup of the other devices is higher than that of the SoC. Besides the SN65HVD251 CAN transceiver, all other devices have a threshold above the iron knee, substantially reducing their susceptibility to latchup events. The three decade reduction in flux across the iron knee, if one assumes the same sensitive area for all devices, means that other devices should experience latchup events three orders of magnitude less frequently than the Zynq-7000 SoC, making it the most vulnerable part of the system. This is corroborated by the latchup thresholds for a number of other MCUs and SoCs compiled in the literature study [16], which suggest that these processing units are in fact more prone to latchup than other ICs.

11.3.3. Single event transients

Differential bus transceivers are used in space for multiple communication protocols from CAN to RS-485 to SpaceWire. The SET behaviour under heavy ion exposure of a COTS transceiver and its space qualified counterpart are compared in the following paragraphs.

[2] For reference, according to Zynq's power estimation tool, the VccAux input with fully used FPGA resources on the Zynq-7020 does not exceed more than 0.4A.

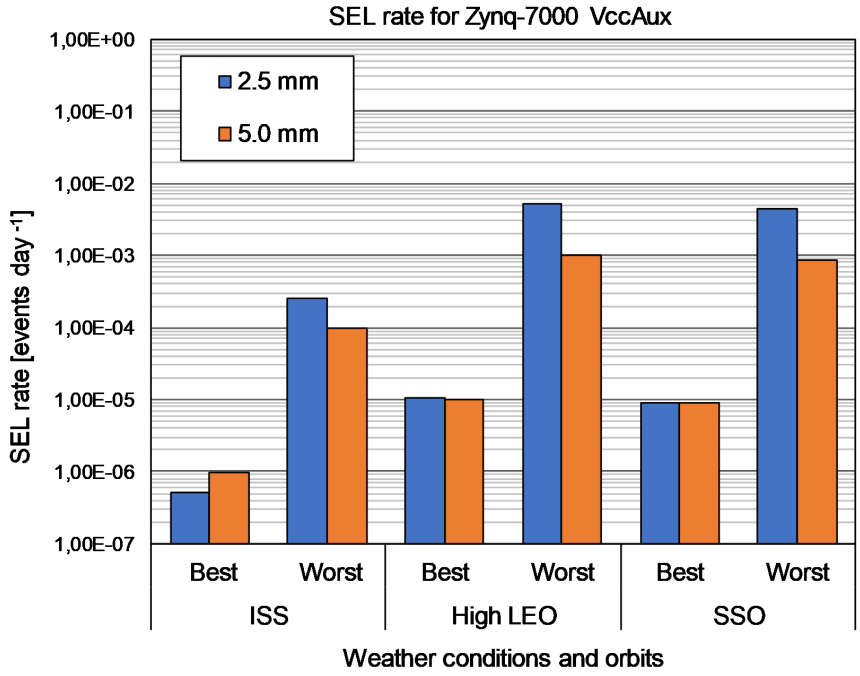


Figure 11.6: Expected latchup rates for the Zynq-7000 VccAux power input for the reference orbits, weather conditions and shielding thicknesses.

Transient effects at the receiver outputs might be sensed under exposure to heavy ions and protons. Pulses can either be positive or negative going signals with heights reaching rail voltages. Usually, SET are detected by setting a certain trigger voltage during exposure. The Weibull parameters for two functionally-similar CAN transceivers are presented in table 11.6, the COTS SN65HVD251 and the qualified SN55HVD233-SP. The lowest L_0 in the commercial device is balanced by its lower cross-section.

Device	$\sigma_{sat}[cm^2]$	$L[\mu m]$	$t[\mu m]$	$L_0[MeVcm^2/mg]$	$W[MeVcm^2/mg]$	$S[-]$
SN55HVD233-SP [31]	1.93-4	138.92	2	4.5	28	1.56
SN65HVD251 [143]	1.00E-4	100.00	2	1.2	∆	∆

Table 11.6: Device and Weibull parameters for the heavy ion exposure of a COTS (SN65HVD251) and a rad-hard (SN55HVD233-SP) CAN transceivers. The calculation assumes as a sensitive volume a rectangular parallelepiped of sides **L** by **L** and thickness **t**. The sides of the parallelepipeds are obtained from saturation cross sections. The thicknesses are assumed equal for both devices at 2 μm [15]. ∆: Data points used instead of Weibull parameters.

There are two main factors affecting the accuracy of this particular comparison. First, the assumption on the thickness of the sensitive volumes. Due to missing data, it was assumed that the thicknesses of the sensitive volumes are equal for both devices at 2 μm as is a standard in literature. However, Inguimbert et al have demonstrated that this is not always adequate [15]. The second factor is related to the device's bias conditions since it affects pulse widths and amplitude. In this comparison, the input data considers the SN55HVD233-SP at 3V3 bias and the SN65HVD251 at 5V. Nevertheless, Koga et al [143] tested other transceivers (SN65HVD10/11/12/72), functionally similar to the SN65HVD251 at 3V3 bias with similar response to heavy ions and protons.

Using the parameters in the table and the previously presented environmental models it is possible to calculate the number of expected transient events using SPENVIS' short-term SEU rate tool. These results are shown in figure 11.7. The results reveal that the SN55HVD233-SP is less prone to these events, with a typical reduction in event rate of around one order of magnitude compared to the other device. This is mostly justified by its higher onset LET for SET, although this difference is less noticeable compared to the onset values for SEL.

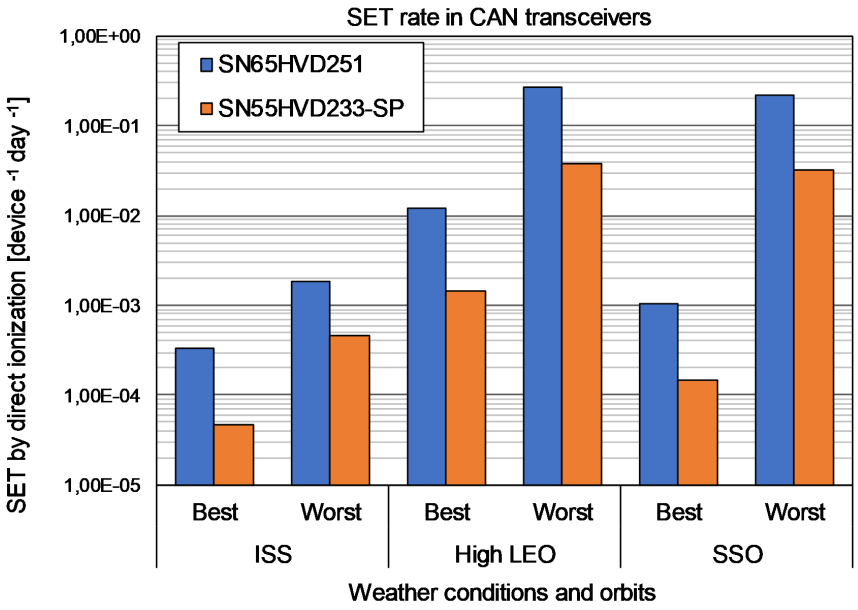


Figure 11.7: Results of the SET rate by direct ionization for a COTS (SN65HVD251) and a rad-hard (SN55HVD233-SP) CAN transceivers. Assumes a 2.5mm aluminum-equivalent shielding. Calculated with SPENVIS' short-term SEU rate tool.

The actual event rate for both devices fluctuates between $3.14e-5$ and $3.82e-2$ events per day and $2.05e-4$ and $2.63e-1$ events per day, for the HVD233-SP and HVD251 respectively. These are both obtained at 5.0 mm shielding in the best case ISS and worst case High LEO environments. Such event rates, when converted into mean days between events, suggest that one is not to expect more than a couple of transient events per week even in the worst case environment with a commercial device. This suggests that, default error handling methods employed in protocols such as the CAN bus, are sufficient to handle single bit errors caused by transients.

11.3.4. Single event upsets

Storage of platform and payload data in this architecture is performed by NAND devices. This information is stored in floating gates, depending on the presence or absence of trapped charged on an isolated conductor. The technology is sensitive to radiation effects in particular single event effects. The origins for upsets in NAND devices are attributed to either the internal control circuitry as well as floating gates [111].

As previously described, MLC and TLC technologies store more bits per floating gate cell than SLC devices. This reduces margins within each stored voltage level, decreasing threshold in energy deposition in order to induce an upset. At the same time, feature sizes are shrinking. However, the trend is for SEU cross-sections to increase and devices to either be more sensitive in the control logic or floating gate arrays [111] [130].

Characterization of memories in radiation environments is a complex ongoing subject. This subsection focuses on determining SEU rates for NAND memories which are in the interest of ESA and for which a number of reports are available. In particular, both SLC and MLC technologies for Micron's MT29F series NAND flash devices are compared. Three devices sharing the same package dimensions and functionality are considered, at 128Gbit (MLC), 32Gbit (MLC) and 16Gbit (SLC).

Furthermore, the internal memories of the Zynq-7000 SoC are also analyzed. These include internal on-chip memory (OCM), configuration memory for the PL (CRAM) and the block RAM also associated with the PL (BRAM). No data on the internal cache sensitivity to heavy ions was available, believed to be a limitation of the test software [123]. However, proton sensitivity results are available [145]. The characterization of these devices is given in table 11.7.

The rate of events per bit per day, for the Micron memories is given in figure 11.8. It is possible to observe the lower upset rate in the SLC device compared to the MLC counterparts. This behavior is expected and is important when performing trade-offs. Additionally, it is possible to see that the 32Gbit device is more prone to upsets than the higher capacity 128Gbit device. This is thought to be

Device	$\sigma_{sat}[cm^2/bit]$	$L[\mu m]$	$t[\mu m]$	$L_0[MeVcm^2/mg]$	$W[MeVcm^2/mg]$	$S[-]$
MT29F128 (MLC) [146]	1,50E-10	0,12	0,10	0,89	40.0	0,9
MT29F16 (SLC) [128]	1,60E-10	0,13	0,10	2,85	38.0	1,1
MT29F32 (MLC) [129]	6,00E-10	0,24	0,10	0,35	50.0	1,3
Zynq OCM [147]	2,50E-09	0,50	0,10	8,40	△	△
Zynq BRAM [134]	2,00E-09	0,45	0,10	0,5	12,5	0,7
Zynq CRAM [134]	1,40E-09	0,37	0,10	0,5	14.0	0,6

Table 11.7: Device and Weibull SEU parameters for a selection of memories. The calculation assumes as a sensitive volume a rectangular parallelepiped of sides **L** by **L** and thickness **t**. The sides of the parallelepipeds are obtained from saturation cross sections and the thicknesses from the cited sources. △: Data points used instead of Weibull parameters.

explained due to the 25 nm to 16nm reduction in feature size. In this case, the shrinking lead to an effective reduction in cross-section per bit since both are MLC devices. For comparison, the 16Gbit SLC device despite being built using a 34 nm process has similar cross-section per bit as the 128Gbit device due to the SLC technology. Furthermore, this distinction between SLC and MLC technologies is noticeable in the threshold LET for upset, L_0, with the MLC devices being susceptible to upset for particles at much lower LET levels.

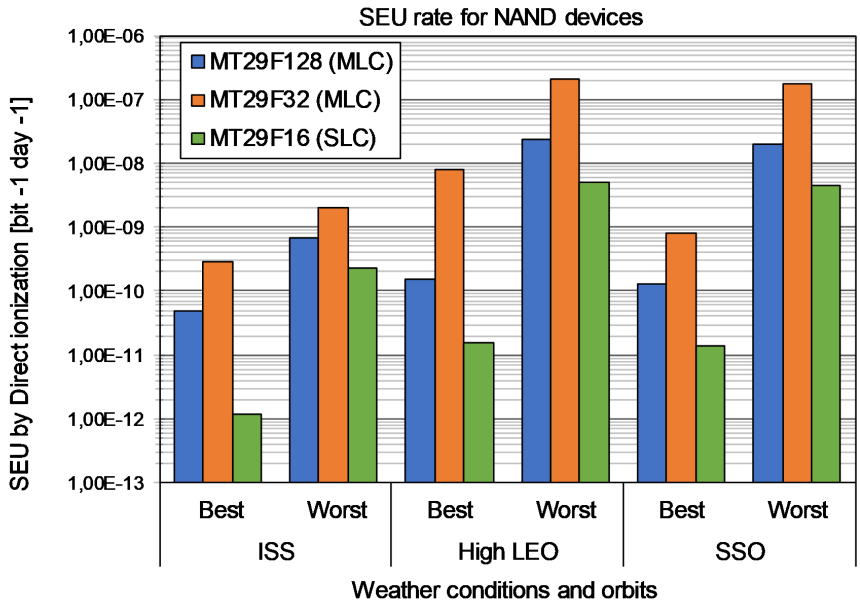


Figure 11.8: Upset rates for the NAND flash memories assuming a 2.5mm aluminum-equivalent shielding. Notice the effect of the changing orbits and weather conditions for each device. It is also interesting to notice the consistently lower upset rate of the SLC memory compared to the MLC counterparts. Calculated with SPENVIS' short-term SEU rate tool.

The simulation results of the internal memories of the Zynq SoC are seen in figure 11.9. In it, the SEU rate for the three internal memories with 2.5mm shielding is shown for all orbits and weather conditions. One can observe the similarities in the PL side memories, OCM and BRAM, and their higher sensitivity compared to the OCM. In fact, the former consistently displays one to two orders of magnitude more events than the latter. Hence, it is to be expected that upsets in the PL segment are more frequent than on the PS segment.

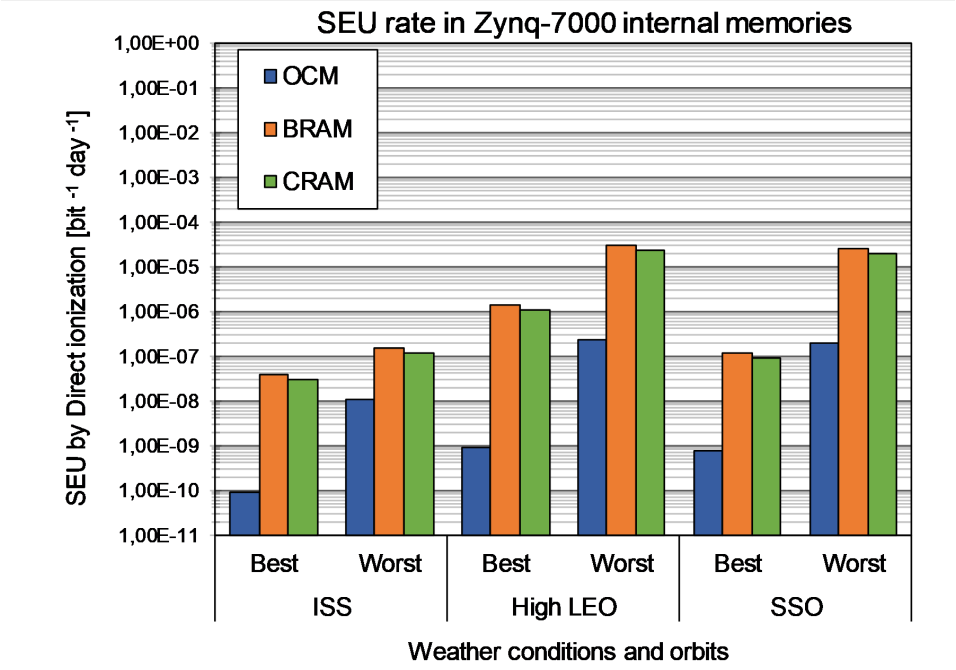


Figure 11.9: Results of the upset rates calculation for the Zynq internal memories assuming a 2.5mm aluminum-equivalent shielding. The OCM is shown to be less susceptible to upsets, with BRAM and CRAM presenting similar behaviours.Calculated with SPENVIS' short-term SEU rate tool. Columns from left to right: OCM, BRAM and CRAM.

11.3.5. Single event functional interrupt

The rate of SEFI for both NAND Flash and the Zynq-7020 SoC is calculated in this subsection.

NAND Flash

Functional interrupts in NAND flashes are due to control logic errors, leading to malfunctions in parts or the entire memory device. These errors may be found when reading certain columns, rows or blocks when the device is powered on [148]. SEFI are a more significant problem in modern flash memories than bit errors since the former requires recovery by reset or power cycle whilst the latter is correctable using ECC methodologies [149].

Similarly to what was previously performed, two NAND memories from Micron were analyzed to compare SLC and MLC technologies. The SEFI characterization of a 32Gbit MLC and a 16 Gbit SLC memories is shown in table 11.8. These values are then used to calculate SEFI rates according to orbit and weather conditions as it is seen in figures 11.10 and 11.11.

Device	$\sigma_{sat}[cm^2]$	$L[\mu m]$	$t[\mu m]$	$L_0[MeVcm^2/mg]$	$W[MeVcm^2/mg]$	$S[-]$
MT29F16 (SLC) [128]	1.20e-5	34.64	1.00	3.90	23	1.5
MT29F32 (MLC) [129]	1.13e-4	106.30	2.00	2.85	22	2.0

Table 11.8: Device and Weibull SEFI parameters for two SLC and MLC NAND flash devices. Notice the higher cross section of the MLC Flash.

Once again, the results demonstrate the lower tolerance to radiation of MLC memories compared to SLC ones, in this case for SEFI events. The effect of shielding is small but considerable, around half order of magnitude rate reduction when increased to 5.0 mm. These results also show that the event rate is manageable in all conditions, in particular for the ISS orbit and best case conditions. The worst results, at the High LEO orbit, in worst case conditions and 2.5mm shielding, one is expected to observe a functional interrupt per device once every month. Noticeable also is that this is recoverable by power cycle without data loss.

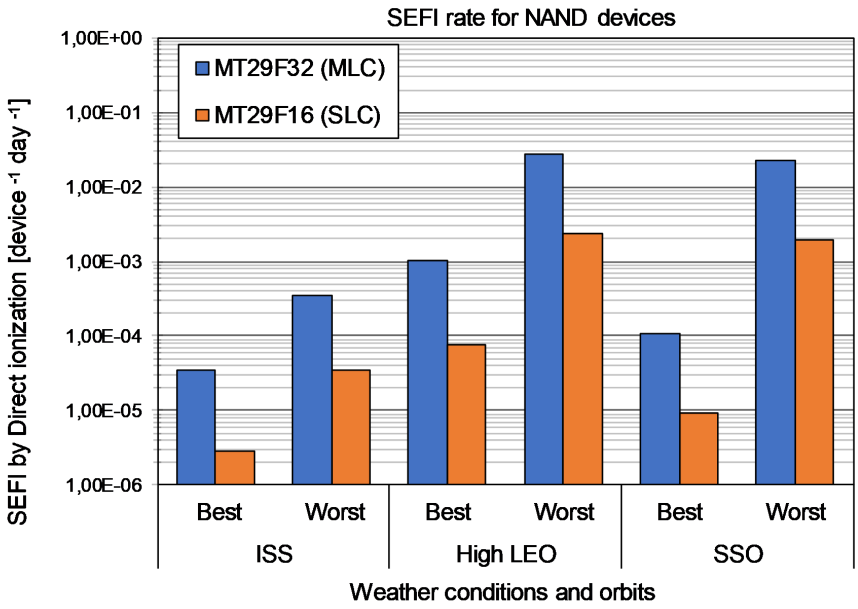


Figure 11.10: SEFI event rate comparison between SLC and MLC NAND flash. Assumes 2.5mm Al-equivalent shielding. Calculated using SPENVIS SEU rate tool.

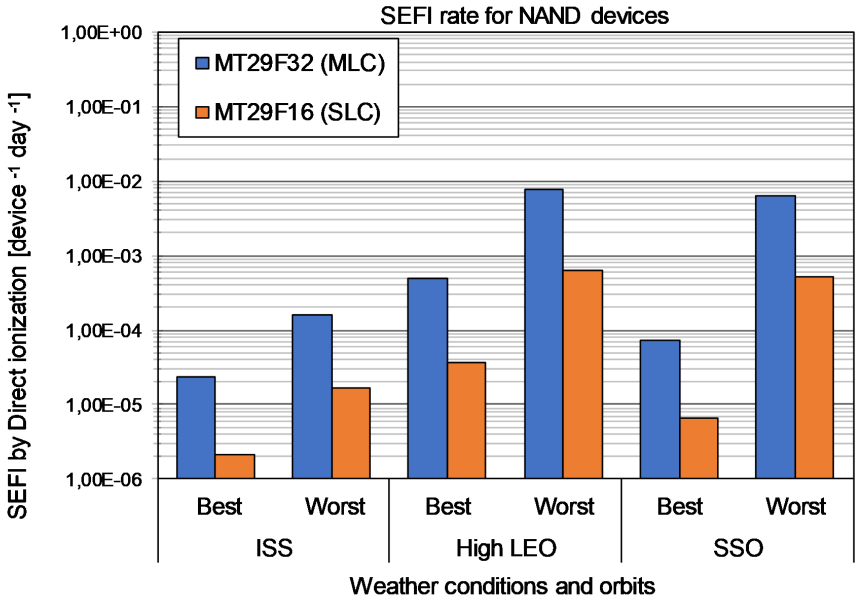


Figure 11.11: SEFI event rate comparison between SLC and MLC NAND flash. Assumes 5.0mm Al-equivalent shielding. Calculated using SPENVIS SEU rate tool.

It is important to notice that historically, authors have found Micron flash memories to be more prone to SEE than competitive memories such as Samsung [149] [150]. Some papers point to thresholds as high as $30MeVcm^2/mg$ for Samsung devices compared to $3MeVcm^2/mg$ for Micron. Therefore, these results may be improved by utilizing other memory suppliers as long as the radiation hardness of these devices is known.

Zynq-7020

Experimental results on the SEFI susceptibility of the Zynq-7000 SoC are inconclusive. Possibly since SEFI are only detectable few clock cycles after an upset event, pin-pointing the exact upset event is not simple [151]. Together into parity ECC on the L2 caches, it is understandable that SEFI characterization

of complex SoC like the Zynq-7000 is challenging and disparate results are acquired by different authors [123]. For instance, Amrbar et al [134] didn't find any SEFI with heavy ion cocktails whilst Du [152] [145] observed interrupts with 239Pu Alpha irradiation and protons. Additionally, Hiemstra [144] and Tambara [151] found SEFI event rate to be software dependent with operating systems leading to more events compared to application running bare to the metal.

Device	$\sigma_{sat}[cm^2/bit]$	$L_0[MeVcm^2/mg]$
Zynq [151]	1.00e-5	7.3

Table 11.9: Saturation cross section and threshold LET for SEFI on the Zynq-7020 SoC.

For calculation purposes, heavy ion experimental results from Tambara [151] were used. In table 11.9, saturated cross sections and threshold LET under 16O beam exposure are shown. Upset rates were calculated using the RPP method and are displayed in 11.12. It shows the low event rate, in particular at solar minimum conditions. The inconclusive reports and calculated SEFI rates suggest that SEFI are not frequent and are mitigable using the aforementioned functional monitoring methods.

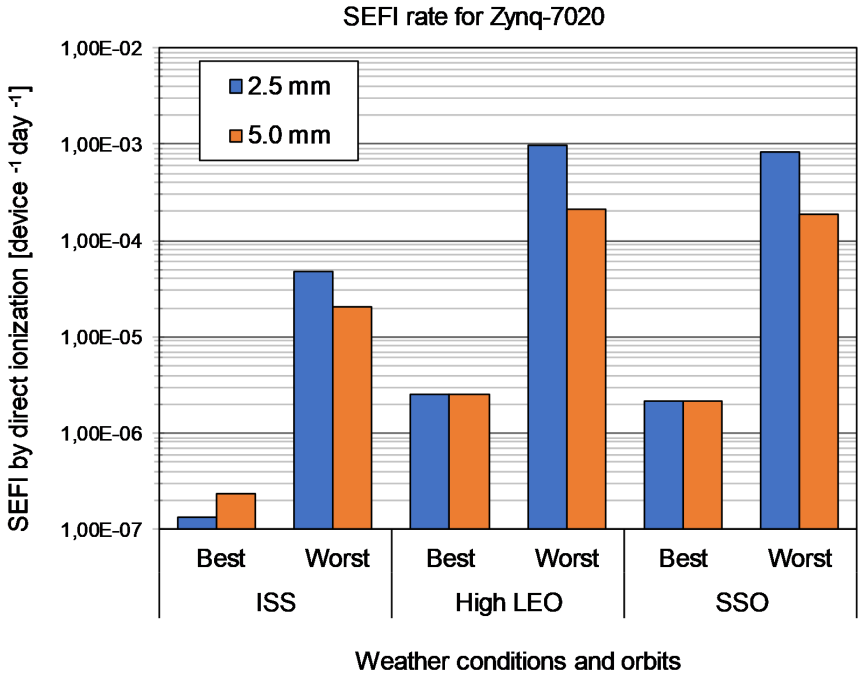


Figure 11.12: SEFI event rate for the Zynq-7000 SoC.

11.4. Validation

The calculated upset rates are validated using upset rate predictions from literature. These corroborate the methodology and some assumptions such as the sensitive volume thickness. The validation process is challenged by the large influence that radiation models, calculation methods and sensitive volume dimensions have in the final upset rate [153]. Literature suggests that differences in radiation models such as GRC can lead to one order of magnitude differences in upset rates even when both models consider solar maximum. Comparing to actual in-orbit upset rates, *'results suggest that the most common calculation methods overestimate upset rates by at least 2 times'* [140].

The literature on the radiation response of the aforementioned NAND flash devices provides upset rate predictions for similar orbits as this study in solar minimum conditions. The ISS orbits have a 100km altitude difference and a 0.04 mm shielding thickness difference. The SSO orbit can only be compared against a reference Proba orbit. The thickness of the sensitive volume is equal in both cases as well as the trapped proton model (AP8min). No information on GCR models utilized is given. Despite these modelling differences, agreeable results are shown in table 11.10. The relative difference

is below 1 for all cases which is a good agreement considering the large influence of GCR and proton models in the upset rate events.

Device	Orbit	Calculated SEU [bit^{-1} day^{-1}]	Reference SEU [bit^{-1} day^{-1}]	Absolute difference [bit^{-1} day^{-1}]	Relative Difference
MT29F32	**ISS**	2.88e-10	1.97e-10 [129]	9.15e-11	0.46
	SSO/Proba	8.26e-10	5.18e-10 [129]	3.07e-10	0.59
MT29F16	**ISS**	1.16e-12	5.16e-12 [128]	-3.99e-12	-0.77
	SSO/Proba	1.37e-11	2.70e-11 [128]	-1.33e-11	-0.49

Table 11.10: Validation of SEU rate in best case conditions calculations for NAND flash memories. The ISS orbit considered in the reference sources is at 500km altitude and 56.4º inclination. Proba orbit at 98.3º inclination and 715km to 735km altitude. Both reference orbits consider 100 mils Al-equivalent shielding (2.54 mm). AP-8 min model with Creme96.

Assumptions on the sensitive thickness of the Zynq internal memories are validated with a reference calculation for solar minimum at the ISS orbit. The relative difference between 1.95 and 3.09 is expected, as previously mentioned, considering the unknown models of the reference. This validation is important since the upset rate of the CRAM plays a significant role in determining the system's overall availability, as seen in the following chapter. Results from this exercise are presented in table 11.11.

Device	Conditions	Calculated SEU [bit^{-1} day^{-1}]	Reference SEU [bit^{-1} day^{-1}]	Absolute difference [bit^{-1} day^{-1}]	Relative Difference
CRAM	**B**	2,98E-08	7,29E-09 [123]	2,25E-08	3,09
BRAM	**B**	3,83E-08	1,30E-08 [123]	2,53E-08	1,95

Table 11.11: Validation of the SEU rates for Zynq's CRAM and BRAM at the ISS orbit. The reference source considers a ISS orbit of 400km altitude and 51,6º inclination. Reference considers 100 mils Al-equivalent shielding (2.54 mm). No information on the models used to model solar minimum conditions or calculate upset rates. No information on assumed sensitive thickness.

11.5. Discussion

It is important to notice that radiation analysis of other types of active components, in particular, opamps, SDRAM memories, signal converters and multiplexers, is required in order to select all the technologies required for this avionics unit. Due to time constraints, these comparisons were not performed. Nevertheless, the presented comparisons are those thought to represent the largest impact on availability.

Only direct ionization SEE due to heavy ions were considered in this study. This underestimates the overall SEE rate as it disregards protons direct ionization and other non-ionizing radiation. Modern ICs were shown to be susceptible to proton direct ionization [154] and low-energy protons [145] [155]. Cross-sections for proton ionization were found to be substantially lower than for heavy ions for the considered devices [143] [147] [128]. However, proton flux is high in LEO in particular when crossing the Van Allen belts. Literature suggest that the considered NAND flash memories have similar SEU rates for heavy ions and protons for LEO [156] [129]. Hence, a deeper understanding of the effects of protons and non-ionizing radiation is required in order to better determine the expected upset rates. Due to large variability of results and the impact of models and device dimensions, only order of magnitude values should be considered. Results are, therefore, only indicative of event rates.

As shown in table 11.5, most COTS devices considered have LET thresholds above the iron knee which is significant as they can be considered radiation tolerant. Hence, latchup events are uncommon but to be expected in longer duration missions and in periods of higher solar activity.

Transient events for COTS parts are usually one order of magnitude more frequent than their space grade counterparts. Nevertheless, for most orbits, this is thought to not be significant as these faults are mitigable.

High altitude and high inclination orbits lead to significantly more total dose and events than other orbits since they cross regions with higher flux of particles. Hence, these require a more careful radiation hardness assurance process prior to the mission. Shielding is effective at reducing the total

dose and event rate, at least up to 5.0mm. However, shielding introduces uncertainty due to secondary particles which may increase event rates for commercial parts [157].

A comprehensive study into the radiation hardness of SLC, MLC and TLC memories built on the same 25nm process was performed by Irom et al [111] and corroborates the reduced sensitivity of the SLC technology found in this study. Following the considerations on the effects of protons and indirect ionization, it is important to further study these memories in order to determine the appropriate ECC methods.

Functional interrupt events for NAND flash and the SoC were found to be highly dependent on orbital environments and are only expected with multiple months periodicity. With the inclusion of functional monitoring processes, these uncommon events are thought to be correctable.

Overall, the COTS components analysed in this chapter were found to be radiation tolerant. Constraints due to TID were found to not be significant as shielding up to 5.0mm limits dose levels to well below the tolerance of commercial parts. Thresholds for latchup were found to be above the iron knee which suggest that latchup events are uncommon in these orbits, although expected. The Zynq has a lower threshold for micro-latchups and is the most susceptible part. The findings suggest that destructive consequences of radiation, TID and SEL, are not common and are tolerable for 5 year missions in the reference orbits, if the suggested protection systems are employed. Thus, modern COTS components are suitable for this architecture, although continuation of the radiation hardness assurance process is required.

11.6. Conclusions

In this chapter, reference orbits were characterized in terms of their radiation environments. The outputs were TID ranges and shielded fluxes for boundary space weather conditions and 2.5mm and 5.0mm shielding. A number of parameters that characterize the radiation sensitivity of COTS and rad-hard devices were presented and compared. Most concretely, SEU, SET, SEL and SEFI rates were calculated for a variety of ICs. Validation of the results suggest that only order of magnitude values for these calculated event rates shall be considered due to uncertainty of radiation models and the fact that only direct ionizing from heavy ions was considered. The findings suggest that the considered COTS components are suitable for the reference orbits as they can be categorized as radiation tolerant, with low probability of permanent and destructive consequences from radiation exposure.

At the end of this chapter, the reader is expected to understand the radiation environment the system will be exposed to. It shall also understand the models and calculations methods utilized to estimate the effects of this radiation on target COTS technologies. The suitability of COTS components shall be understood. The following chapter utilizes some of these results to forecast the system availability and the impact of these faults mechanisms.

12

System Specifications

This chapter presents the specifications of the developed avionics architecture. It presents the most important characteristics required to validate and compare the design against competitors and help answer some of the research questions.

The versatility of the design makes it possible to have multiple configurations with low recurrent costs. These configurations are presented including expected availability figures as a consequence of radiation effects. Comparison of specifications with respect to avionics configurations is thus possible. Metrics including size, weight and power are estimated. Rough order of magnitude component costs are compiled for each unit and conclusions are drawn. The expected performance figures are estimated. These specifications are used to validate the design against other commercial avionics units.

Conclusions from this chapter are paramount in answering research questions RQ-3C and RQ-4. The former, related to the effect of component qualification in overall cost, is answered by the analysis of costs for each unit. The latter is answered by the results of the exercise to calculate system availability. With this chapter, the reader is expected to understand the metrics that differentiate the proposed avionics from other solutions and how they were estimated.

12.1. Configurations

The architecture of the system and utilization of COTS devices allows multiple configurations to be produced with low impact in recurrent engineering costs. Multiple configurations for the system are achieved by changing the number of OBC/PLIU units, interface specifications, storage and memory capabilities.

The separation of functions over three distinct units is purposefully made so that availability figures are maintained independently of the possible configurations. Each configuration is based on the supervisor board, which is a standalone unit capable of reconfiguration, clock distribution and monitoring of system status. Adding PLIU and OBC units expands on these basic functions. Adding redundant units contributes to increasing reliability levels. According to customer requirements, this baseline design adapts to required functionality and expected reliability levels. Additionally, SBC based on this design increase the applicability of this design.

As shown in 9.5, COTS transceivers sharing the same packaging and similar pinouts can be placed on the final hardware design with ease and thus adapt to the number and type of external interfaces required. With the use of redundant units, the number of and possible combinations for external interfaces is immensely increased. Since some of these transceivers built using the same technologies have already undergone radiation testing, radiation assurance processes are simplified.

Similarly packaged memory ICs are also common. As shown in 11.3.4, SLC and MLC NAND flash technologies present distinct radiation behaviours. These two factors can be explored to adapt the final system to reliability, availability and BER requirements of the mission. The same can be said for volatile memories.

The following table compiles a number of parameters that can be configured according to the mission following the suggested ICs presented in the previous chapters.

Units	Supervisor + OBC + PLIU or SBCs
Redundancy	Cold, warm or hot redundancy schemes
Platform Storage	SLC (1Gb to 64Gb) or MLC (16Gb to 128Gb) NAND flash
Payload Storage	SLC (8Gb to 512Gb) or MLC (Up to 1Tb) NAND flash
Interfaces	Combinations of RS-422, RS-485, CAN or LVDS

Table 12.1: Configuration parameters

12.2. Availability

The availability of a system is a metric to evaluate the deliverance of a correct service at a given time. This is dependent not only on the individual parts that constitute the system but also its architecture, software and handling of faults [158].

To calculate the availability one also requires knowledge of the fault rate [1], as mean-time-to-fault (MTTF) or mean-time-between-faults (MTBF). The latter relates to repairable systems where MTBF is calculated as the sum of MTTF and the time required to detect, isolate and recover said fault, measured as a mean-time-to-repair (MTTR) [159]. In this system, as the MTTF is much larger than MTTR, it is assumed that MTTF and MTBF are identical. The time is calculated as the inverse of the device's yearly upset rate.

The availability of each individual part of the system can then be calculated as:

$$Availability = \frac{MTBF}{MTBF + MTTR} \tag{12.1}$$

A common way to compare the availability of multiple systems is using the nines-notation. For example, a system with 5-nines would have 99.999% availability or 5 minutes downtime per year. As per requirements SR-R04, this system shall have an availability better than 3 nines, or less than 8 hours and 46 minutes downtime per year.

12.2.1. Methodology

The methodology to estimate the availability consists in first identifying the parts with the highest impact, then generating a reliability block diagram of the system and finally perform the availability calculation for each layer of the block diagram.

The identification of parts is done by accessing their rate of SEL, SEFI, or the frequent need to implement time and resource consuming EDAC and scrubbing codes. In the case of SEL, table 11.5 shows that the susceptibility of the Zynq-7020 SoC is much higher than the other parts. Section 11.3.5 presents the SEFI rate for both the Zynq and NAND flash. Lastly, the rate of SEU for the Zynq CRAM was calculated in 11.3.4 which is expected to require frequent scrubbing as described in 10.1.5.

This estimation is limited as it only considers faults attributable to direct ionization of some of the system constituents. Other faults related to software or hardware are not considered. Therefore, the estimation is able to inform the reader on the expected loss of availability due to radiation and not the overall system availability. Furthermore, the uncertainty of the radiation analysis is also a factor in the accuracy of this estimation.

As the system is divided into units, this division is also noticeable in the representation via block diagrams. It is defined that a fault in each of the mentioned units or parts leads to an unavailable system and therefore each will be connected in series, representing an "and" operation [159]. The analysis considers the OBC and PLIU units, despising the impact of the supervisor block as it is believed that this has a very high availability due to the qualification level of its parts. The block diagram is shown in figure 12.1.

Configurations with warm redundancy and no redundancy in the OBC and PLIU are considered. Although redundant operation is represented by blocks in parallel, "or" operation, a fault event still requires a re-configuration or activation process of the redundant unit, which implies a non-negligible MTTR. This is more similar to a block diagram of a repairable system but with a reduced MTTR compared to a non-redundant implementation.

The calculation of the availability of the system is the following:

[1] In this context, only faults related to radiation effects are considered.

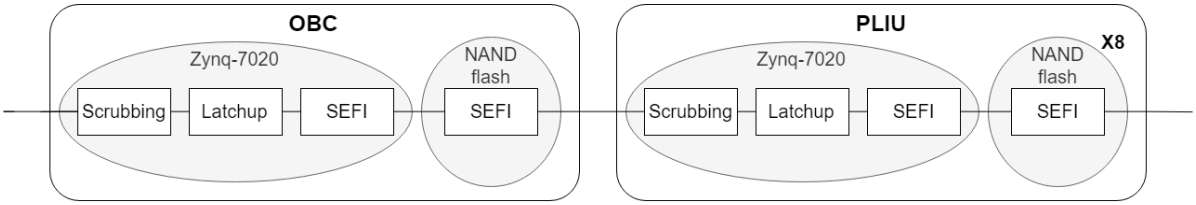


Figure 12.1: Reliability block diagram representative related to the system's availability.

$$Availability_{system} = Availability_{OBC} \times Availability_{PLIU} \tag{12.2}$$

With the availability of each unit as follows:

$$Availability_{PLIU} = Availability_{Zynq-7020} \times (Availability_{NAND})^{8\,[2]} \tag{12.3}$$

$$Availability_{OBC} = Availability_{Zynq-7020} \times Availability_{NAND} \tag{12.4}$$

The combination of the Zynq-7020 faults leads to this calculation:

$$Availability_{Zynq-7020} = Availability_{Scrubbing} \times Availability_{Zynq_{SEL}} \times Availability_{Zynq_{SEFI}} \tag{12.5}$$

12.2.2. Sources of reduced availability

The main sources of radiation related downtime are SEL, SEFI and scrubbing. These, and their respective MTTR are shown in table 12.2. In it, fault event rates and repair times for cold and warm-redundant operations are shown. The MTTR for a repairable, non-redundant system is considered the same as for a cold-redundant one.

Device	Fault event	MTTR
Zynq-7020	SEL	5 min / 1 min
	SEFI	5 min / 1 min
	Scrubbing [135]	27 ms
NAND	SEFI	10 s

Table 12.2: Non-redundant and warm-redundant MTTR for zynq SEFI and SEL.

Scrubbing

One of the expected protection mechanisms against SEE is the utilization of scrubbing processes in the event of SBU or MBU. Following the calculated SBU event rates presented in 11.3.4, it is possible to estimate the total time spent scrubbing the PL configuration bitstream (27.7 Mb [147]) for each orbital condition. This time is considered lost and a consequence of the chosen technology. The upset rate in CRAM is significant and therefore must be considered for availability calculations. The mean time to correct the errors is calculated based on the percentage of faults (89% SBU, 10% MBU and 1% full reconfiguration) and their respective total correction times (8ms, 15ms and 1.8s)[135]. This leads to an average of around 27 milliseconds duration for each upset event.

SEL

It was calculated that in worst case conditions, a micro-latchup of the Zynq's VccAux is expected around three times a year. This implies the power cycle of the SoC and subsequent reboot. The reboot process is assumed to take 5 minutes. This value considers 20 seconds for the detection, 10 seconds to load the FSBL, 2 minutes to download the SSBL over CAN at 1Mbps (65Mbit with 70% overhead bits) and finally 2min30s to boot and initialize the final software). Another option considered is a warm-redundant operation. In this case, a SEL would lead to the switch-over to the redundant unit. It is assumed that this process would take a maximum of 1 minute assuming the redundant unit is already booted with the most recent software image.

[2]There is an array of 8 NAND flash devices in the PLIU board.

SEFI

SEFI on Zynq-7020: Previously calculated functional interrupts on the SoC were shown to be non-negligible. Halting of normal program flow and other unpredictable effects are to be expected. In these cases, where functional interruption is detected by the supervisor or other internal mechanism causing a reset/power-cycle, a MTTR equal to the SEL case is assumed.

SEFI on NAND memories: Commercial NAND devices were shown in 11.3.5 to be susceptible to functional interrupts. These events also require reset or power cycle to recover. The impact of this is mostly related to the inability to store memory in the expected location and need to store it elsewhere. The calculations assume 10 seconds as the time required from error detection through power cycle to restoration of functionality.

12.2.3. System predicted availability

Taking into consideration all the previously presented data and methodology, the estimated system availability due to ionizing radiation for a non-redundant system employing SLC NAND flash is shown in table 12.3. It displays results with a precision of three decimal places following the 5 nines standard.

Overall availability is equal or better than 5 nines in 6 out of 12 study cases. Highest availabilities are concentrated at the ISS orbit and in best conditions, 5.0mm shielding cases. Worst-week solar flare cases represent the most impact on the results in particular at the 1200km orbit with 2.5mm shields. This has the lowest availability at 99.956% or less than 4 hours downtime per year. This is better than the targeted availability which was set at less than 8 hours 46 minutes downtime, or 99.9% availability.

Orbit		**ISS**		**High LEO**		**SSO**	
Weather conditions		**Best**	**Worst**	**Best**	**Worst**	**Best**	**Worst**
OBC							
Shielding [mm]	**2,5**	100,000%	100,000%	99,999%	99,978%	100,000%	99,982%
	5,0	100,000%	100,000%	100,000%	99,994%	100,000%	99,995%
PLIU							
Shielding [mm]	**2,5**	100,000%	100,000%	99,999%	99,978%	100,000%	99,982%
	5,0	100,000%	100,000%	100,000%	99,992%	100,000%	99,993%
System							
Shielding [mm]	**2,5**	100,000%	100,000%	99,998%	99,956%	100,000%	99,963%
	5	100,000%	100,000%	99,999%	99,988%	100,000%	99,990%

Table 12.3: Calculated availability for a non-redundant configuration using SLC NAND.

One can also notice the similar contribution of both OBC and PLIU to the availability. Since they are composed by similar components, it is expected that this is the case. However, it is important to consider that the data engine of the PLIU was not considered in this calculations. Nevertheless, if the rad-hard HPDP or RC64 devices are used, as described in chapter 9, it is not expected that this conclusions are significantly changed. Additionally, as it will become clearer in the following paragraphs, the downtime is mostly caused by one single type of fault.

Impact of fault modes

Calculated availability due to each fault mode provides important clues into understanding the behaviour of the entire system and how radiation induced downtime can be reduced. The results suggest that the contribution of some of these fault modes to the total availability is very small or negligible compared to others. It is also seen that in best case conditions and in the ISS orbits, the availability is equal or better to five nines for all fault modes.

Table 12.4 shows the minimum availability related to each fault. This is the calculated availability in the High LEO orbit, in worst case space weather conditions and with 2.5mm shielding. Values are presented as a percentage with 3 decimal points for easier comparison with the 5 nines suggested availability for space systems [160] and avionics units [161]. It is possible to conclude that the scrubbing process is the most influential event, followed by the SEL in the SoC. The other faults lead to a better than five nines availability even in worst case conditions.

Fault	Minimum Availability
Zynq SEL	99.998%
Zynq SEFI	100,000%
Scrubbing	99.980%
SLC NAND SEFI	100.000%
MLC NAND SEFI	100.000%

Table 12.4: Minimum availability due to each fault mode in non redundant configuration.

The impact of scrubbing is explained not only by its frequency, with approximately 23000 events per year, but also to its MTTR. Knowing that 1% of all faults in CRAM require a 1.8 second reconfiguration, a downtime of almost 70 minutes per year is expected for full reconfiguration of the Zynq's PL, compared to the 104 minutes downtime attributed to the sum of all scrubbing events. Such results suggest that the correction of SBU and MBU in the programmable logic of COTS SoC have the largest impact on the overall system availability. In particular, although there is a low probability of a SBU requiring a full reconfiguration of the logic, this has a very significant contribution to downtime in harsh radiation environments.

Effect of warm-redundancy

Reviewing the effects of a warm redundant configuration concludes that these effects are most noticeable with reduced shielding and worst case weather conditions. These differences in availability between redundant and non-redundant systems are shown in figure 12.2.

A warm redundant configurations was previously described as enabling lower MTTR since it is not necessary to perform loading and booting of software images. Therefore, MTTR is assumed to reduce from 5 minutes to just 1 minute. Increasing in shielding is beneficial to the availability except in the ISS orbit in best case conditions due to the increase in secondary particle flux behind shielding. The effect is more noticeable in higher orbits and worst weather conditions. However, not a significant increase is expected, with only the High LEO and SSO orbits with 2.5mm shielding having a increase on the 5th nine.

Comparing the results in the same orbit, it is clear that the effects of redundant operation in availability are more significant in the worst case conditions. This is explained due to the fact that event rates in these conditions are higher and thus leads to higher number of cases where it is required to switch to the warm unit.

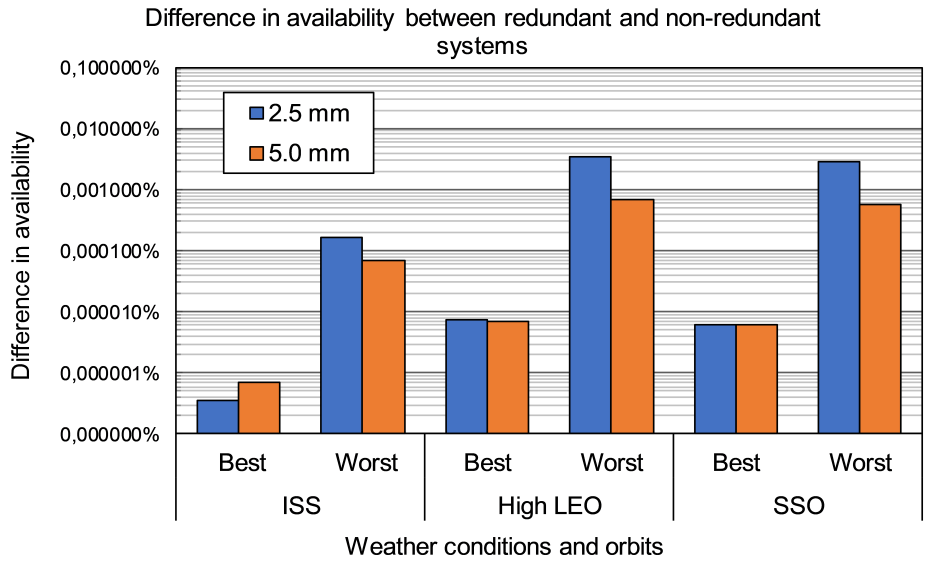


Figure 12.2: Effect of warm redundant configuration in the systems availability compared to non-redundant configuration. Considers the use of SLC NAND flash.

From the twelve test scenarios, only two have shown an improvement in availability equal or higher

than the third decimal place. Considering the 5 nines standard and the calculated overall availability (table 12.3) one can conclude that a warm redundant configurations does not significant benefit the overall availability. This conclusion is dependent on the actual MTTR in both warm and cold configurations since only assumptions for these times were made at this point. It is also interesting to notice that, as seen in table 12.4, scrubbing is the most noticeable cause of downtime, and since active unit swapping is not required in these cases, the benefits of a warm configuration are limited. Nevertheless, it is important to draw attention to the fact that redundant units still contribute to dependability increase in the form of reliability, if the nominal unit fails.

12.3. SWaP-C

Size, weight and power are still some of the most notorious limitations of spaceflight [162]. This section addresses these aspects as well as another fundamental one related to this project, the components cost. It is shown that the SWaP-C of the proposed system is competitive with other products.

12.3.1. Size

Large ICs and connectors are the biggest contributor to size of the PCB for each unit. The utilization of nano connectors and COTS devices, as shown in chapter 9, contributes to a reduction in the minimum required area. The proposed physical architecture was found to be implementable in VME 3U size A PCBs, measuring 16cm by 10cm by summing the sizes of the ICs shown in the diagrams of figures 9.6, 9.7 and 9.8.

Function	COTS device	Footprint [mm^2]	Rad-hard device	Footprint [mm^2]	Footprint increase
Processing	Zynq-7020	361	Cobham GR712RC	1024	184%
LVDS transceiver	TI SN65LVDS051	45	ST RHFLVDSR2D2	84	87%
CAN transceiver	TI SN65HVD251	20	Intersil ISL72028SEH	45	124%
NAND flash	Micron MT29F8	216	3D Plus 3DFN8	252	17%

Table 12.5: Footprint comparison between COTS and space-qualified components.

Comparisons of footprint between COTS and rad-hard components with identical functionality, as seen in table 12.5, reveal the larger footprint of rad-hard devices. This difference is most noticeable in processing units which, at a commercial level, are being developed at shrinking feature sizes, not accompanied by rad-hard devices. Commercial transceivers are also shown to have half the footprint of functionally identical rad-hard ones. The benefits of commercial devices in terms of footprint are less significant for NAND flash memories. The use of 3D memory technologies for rad-hard applications leads to similar footprints when the same memory densities are considered.

12.3.2. Weight

The proposed sizes of the architecture allows for a mass prediction based on the presupposition that an aluminum casing is the single contributor to the mass. This excludes the mass of PCBs and the PSDU which is out of scope.

The methodology consists in assuming a volume for the assembly based on the PCB sizes, a 5.0 mm thickness aluminum casing ($2.7 g/cm^3$ mass density) and 5.0mm spacing between casing and PCB. A ratio of casing volume to empty volume of 0.3, calculated ratio for the Amethyst avionics suite with same thickness casing, enables the prediction of mass [161]. An external volume of 18cm x 12cm x 12cm follows.

A total mass of approximately 2 kg is calculated from the aforementioned methodology. This results is below the requirement laid out in SR-O02. Comparing this to similar suites, such as the Amethyst centralized avionics with a mass of 3.5kg [161] the proposed avionics is expected to have a competitive mass. The 1.5kg difference between the two is thought to be related to internal stiffeners and the mass of a PSDU.

12.3.3. Power

It is expected that internal power consumption is mostly attributed to processing units. In this architecture it consists of two Zynq-7020, one data-engine and one FPGA. For this estimation, the

HPDP data engine and a Xilinx Virtex-4QV (part XQR4VSX55-10CN1140V) were considered.

In order to obtain estimates for the power consumption, different methods were used. For the Zynq-7020 (part XC7Z020-CLG484), Xilinx power estimation tool was used, estimating around 4W power consumption with two PS cores at 766MHz and the expected I/Os. The accuracy of this estimate is largely dependent on resource utilization and is therefore only indicative. The HPDP power consumption was considered as 1.82W when powered at 3V3 [11]. The FPGA power consumption was considered as the typical power-on consumption calculated from the device's datasheet at 1.619W.

The estimation for the entire system is around 11.5W and 21.3W for non-redundant and warm-redundant configurations. This is a optimistic estimate as it only considers the power consumption for the processing units and disregards efficiency of the power conversion and distribution process (thought to be around 70%). Nevertheless, it suggests the power requirements of the final system. It also suggests that the Zynq-7020 has a large impact on power consumption, in particular when all its resources are being fully utilized.

12.3.4. Cost

In order to validate that this architecture is in fact 'cost-effective', rough order of magnitude estimates (ROM) of most costly integrated circuits for each unit and the system was performed. The devices shown are mentioned previously in this document or are found to be representative for the application. Websites of suppliers of electronic components such as Digikey, Mouser and Arrow were consulted along with quotations from suppliers of qualified components. The qualification level of each IC is mentioned in the caption of each table.

The conclusion from this exercise is that the biggest contributor to IC cost is the Supervisor unit, as expected. Since it is built with qualified devices, its components are much more expensive than the OBC unit which is made up of COTS components except for the NOR flash storing the FSBL. In fact, this NOR flash represents almost 90% of the OBC's component cost. The PLIU unit cost is largely a consequence of the data engine. Either the qualified HPDP data engine or high-end commercial FPGAs are expected to cost close multiple thousands of euros per unit.

It is interesting to trade-off the large difference in price between COTS and qualified components and their radiation tolerance. In particular, section 11.3.3 showed the similarities in cross sections and threshold LET between differential transceivers. However, table 12.6 and 12.7 show that qualified versions are up to 100 times more expensive. This suggests that a cost/benefit exercise mapping functions and components, could lead to considerable cost savings with acceptable risks.

OBC

Despite the larger number of ICs, the OBC has an expected component cost under 10000€. It is interesting to note that the Zynq-7020 SoC (part number XC7Z020-CLG484 widely referenced in experimental radiation exposure reports) costs 137€. All other commercial components are found for less than 100€ a unit. As mentioned, the space-grade NOR flash storing the FSBL represents approximately 90% of the unit's component cost. Table 12.6 summarizes the ROM costs for the OBC.

Function	Name	Number	ROM Unit Cost[€]	ROM Cost [€]
SoC	Xilinx Zynq-7020 ∆	1	137	137
SLC NAND 64Gb	Micron MT29F32 ∆	1	70	70
DDR3 SDRAM 4Gb	Micron MT41J512M8RA ∆	1	28	28
NOR	128Mb †	1	6000	6000
Transceivers half duplex	TI ISO15 ∆	3	5	15
Transceivers full duplex	TI ISO35 ∆	3	7	21
Transceivers CAN	TI ISO1042 ∆	3	5	15
8-ch MUX	MAX308ESE+ ∆	4	7	28
Dual OpAmp	Analog Devices AD8572 ∆	5	5	25
Transceivers SpaceWire	TI ISO35 ∆	4	7	28
Total component cost [€]				6367

Table 12.6: ROM cost for main components of OBC unit. Non-exhaustive list. ∆: COTS. †: QML V.

PLIU

Increasing the estimated cost of the PLIU is the data engine. Besides this, expected component cost is close to the OBC. Therefore, one can concluded that the choice of DSP or FPGA for the data engine is a large contribution to the cost of this unit. Expected unit component cost is less than 30000€ as shown in table 12.7.

Function	Name	Number	ROM Unit Cost[€]	ROM Cost [€]
SoC	Xilinx Zynq-7020 ∆	1	137	137
MLC NAND 128Gb	Micron MT29F128 ∆	8	17	136
Data Engine	HPDP †	1	20000	20000
Transceivers CAN	TI ISO1042 ∆	3	5	15
Transceivers full duplex	TI ISO35 ∆	3	7	21
DDR3 SDRAM 4Gb	Micron MT41J512M8RA ∆	2	28	56
NOR	128Mb †	1	6000	6000
Total component cost [€]				26365

Table 12.7: ROM cost for main components of PLIU unit. Notice the cost of the data-engine. Non-exhaustive list. ∆: COTS. †: QML V

Supervisor

In the case of the Supervisor, the choice of FPGA is incredibility important as its radiation hardness level is assumed to lead to no SEFI or SEL in the availability calculations. Prices for rad-hard and rad-tolerant FPGAs were found to vary widely depending on the existence of integrated processing cores and number of logic cells. A Xilinx Virtex-4QV (part XQR4VSX55-10CN1140V), with a ROM estimate of 20000€, is found to be a good starting point for the design since it offers SEL threshold above $100 MeVcm^2/mg$ and full QML-V space grade qualification. For comparison, a QML-V Virtex-5QV (part XQR5VFX130) can cost around 50000€. ROM cost list for Supervisor components is seen in table 12.8.

Function	Name	Number	ROM Unit Cost[€]	ROM Cost [€]
FPGA	Xilinx Virtex-4QV †	1	20000	20000
RS-422 Driver	HS9-26CLV31RH-8 †	2	544	1088
RS-422 Receiver	HS9-26CLV32RH-8 †	2	544	1088
SDRAM	DDR2 1Gb †	1	10000	10000
NOR	128Mb †	1	6000	6000
Mux 16-ch	HS9-1840ARH-8 †	1	1000	1000
ADC 1-ch	RHF1201KS01 †	1	3500	3500
Oscillator	XO †	1	12000	12000
Total component cost [€]				54676

Table 12.8: ROM cost for main components of Supervisor unit. Xilinx Virtex-4QV part number XQR4VSX55-10CN1140V. Non-exhaustive list. ∆: COTS. †: QML V

System

Concluded the calculation of ROM costs for each unit it is possible to estimate the component for the entire system. Table 12.9 reveals this calculation for redundant and non-redundant options.

One observes that the Supervisor unit is the single largest contributor to system cost. It has a ROM cost almost ten times higher than the OBC. The difference is less noticeable for the PLIU due to the data engine. The impact of COTS components in the OBC and PLIU is notorious. Assuming an OBC and PLIU based on space-grade components with the same functionality, one could expect multiple fold increase in overall system cost.

Redundant and non-redundant configurations have a cost difference related to the added OBC and PLIU boards. Since these are COTS-based the impact of internal redundancy on component cost is less significant than on other architectures, around 30% overhead. Reliability is hence improved, ensuring system operation after the failure of the OBC and PLIU boards, with low cost overhead. ROM system cost for non-redundant configuration is 87408€ and 120140€ for redundant configuration.

	ROM Cost [€]
OBC	6367
PLIU	26365
Supervisor	54676
Non-redundant system	87408
Redundant system	120140

Table 12.9: Overall ROM component cost of proposed avionics.

12.4. Performance

The performance of the proposed system is leveraged by the use of modern COTS devices. Rad-hard technologies are known to lag behind commercial technology by several generations[163] [39], hence limiting their performance and applications.

Heterogeneity in performance is most noticeable in the raw number of operations performed by COTS SoC and MCUs compared to rad-hard architectures [3]. For example, the Zynq-7020 at 866MHz is capable of 2500 DMIPS compared to only 150 at 100MHz by the LEON-3 GR712RC, still in use for small-sat applications [164]. This translates into 2.5DMIPS/MHz compared to 1.5DMIPS/MHz. Additionally, the combinations of processing cores with logic fabrics enable a all new range of applications, an hybrid approach long anticipated by the space industry [78]. Rudolph et al present the ratio between the Zynq-7020 and common rad-hard processors for a variety of normalized performance figures [165].

Benefits derived from the Zynq hybrid approach are being utilized by SSTL's new CoreDHS avionics. This system combines the LEON3 processor with the Zynq for mission specific high-end processing [44]. However, this applications is still relying on a LEON3-FT architecture for OBC and AOCS functions. The proposed architecture makes use of the Zynq-7020 for a larger number of functions, further improving performance whilst striving to maximize reliability and availability.

12.5. Conclusions

This chapter focused on calculating and presenting the main specifications of the design. It calculated expected availability levels, SWaP-C and performance. The results suggest that the system is competitive with comparable systems in all aspects.

Availability attributable to ionizing radiation effects was found to be better than 3 nines, or 99.9% occurring at High LEO orbits in solar maximum conditions and minimal shielding. For solar minimum conditions availabilities of 99.999% or better are estimated. The SWaP analysis suggests that these metrics are similar to other comparable products in the market. Cost reductions due to the use of COTS components were found to be particularly significant for the OBC board. Comparing the OCB, COTS-based, with the supervisor board, with only QML-V components, the ROM components cost ratio is approximately one tenth. The cost of the PLIU unit is largely influenced by the selected data engine. A non-redundant system is expected to have a ROM component cost lower than 100000€, with redundancy incurring in an 30% cost overhead. Achievable performance, measured in terms of DMIPS, is ahead of systems employing the GR712 MCU by a factor of 1.6 DMIPS/MHz. Performance for payload data processing is dependent on selected data engine.

At this stage of the report, the reader is expected to fully understand the proposed architecture at both functional and physical levels. It shall also understand estimated system specifications based on target technologies with special focus on radiation-induced system downtime, ROM component cost and performance. The following chapter verifies the design against the defined system requirements and validates the design for the reference missions.

[3] A number of COTS and rad-hard processors characterization parameters are shown in annex A.5

13

Verification and Validation

The sheer complexity of such a versatile avionics suite makes it impossible to define, design and verify a system on a single thesis project. Hence, the verification and validation process is performed at the current high level design stage that this thesis project has achieved. It provides confidence that the proposed system can be further developed into a higher technology readiness level (TRL) level with the expectation that these baseline requirements are verified. Validation of the radiation analysis results was already performed in chapter 11. Verification against requirements is mostly based on review of the design, since there is no hardware prototype to test. Similarities with other missions, products or literature are also employed. The radiation hardness calculations provide the confidence to verify some non-functional requirements.

Validation of the design, in relation to the intended use, is achieved by comparing the design with systems employed in reference missions and other avionics suites. The functional and physical design, in addition to the previously calculated system specifications, support this exercise.

This chapter summarizes the final thesis activities. Its contents reassures the reader that the designed system is according to specifications and that it fulfills its intended application. In this case, it confirms that the research goal is achieved with supporting evidence. The reader shall then be convinced of the fulfilment of the research goal and main thesis research activities.

13.1. Verification of requirements

The first section is related to the verification of system requirements, compiled in annex C.3. It is divided into functional and non-functional subsections.

13.1.1. Functional requirements verification

The verification of functional requirements is mostly based on similarity and review of the design. Devices used in similar use-cases and cited sources are the main sources for similarity. Interfaces number and type are reviewed to ensure compliance to requirements.

It was found that all required functions are implemented with the exception of the ones related to power distribution as since they are out of scope for this project. In particular, analog magnetorquer interfaces and motor control for solar panels are not yet implemented. The decision to not implement this functions is twofold. First, these are largely dependent on the architecture of the PSDU. Second, as they implement baseline functionality for attitude control and power generation, they shall be implemented with high reliability figures, precluding the use of COTS components.

It is also important to note the impact of non-redundant configurations on the verification of requirements. The flexibility for the end-user to implement non-redundant configurations has a negative impact on the verification of requirements that require no loss of functionality following a single failure (requirements SR-A09). In these cases, a failure in a component or entire unit leads to a high level of functional failure, an inherent risk of non-redundant configurations.

The methodology to follow the SAVOIR reference functional architecture during the functional design process ensures the functional completeness of the design. The physical architecture, presented in chapter 9, describes the implementation of this functional architecture into a physical one.

13.1.2. Non-functional requirements verification

Analysis of the radiation response of a set of components is the main method for verification of non-functional, dependability related requirements. Additionally, literature enables the verification by similarity of reliability and performance related requirements. Revision of the design, suggests the verification of SWaP-C related requirements.

A 5 year radiation analysis was performed and verified that compliance with the required availability and tolerance to SEE and TID effects. Better than 3 nines availability is achieved even in worst case conditions assuming the limitations and uncertainties presented in chapter 12. The tolerance and mitigation of radiation effects is achieved as presented in chapters 11 and 10. Only analysis for nominal missions of 5 years were performed. SWaP requirements were verified by similarity with other systems (see the previous chapter), since it is not possible at this stage to calculate such values with precision. The high level design performed until this stage nevertheless suggests that these can be met. Mechanical design was not performed so a number of related requirements were not verified.

A list of unverified requirements is shown in table 13.1.

Requirement ID	Category
SR-A11	Functional - AOCS
SR-A12	Functional - AOCS
SR-A17	Functional - Sun Sensor
SR-A18	Functional - Sun Sensor
SR-A28	Functional - Star Tracker
SR-A39 to SR-A48	Functional - Magnetorquers
SR-SP08	Functional - Supervisor
SR-SP13	Functional - Supervisor
SR-R02	Non-Functional - RAMS
SR-R03	Non-Functional - RAMS
SR-E02	Non-Functional - Environment
SR-O06	Non-Functional - Others
SR-O13	Non-Functional - Others
SR-O14	Non-Functional - Others

Table 13.1: Unverified system requirements. Relates to annex C.3.

13.2. Validation of the design

Validation of the design is difficult as similarly highly integrated systems combining COTS and rad-hard components are non-existing, to the authors knowledge. Additionally, a prototype unit is not yet built. Comparing the proposed avionics with other systems and S/C platforms reveals that the proposed system fulfills the demands of current and future small satellite missions by incorporating multiple avionics systems into a single package, due to the combination of COTS and rad-hard components.

The first metric to evaluate the validity of the avionics is to compare the interfaces made available by the system and the expected requirements of a small satellite mission. As described in chapter 9, the number and type of interfaces is adequate to the reference missions presented in 4. Interfaces are made for serial communication with AOCS and other peripherals in addition to a number of analog inputs. Radio transmitter and receiver units are also supported via serial interfaces. Payloads can be controlled by a CAN bus and high-data rates established via LVDS inputs. The unit is powered by the main spacecraft power supply unit via an unregulated 28V supply. Supported by processing power, IO management, memory and storage, the system effectively centralizes multiple S/C avionic units fulfilling that market need.

The goal to achieve a cost-effective unit without compromising on availability is validated by the radiation and availability analysis in addition to the use of mostly COTS components. Similar approaches, such as the CHREC Space Processor [165] which mixes rad-hard and COTS components is constrained to a single board and targeted at CubeSats. Despite the similarity, the proposed avionics expands this idea to larger platform and larger variety of functions.

13.3. Conclusions

The chapter presented an overview of the verification of requirements and validation of the design. It was found that the proposed system fulfills the defined requirements except for cases related to power supply and distribution. Validation of the design is achieved by comparing the offered functions and interfaces with the requirements of reference missions.

It is important to note that the validation of the radiation analysis methods and results was already achieved in chapter 11. Furthermore, verification and validation of the design is challenging at this stage of development, hence only review of design and similarity was possible.

The following chapters summarize and conclude on the findings of this thesis project.

14

Conclusions

This chapter presents a summary of the performed work and its key findings. The first part presents the tasks developed during this project, including methodologies employed. The second part presents the key outcomes of the thesis with particular focus on the fulfillment of the research objective and answer to the research questions.

14.1. Key outcomes

Throughout this project, conclusions over the investigated topics were made at the end of each chapter. This section presents the key outcomes pulled from these conclusions divided by categories. The first category is related to market trends and their influence in the development on new avionics system. The second category relates to the functionalities of these avionics. Another category is related to utilization of COTS products in the architecture and its impact on system's metrics. Finally, the main aspects related to radiation hardness assurance are presented.

Approximately 3700 small satellites are expected to be launched between 2016 and 2025. A large percentage of those are in the 50kg to 200kg mass range, with 71% affected to the deployment of Earth observation constellations based on optical systems. A study of the main market players revealed the interest in the development of standardized optical systems, developing LVDS interfaces for data transfer and CAN or other serial interfaces for control. Satellite manufacturers are also interested in developing S/C platforms that share similar designs and systems thus reducing recurrent engineering costs. Metrics such as available power, weight, mission scenarios and downlink data rates were obtained. It was concluded that the similarities between these EO constellations and S/C make it possible to develop an avionics solutions that integrates a large variety of functions to meet these interests.

Selection and division of functions is important in tackling the challenge of reducing recurrent engineering costs for small satellites. It was found that an architecture providing AOCS, C&DH, Payload interface with mass storage, TM/TC at data link layer and reconfiguration could simplify the avionics assembly of small satellites. Additionally, all functions besides TM/TC and reconfiguration can be implemented in cost-effective COTS components with a supervising unit performing these two functions ensuring that dependability, communication with ground and minimal functionality are maintained.

A number of technologies were selected and analyzed for metrics such as functionality, design features, cost, size and performance. It was concluded that COTS transceivers with galvanic isolation and fail-safe operation can be procured at low cost. Commercial transceiver sharing same package and identical pinout are key into developing a PCB design that can be configured for multiple interface protocols with simple 0Ω resistors. Commercial NAND flash with large capacity is a cost-effective data storage option if adequate ECC is employed. The Zynq-7020 SoC with its PL side allows for a large number and variety of interfaces. These characteristics, in addition to the use of NanoD connectors makes it possible to implement a large number of functions and interfaces on a 3U SBC.

The physical architecture was found to require fault masking and reconfiguration techniques to ensure dependability. Fault masking is achieved by means of a latchup current limiter on susceptible lines which are yet to be determined. COTS products with galvanic isolation were found to be procurable with little to no impact on cost or design. The isolation is paramount to avoid failure propagation

between redundant and nominal units. Fail-safe operation of transceivers is also available for COTS devices. In these cases, high impedance states are set when powered-off, disconnected from bus, or cable opens or shorts exist. Customized ECC codes are implementable on the PL side of the SoC. Scrubbing of the internal configuration memories of the SoC is required due to their susceptibility to radiation. The reconfiguration of the system is supported by a custom boot process, with initial boot from NOR flash and a second stage coordinated by the supervisor unit. Functional monitoring via continuous communication between system boards and current monitoring indicates the need for reconfiguration procedures. In the unlikely event of functional interrupt on the Supervisor, a watchdog timer resets this unit. This can be achieved with discrete electronic for high reliability.

Three reference LEO orbits, at low and high inclinations and altitudes, were modelled for radiation environment to understand their impact of target commercial technologies. Total dose effects and single event effects due to heavy ions were considered, both for best and worst case space weather conditions. The analysis showed that a shielding thickness of 5.0 mm Al-equivalent limits accumulated doses to less than 17krad(Si), safe for a selection of COTS devices with no induced effects. Latchup rates for the Zynq-7000 SoC, the most sensitive of the devices considered are, in the worst-case scenario, one event per 195 days. In other conditions the event rate is orders of magnitude lower. In addition, these events are small current steps which are not destructive. Transient events for a COTS and qualified differential transceivers were found to be one order of magnitude more frequent for the commercial device across all study environments. Upsets rates for Flash NAND devices were calculated. The results show the susceptibility of SLC technology is lower than for MLC, although shrinking feature sizes of new devices reduce its susceptibility. These upset rates are thought to be mitigable with ECC. The internal memories of the Zynq-7020 SoC were also tested, revealing the increased susceptibility of the BRAM and CRAM of the PL side. Thus, scrubbing of these memories is required for correct operation. SEFI rates for NAND flash and Zynq SoC show that these events do not significantly impact the system if mitigated. Worst case conditions lead to one to two events per year. In all tests, it was clear that until 5.0mm shielding, upset rates are reduced. Also, high inclination orbits are responsible for increased number of SEE. Models and assumptions were validated with available literature.

Specification for the proposed system were derived with particular focus on availability and cost figures. Reliability block diagrams with the most susceptible blocks were used in conjunction with calculated upset rates to determine mean time to fault. Mean time to recover were assumed with known information and available literature. The results clearly show the impact of the frequent scrubbing of the Zynq's configuration RAM on overall availability. Nevertheless, availability is better than 5 nines in half of the study cases. The lowest availability is for 2.5mm shielding in worst case, high inclination, high altitude orbit. In this case, less than 8h downtime per year is estimated which is better than requirements. Warm redundancy was shown to have a small impact on availability due to the fact that it reduces MTTR in cases with low event rate. However, redundancy increases reliability in the case of unit failure. Rough order of magnitude costs were estimated. It showed that COTS are up to 1000 times less expensive for the same functionality than qualified versions. The Supervisor, as it is composed of only qualified devices is the most expensive unit, representing more than half the total system component cost. This was found to be approximately 87000€ for non-redundant configuration and 120000€ for a redundant configuration. This is significantly lower than if qualified components were the basis of the design. Size, weight and power were estimated to be on par with competitors. Performance is expected to be highly superior to competitors based on the high processing power and programmability of the Zynq SoC.

14.2. Fulfillment of research objective

The research objective proposed in chapter 1 is re-stated below. It is thought that this objective was achieved by the thesis project.

Obj-1: To support the development of EO small satellites constellations (50kg to 200kg) by designing a cost-effective baseline avionics architecture that maximizes availability and reduces recurrent engineering and integration efforts.

The project was able to identify common requirements for EO small satellite constellations that enable a highly recurrent avionics system to be designed. This system incorporates all functionalities predicted in the SAVOIR reference architecture including payload interface, AOCS, C&DH, TM/TC,

reconfiguration and mass memory. The interfaces are customizable with little engineering effort, supporting multiple missions and customer requirements. In turn, this system was designed from the start to employ COTS products as much as possible with little impact on availability. This was accomplished by the use of protection methods that minimize the consequences of using COTS in harsh environments. In particular, space-qualified components in a supervisor unit support these architecture. Availability figures due to ionizing radiation were predicted that show, at this preliminary stage, that less than 8h downtime per year is achievable. Hence, the fulfillment of the research objective is demonstrated.

14.3. Answers to research questions

The thesis strived to answer a number of research questions proposed at the beginning of this project. The following bullet points provide a summary answer to these questions and reference to the chapters and sections where more in-depth information on the subject can be found.

- **RQ-1:** What functional units should an avionics architecture have in order to reduce recurrent engineering and integration efforts?
  - The avionics shall contain the functionalities mentioned in figure 8.4 which essential are related to internal power distribution, calculation of AOCS algorithms and interface with peripherals, running RTOS and other C&DH related functions, interface with payload including processing and storage of data, TM/TC coding/decoding at layer 2 based on hardware and system reconfiguration based on functional monitoring or ground commands. (chapters 4 and 8)
- **RQ-2:** How can a new avionics architecture contribute to reduce recurrent engineering and integration efforts?
  - Providing functions that are similar across a range of LEO missions. (chapter 4)
  - Targeting a wide variety of LEO missions and budgets by developing an architecture that can be made redundant or non-redundant with low additional component cost. (chapters 4 and 12)
  - A single external interface with the possibility of internal redundancy reducing cable harnessing mass and complexity for the S/C whilst ensuring dependability. (chapter 9)
  - Adequate choice and flexibility of implemented I/O protocols by specially designed PCBs that make use of 0Ω resistors to adapt to multiple configurations of peripherals. Choosing commercial ICs that share the same package and similar pinouts along with utilization of multiplexed I/Os on the SoC allows for this flexibility. (chapter 9)
  - Utilizing SAVOIR reference architecture to minimize development risks. (chapter 8)
- **RQ-3:** How can the design maximize system availability in a cost-effective way?

  RQ-3A: What protection systems are required to increase availability?
  - As described in chapter 10, protection systems are based on fault masking and reconfiguration. (chapter 10)
  - Fault masking is achieved by means of LCL, galvanic isolation provided by COTS components, fail-safe devices (also COTS), ECC on memories and scrubbing of the configuration RAM for the Zynq's PL. (chapter 10)
  - A rad-hard supervisor is the heart of the reconfiguration process which is based on functional monitoring via continuous communication and current monitoring, and a custom boot and configuration process. (chapter 10)
  - The last resort protection system is a watchdog timer, resetting the supervisor's FPGA in the event of functional interrupt on this unit. (chapter 10)

  RQ-3B: How can the combination of space-grade and commercial components be exploited to achieve high availability?

- Restrict the use of rad-hard components to certain essential features such as TM/TC, reconfiguration and time distribution. (chapter 8)
- Careful analysis of the response to radiation enables the selection of rad-tolerant COTS with similar functionality to rad-hard counterparts. (chapter 11)
- Filtering for certain features in COTS devices such as galvanic isolation and fail-safe inputs/outputs. (chapter 10)

RQ-3C: How does the combination of highly reliable and less reliable components affect overall cost?

- Main cost inducing unit is the Supervisor. Most costly component is the rad-hard FPGA. (chapter 12)
- COTS components are a fraction of the cost of qualified counterparts. (chapter 12)
- Component cost increase from non-redundant to redundant configurations, or from less to more memory, is a small percentage. (chapter 12)
- This particular functional allocation leads to similar component costs as a fully rad-hard SBC but with a lot more functionality. (chapter 12)

- **RQ-4:** What are the expected performance and dependability figures for this architecture?
  - Tolerates 5 or more years in LEO. (chapter 11)
  - A radiation induced availability better than 3 nines or 99.9% is achievable for LEO orbits even in worst case space weather conditions. (chapter 11)
  - SEL rate is lower than one every 195 days in worst case conditions. Events are limited to micro-latchups which are not immediately destructible and are autonomously mitigated via power cycle. (chapter 11)
  - It provides up to 2500DMIPS of processing power on the OBC unit in addition to a programmable logic fabric. (chapter 12)
  - Up to 128GB of payload data storage. (chapter 12)

15

Recommendations

This thesis project set the direction and laid the foundation to develop a highly integrated avionics system which possesses high dependability at a lower cost than comparable systems. It thus require further work in order to transform the vision into a ready-to-fly product. A number of open questions were identified which could be answered by future projects at PhD or MSc levels. Four recommendations for future work are hereby detailed with suggested methodologies to follow and outcomes to be obtained.

Flexible backplane

The envisioned cross-strapping and backplane design with flexible PCB segments reduce cable harnessing complexity, however it imposes difficult signal integrity challenges. It requires impedance matching along the entire signal path, including PCB vias and connectors. Simulating, implementing, testing and analyzing the results of this backplane solution could demonstrate this type of solution for other demanding applications. The suggestion is to start by determining the impact of the flex PCB with nanoD connectors on its ends on signal integrity. The project shall optimize trace width and separation for low jitter, skew and attenuation. This can be accomplished by simulation using tools such as HSPICE. Results shall be validated with a prototype that mimics the intended use of flexible PCB for internal redundancy depicted in figures 9.4 and 9.5. Hence, the setup shall measure parameters such as jitter, skew and attenuation, for signals flowing in and out of cross-strapped PCBs one at each the end of the flexible PCB 'wing'. Maximum data rates achievable for LVDS signals should also be acquired.

Reconfiguration over CAN bus

Functional monitoring and booting methodologies described in chapter 10 require implementation and validation over a CAN bus. In particular, the project should validate the ability of an FPGA algorithm to detect a fault of a target SoC and perform the reconfiguration process over a redundant CAN network. The project shall first determine a generic FDIR policy that targets the same reference missions. This policy must be flexible enough to adapt to multiple use cases with low recurrent changes. One open question is the type of faults that can be detected and how these can be detected. A test setup consisting of an FPGA communicating with the Zynq-7020 SoC over a CAN bus shall be designed or procured. Implementation of the FDIR policy on hardware and its testing shall validate the methodology. Additionally, optimization of this process, lowering the MTTR, is key into further validating the availability figures calculated in chapter 12. The test conditions shall mimic the intended use-case in terms of utilized computational and power resources, and size and complexity of on-board software. The project shall then generate conclusions on the suitability of this methodology, achieved MTTR and types and number of detectable and recoverable faults.

Shielding optimization

Analysis of the effects of radiation were confined to the effects of heavy ions since it represents the largest contribution to SEE. However, the literature study supporting this thesis project [16], pointed to effects lower energy particles such as low energy protons have on modern ICs. The continuation of the radiation effects analysis to include the effects of protons, other particles and more types of

SEE improves the quality of the radiation hardness assurance exercise. Furthermore, the performed work did not cover sector analysis which is important in optimizing shielding. Ray-tracing calculations also shed light onto the effect of the positioning of shielding and components within the system on the overall SEE rate. This complete radiation study is essential to minimize uncertainty and optimize the radiation hardness of the avionics. It is important that this study generates a recommended layout for the components inside the system and shielding characteristics including shielding materials and locations. SEE rates due to high and low energy particles shall be produced in order to optimize this shielding design.

Selection guidelines for COTS components

Recent advancements of COTS devices in terms of performance, reliability and radiation hardness are drawing the attention of the space community, hence this thesis topic. However, many companies in the industry still lack skills in radiation hardness assurance and understand the impact of COTS technologies on their systems. Additionally, performing radiation analysis for COTS devices requires compilation and handling of experimental data (if good quality results exist), which is resource consuming.

To leverage the utilizing of COTS products, increasing the performance whilst reducing costs, information and knowledge of the response of COTS to radiation environments should be spread amongst the community. In this thesis, some of this work was already performed. Other quality assurance parameters (such as thermo-elastic effects or out-gassing to name two), not addressed in this thesis also play a role in the reliability of COTS technologies in space applications. Building on the idea of comparing COTS and rad-hard components, chapter 12 did observe stark ROM unit cost differences between these types of devices.

It is suggested that a future work considers the aforementioned issues in order to determine guidelines and best policies for the selection and utilization of modern COTS electronics. Due to the high update rate of commercial technologies, the work should start by determining the differences between these and space grade counterparts that affect quality assurance. Besides radiation issues, one could also investigate the packaging of ICs and lot-to-lot variance and their impact. Complementing this, a cost analysis including all stages of the design process would improve the understanding of the impact of COTS products in the entire life-cycle of a space system. At the end, the work should produce a guideline for the selection of COTS, as opposed to space-qualified components, according to mission requirements. This guideline is to be supported by trade-off and meaningful ratios such as component cost versus testing effort or component cost versus radiation hardness, to name a few.

A

COTS components

A.1. Avionics

Company	Product	Architecture	Processor	Risk mitigation	Functions	Interfaces	TID [krad]	Power [Watts]	Mass[g]
Airbus	OSCAR	Modular	LEON3FT + ATMEL ATC18RHA	Full redundancy, functional cross strap, latchup immune	C&DH, TM/TC, PLIU, I/O	Serial, SpaceWire (SpW)	10	<15W	5
RUAG	Constellation Single Board Computer	SBC	PowerPC e500Core + SmartFusion2 (FPGA)	EDAC, latchup protection	C&DH, TM/TC, PLIU, I/O	Ethernet, Serial, SpaceWire	10	<20	225
Space Micro	Proton Box	Modular	Zynq 7020 or P2020 (PowerPc) or RTAX or Virtex FPGA	EDAC , optional latchup protection, autocorrected SEFI	C&DH, PLIU, I/O	Serial, SpaceWire,	<100	<20	<1kg
AAC Microtec	Sirius C&DH	Modular	OpenRISC (FPGA based) or LEON3FT	TMR on all FPGA gates, EDAC, dual redudnancy	C&DH, TM/TC, PLIU, I/O	Spacewire, Serial	20Krad	5	507

Xiphos	Q7	SBC	Zynq-7020 + Actel ProASIC3 (FPGA)	TMR, EDAC, upset monitor, FPGA Bit-stream scrubbing, Software robustness / watchdog	C&DH, I/O, PLIU	Ethernet, Serial, USB 2.0	No info	1	32g (no casing)
Aitech	SP0	SBC	PowerPC e500Core + ACTEL FPGA	Latchup immune, EDAC, watchdogs	C&DH, PLIU, I/O	Ethernet, Serial,	100	<12W	350
AgilSpace	OBC-15	SBC	TSC695FL (ERC32) + ProASIC3L FPGA	EDAC	C&DH, PLIU, I/O, TM/TC	Serial, backplane	No info	<7.5W	1500
Berlin Space Tech	OBC-100 & ACC-100	Modular	No info	No info	CPU (optional), TMTC , ADCS,	Serial etc	No info	No info	870
Seakr	Athena 2/3	SBC	PowerPC e500	No info	PLIU, TM/TC	SpaceWire, Serial, PCI, Ethernet (Optional)	No info	16W	500
Seakr	RCC	SBC	3 Virtex-5 FX-130T FPGAs	No info	PLIU	Ethernet			1600
Seakr	C&DH 2GEN	Modular	LEON	Warm redundancy	I/O, AOCS, TM/TC			<72W	9000
SSTL	CoreDHS	SBC	(LEON3FT + Zynq)	Dual Redundancy	C&DH, TM/TC, PLIU, AOCS				

Table A.1: Information in this table consists of information explicitly available from supplier's brochures and website and therefore might not fully represent the system's capabilities and specifications.

A.2. AOCS peripherals

Name	Company	Interfaces	Baud Rate [Kbps]	Update rate [Hz]	Power in
Reaction Wheels					
VRW-02	Vectronics Space	RS-422 or RS-485 or CAN	<1000	†	†
RWA1000	Millennium Space Systems	RS-485 or CAN	†	†	24V to 34V
RWU	Bradford	Analog or MIL-STD-1553B	†	†	±28V

HR04	Honeywell	CAN or LVDS or RS-422	†	†	22V to 34V
RW3 V1.9	Sinclair Interplanetary	2x RS485 or RS485+CAN	†	†	3.5V to 36V
GPS Modules					
SGR10	SSTL	2x RS-422 or CAN	†	1	±28V
NGPS-.1-422	New Space Systems	RS-422 or UART	†	1	24V to 36V
Space Explorer	General Dynamics	RS-422 or MIL-STD-1553B	†	1	22V to 36V
Phoenix	DLR	†			
301	SpaceQuest	2x (LVTTL or RS-422) + CAN (Optional)	921	†	3V3 or 6V to 42V
Sun Sensors					
FSS	Bradford	Analog (0V to 5V)	∆	∆	
SSOC-D60	Solar MEMS	RS-422	115.2	50	4.95V to 5.05V
SSOC-A60	Solar MEMS	5x Analog (0V to 5V) ∆	∆	3V3 or 5V	
NFSS-411	New Space Systems	RS-485	57.6	5	5V to 50V
NCSS-SA05	New Space Systems	5x Analog (0V to 5V)	∆	∆	5V
Control Moment Gyros					
Microsat CMG	Honeybee	RS-232 or RS-422			
Magnetometers					
3-axis MGTM	Meisei Electric	Analog (0V to 5V)	∆	∆	12V to 15V
MAG-3	Space Quest	Analog (±10V or ±5V)	∆	∆	15V to 34V or 5V
ACM	Magson	RS-485	†	†	16V to 40V
NMRM	New Space Systems	RS-485	†	<18	5V
Magnetorquers					
MTA	Meisei Electric	Analog	∆	∆	15V
NMTR-X	NewSpace Systems	Analog	∆	∆	5V to 28V
VMT-35	Vectronics Space	Analog	∆	∆	16V 28V
Star Trackers					
VST-41M	Vectronics Space	RS-422 or RS-485	†	4	9V to 18V or 18V to 40V
VST-68M	Vectronics Space	2x RS-422 or 2x Can	†	5	9V to 40V
Auriga	Sodern	SpaceWire	†	5	†
Pyxis	Andrews Space	RS-422 or RS-485	†	1	†
ST-16	Sinclair Interplanetary	CAN or RS-485+CAN or 2x RS-485	<2000 or 115.2	2	4V or 28V
T1 (only optical head)	Terma	SpaceWire	†	10	5V

T1 (with electronic unit)	Terma	2x SpaceWire or 2x RS-422	†	△	20V to 36V
Fiber Optics Gyros					
Astrix 1000	Airbus	Mil-STD-155B or RS-422	†		22V to 50V
1775	KVH	RS-422	9.6 to 4100	1 to 5000	9V to 36V
3000	KVH	RS-232 or Analog	115.2	100 to 1000	5V
3400	KVH	RS-422	115.2	1000	5V
GG1320AN	Honeywell	RS-422	1000	1000	15V to 5V

Table A.2: COTS AOCS peripherals and their specifications. For the peripherals were multiple factory configurations are available, ”or” is used in the specification. △: Not applicable; †: Not found

A.3. Satellite platforms

Satellite	Prime	Weight [kg]	Star Tracker		Magnetorquer (1-axis)		Magnetometer (3-axis)		Gyroscope	
			#	Interface	#	Interface	#	Interface	#	Interface
SSTL-X50	Surrey	50-100	2	SpaceWire	3	PWM	2	RS-422	2	RS-422
FLP2	DLR	50-200	1	†	3	†	2	†	4	†
RapidEye	Surrey	156	1	CAN	3	†	2	†	0	∆
Proba V	QinetiQ	138	2	†	3	†	2	Analog	0	∆
Biros	DLR	130	2	†	3	†	2	†	0	∆
STSat-1	Surrey	106	2	MIL-STD-1553B	3	MIL-STD-1553B	2	MIL-STD-1553B	4	MIL-STD-1553B
Deimos 2	Satrec	310	2	†	0	∆	2		4	
Dubai Sat 2	Satrec	300	2	CAN	3	CAN	2	CAN	4	CAN
STSat-3	Surrey	175	2	RS-422	0	∆	1	RS-422	4	RS-422
YouthSat	ISRO	92	1	†	2	†	1	†	2	†
Average/Mode			1.7	2	2.3	3	1.8	2	2.4	4
Standard Deviation			0.46		1.19		0.42		1.74	
Relative Standard Deviation			27%		52%		23%		73%	

Satellite	Prime	Weight [kg]	Sun Sensors		Reaction Wheel		GPS receiver		Propulsion		IMU	
			#	Interface	#	Interface	#	Interface	#	Interface	#	Interface
SSTL-X50	Surrey	50-100	4	Analog	3	RS485 + CAN	2	Switch + CAN	1	4x Switch	0	∆
FLP2	DLR	50-200	16	†	4	†	2	†	0	∆	0	∆
RapidEye	Surrey	156	3	†	4	CAN	1	CAN	1	CAN	0	∆
Proba V	QinetiQ	138	0		4	†	2	†	0	∆	0	∆
Biros	DLR	130	2	†	4	†	2	†	1	†	2	†
STSat-1	Surrey	106	1	MIL-STD-1553B	4	MIL-STD-1553B	1	MIL-STD-1553B	0	∆	0	∆
Deimos 2	Satrec	310	6	†	5	†	0	∆	1	†	0	∆
Dubai Sat 2	Satrec	300	6	CAN	5	CAN	2	CAN	1	CAN	0	∆
STSat-3	Surrey	175	4	RS-422	4	RS-422	1	RS-422	1	RS-422	0	∆
YouthSat	ISRO	92	4	†	4	†	2	†	1	†	0	∆
Average/Mode			4.6	4	4.1	4	1.5	2	0.7	1	0.2	0
Standard Deviation			4.22		0.54		0.67		0.46		0.63	
Relative Standard Deviation			92%		13%		45%		65%		283%	

Table A.4: Compilation of AOCS subsystem specifications of a selection of mission. The S/C were selected as representative of the reference mission on a basis of mass range, mission objective and use of a commercial satellite bus. Information retrieved from eoportal.org. ∆: Not applicable; †: Not found.

A.4. Low-Performance processing units

SoC	Manufacturer	Cost [€]	Architecture	DMIPS	Frequency [MHz]	Memory	Maximum Power [W]	TID [krad]	SEL [$MeVcm^2/mg$]
VA10820	Vorago Technologies	1000	ARM Cortex-M0	50	50	32KB Data + 128KB Program	0.06	300	110
ATmegaS128	Microchip	2000	8-bit AVR	8	8	4KB SRAM + 4KB EEPROM + 128 KB Flash	0.02	>30	62.5
ATmegaS64M1	Microchip	2000	8-bit AVR	8	8	2KB SRAM + 4KB EEPROM + 64 KB Flash	0.02	>30	62.5
UT32M0R500	Cobham	TBD	ARM Cortex-M0+	50	50	96KB SRAM + 64Mb Flash Memory	0.02	50	80
MSP430FR5969-SP	Texas Instruments	3200	16-bit RISC	8	16	64KB FRAM	0.008	50	72.5

SoC	UART	GPIO	I2C	SPI	CAN	ADC	Watchdog	PWM	External Memory	External Clock
VA10820	2	56	1	2	0	0	Yes	0	Via SPI	
ATmegaS128	2	46	1	1	0	7 differential channels 10-bit	Yes	Yes	Via SPI	Yes
ATmegaS64M1	1	27	0	1	1	3 differential channels 10-bit	Yes	Yes	Via SPI	Yes
UT32M0R500	2	48	2	1	2	16 channels 12 bit	Yes	3	Via SPI	Yes
MSP430FR5969-SP	1	40	1	1	0	16 channels 12 bit	Yes	Yes	Via	

Table A.6: Single Core. EAR restriction applies for VA10820 and UT32. Prices for ceramic packages versions. Prices obtained from mouser.com or contact with supplier. TBD: to be determined

A.5. High performance processing units

SoC	Manufacturer	Cost [€]	Architecture	DMIPS	Frequency [MHz]	Memory	Maximum Power [W]	TID [krad]	SEL [$MeVcm^2/mg$]
VA10820	Vorago Technologies	1000	ARM Cortex-M0	50	50	32KB Data + 128KB Program	0.06	300	110
Zynq-7020	Xilinx	137	2x ARM Cortex-A9 + Artix 7 FPGA	2500	866	576KB Cache +256KB SRAM	10	126	16
GR712RC	Cobham	25000	2x LEON3-FT	150	100	16KiB Cache + 192Kb Memory	1.4	300	37
GR740	Cobham	TBD	4x LEON4	425	250	2MiB Cache	1.8	300	60

Zynq UltraScale	Xilinx	3800	2x ARM Cortex-R5F + 2x ARM Cortex-A53 + FPGA	7760	1300 & 533	1MB Cache +384KB SRAM			

SoC	UART	GPIO	I2C	SPI	CAN	ADC	Watchdog	PWM	External Memory	External Clock
VA10820	2	56	1	2	0	0	Yes	0	Via SPI	
Zynq 7020	2	118	2	2	2	2x 18 differential channels 12-bit	Yes	Yes	Via QuadSPI or parallel	Yes
GR712RC	6	63	1	1	2	0	Yes	0	Parallel	Yes
GR740	2	38	0	1	2	0	Yes	0	Parallel	Yes
Zynq UltraScale	2	128	2	2	2	2x 17 differential channels 12-bit	Yes	Yes	Via QuadSPI or parallel	Yes

Table A.8: Prices obtained from mouser.com or contact with supplier. Zynq Ultrascale part is XCZU9CG-2FFVB1156I. Zynq-7020 part is XC7Z020-CLG484. TBD: to be determined

B

Preliminary FMECA

Faults related to data flowing in and out of functional units

ID	Item/Unit	Function	Failure Mode	Failure Cause	Local effects	Next higher level effects	End effects	Severity	Probability	Fault Prevention	Fault Detection	Fault Containment	Fault Recovery
F-S-1	OBC	OBC	Loss of interface to units	SEE on interface drivers	No data to/from functional units	Unavailable functional units	Unavailable functional units	III	Low		Current limiters	Isolate bus nodes	Power cycle affected driver
F-S-2			Loss of power to OBC	PCDU failure	No power		Loss of avionics	III	Low		Current monitors	Reset PCDU	
F-S-3			High current state in unit	SEL	Increased power consumption	Loss of components inside unit or entire unit	Unmanaged avionics	III	Medium		Current monitors	Current limiting	Power cycle system or affected units
F-S-4			Erroneous data in	SEU, SEFI	Wrong input to S/C command	Unpredictable	Unpredictable	II	Medium	EDAC	EDAC	EDAC	Report fault, ask for data resend
F-S-5			Erroneous data out	SEU,SEFI	Wrong input to functional units	Unpredictable	Unpredictable	II	Medium	EDAC	EDAC	EDAC	Report fault, resend data
F-S-6			Unresponsive unit	SEFI	Unpredictable behaviour	Unavailable unit	Unpreditable	III	Medium	Functional monitoring	Functional monitoring	Reset device	Restart previous activities
F-S-7	COMMS	COMMS	Loss of interface to antennas	SEE on interface drivers	No uplink or downlink to/from antennas	Inability to interact with ground	Uncommunicating S/C	III	Low		Current monitors	Current limiting	Power cycle, Use spare unit
F-S-8			Loss of interface with OBC	SEE on interface drivers	Inability to control communications	Inability to interact with ground	Uncommunicating S/C	III	Low		Current limiters	Isolate bus nodes	Power cycle affected driver
F-S-9			Loss of interface with OBC	SEFI on OBC	Inability to control communications	Inability to interact with ground	Uncommunicating S/C	III	Medium		Functional monitoring	Reset device	Restart previous activities
F-S-10			Loss of interface with payload data		Inability to receive payload data	Inability to downlink payload data	Mission failure	III	Low		Functional monitoring		Report fault
F-S-11			Loss of Power to Comms unit	PCDU failure	No power to Comms unit	Inability to encode/decode radio signals	Uncommunicating S/C	III	Low		Current monitors	Reset PCDU	Reset PCDU
F-S-12			High current state in unit	SEL	Increased power consumption	Loss of components inside Comms unit or entire unit	Uncommunicating S/C	III	Low		Current monitors	Current limiting	Power cycle system or affected units
F-S-13			Erroneous OBC data into unit	Error in OBC command, SEU	Unpredictable behaviour	Unpredictable behaviour	Unpredictable behaviour	III	Low	EDAC	EDAC	EDAC	Report fault, ask for data resend
F-S-14			Erroneous payload data into unit	SEU, SEFI in payload unit	Erroneous data into encoder	Bad downlink data	Degraded mission performance	II	Medium	EDAC	EDAC	EDAC	Report fault, ask for data resend
F-S-15			Erroneous data out of unit	SEU, SEFI	Erroneous data into antennas	Bad downlink data	Degraded mission performance	II	Medium	EDAC	EDAC	EDAC	Report fault, data resend
F-S-16				SEU, SEFI	Erroneous data into OBC	Unpredictable behaviour		II	Medium	EDAC	EDAC	EDAC	Report fault, data resend
F-S-17			Unresponsive unit	SEFI	Unpredictable behaviour	Unavailable unit	Uncommunicating S/C	III	Low	Functional monitoring	Functional monitoring	Reset device	Restart previous activities
F-S-18	AOCS	AOCS	Loss of interface with 1 AOCS component	SEE on interfaces	Inability to control or receive input from component	Reduced control algorithm input	Erroneous control algorithm output	I	Medium		Software	Isolate component from control loop	Use redundant unit
F-S-19			Loss of interface with multiple AOCS component	SEE on interfaces	Inability to control or receive input from component	Reduced control algorithm input	Erroneous control algorithm output, Uncontrolable S/C	III	Low		Software	Isolate components from control loop	Use redundant unit
F-S-20			Loss of data interface with OBC	SEE on interface drivers	No telemetry or commands to/from AOCS unit	Inability to control AOCS	Unavailable AOCS	III	Low		Current limiters	Isolate bus nodes	Power cycle affected driver
F-S-21			Loss of power to AOCS unit	PCDU failure	No power to AOCS unit	No power to AOCS devices	Uncontrolable S/C	III	Low		Current monitors	Reset PCDU	Reset PCDU
F-S-22			High current state in unit	SEL	Increased power consumption	Loss of component inside unit and/or AOCS devices	Uncontrolable S/C	III	Low		Current monitors	Current limiting	Power cycle system or affected units
F-S-23			Erroneous data into unit	Error in OBC command, SEU	Unpredictable behaviour	Unpredictable behaviour	Unavailable AOCS	III	Medium	EDAC	EDAC	EDAC	Report fault to OBC
F-S-24			Erroneous data out of unit	SEU, SEFI	Erroneous data into AOCS devices	Unpredictable behaviour	Uncontrolable S/C	III	Medium	EDAC	EDAC	EDAC	Recalculate control outputs
F-S-25			Unresponsive unit	SEFI	Unpredictable behaviour	Unavailable unit	Uncontrolable S/C	III	Medium	Functional monitoring	Functional monitoring	Reset device	Restart previous activities
F-S-26	PIU	PIU	Loss of data interface to payload	SEE on interface drivers	No interaction with payload	Payload Unavailable	Mission failure	II	Low		Current limiters	Power cycle	
F-S-27				Bad mechanical connection	No interaction with payload	Payload Unavailable	Mission failure		Low	During assembly	Lack of data input	Isolate interface	
F-S-28			Loss of data interface with OBC	SEE on interface drivers	No commands/telemetry to/from PIU	Unavailable PIU	Mission failure	III	Low		Current limiters	Isolate bus nodes	Power cycle affected driver
F-S-29			Loss of power to PIU	PCDU failure	No power to PIU	Unavailable PIU	Mission failure	III	Low		Current monitors	Reset PCDU	Reset PCDU
F-S-30			High current state in unit	SEL	Increased power consumption	Loss of component inside PIU and possibly entire PIU	Mission failure	III	Low		Current monitors	Current limiting	Power cycle system or affected units
F-S-31			Erroneous data into unit	Error in OBC command, SEU	Unpredictable behaviour	Unpredictable behaviour	Unavailable PIU	II	Medium	EDAC	EDAC	EDAC	Report fault to OBC
F-S-32			Erroneous data out of unit	SEU, SEFI	Unpredictable behaviour from OBC, bad downlink data	Unpredictable behaviour from OBC, bad downlink data	Mission performance degraded	II	Medium	EDAC	EDAC	EDAC	Resend data
F-S-33			PIU unresponsive	SEFI	Unpredictable behaviour	Unavailable PIU	Mission performance degraded	II	Medium	Functional monitoring	Functional monitoring	Reset device	Restart previous activities

C

Requirements

All requirements lists are organized in the form of tables composed of three columns:

- **ID:** Requirements are marked with a unique identification of each one of them and initials, that simplify its recognition as requirements. The definition of these initials is explained in the following section.
- **Description:** The text that specifies the requirement.
- **Traceability:** The code that provides traceability for the definition of that requirement. The code refers to a table, figure or other resource as mentioned in a footnote.
- **Compliance:** The compliance of the design to the requirements and respective verification method.

Below the description, an explaining text may be added. It is preceded by the word "NOTE:" and written in italics. It provides extra information aiding a better understanding of the requirements or verification methods. For clarity, requirements using the auxiliary verb "shall" are mandatory requirements and those using the verb "should" describe goals which are "nice-to-have" .

C.1. Requirements Identifier

The identification code (ID) of the requirements mentioned in this document is generated in the following manner:

1. The first letters specify the level of the requirement:
    - **HLR - High Level Requirement:** These requirements are the most high level requirements that provide a steering function to the rest of the project since there are no external stakeholders consulted to provide requirements.
    - **SR - System Requirement:** These are the requirements that concretely define the system.
2. The second set of letters indicate the type of requirement:
    - A - Attitude and orbital control system
    - P - Payload(s)
    - T - Telemetry and radio communications
    - C - Command & Data Handling
    - L - Lifetime
    - R - Reliability, Availability, Maintainability and Safety
    - S - Size, Weight and Power
    - W - Cost

- F - Performance
- E - Environmental
- O - Others
- I - Interface
- OP - Operational
- D - Design
- EL- Electrical
- SP - Supervisor

3. The last three digits indicate the number of the requirement that falls within the requirement type.

C.2. High-level requirements

C.2.1. Functional requirements

ID	Requirement Description
HLR-D01	The avionics shall consist of a single unit. *NOTE: the self-standing unit can consist of different modules/boards*
HLR-EL01	The avionics shall be capable of down-converting a 28V unregulated input power feed to the necessary regulated secondary voltage levels (e.g. 5V, 12V, 15V) and distribute them to peripherals.
HLR-EL02	The avionics shall be capable of down-converting a 28V unregulated input power feed to the necessary regulated secondary voltage levels (e.g. 5V, 12V, 15V) and distribute them inside the unit to the required components.

C&DH	
HLR-C01	The avionics shall supervise all spacecraft functions.
HLR-C02	The avionics shall collect telemetry data from the S/C systems, components and payloads.
HLR-C03	The avionics shall be able to store at least 4Gbyte of general housekeeping data on a non-volatile memory.
HLR-C04	The avionics shall cope with digital and analog inputs and outputs.
HLR-C05	The avionics shall route the decode telecommands to the appropriate units/subsystems inside or outside the avionics.
HLR-C06	The avionics shall run a RTOS.

AOCS	
HLR-A01	The avionics shall cope with at least twenty (20) AOCS peripherals (sensors and actuators). *NOTE: This number is required to accommodate the nominal and redundant AOCS peripherals used in current small satellite platforms.*
HLR-A02	The avionics shall control each of the AOCS peripherals via analog or digital interfaces.
HLR-A03	The avionics should provide regulated secondary voltage to AOCS peripherals.
HLR-A04	The avionics shall gather the analogue and digital housekeeping telemetry from AOCS elements (temperature, current, voltage, digital status, etc.).
HLR-A05	The avionics shall cope with at least one (1) propulsion units.
HLR-A06	The avionics shall control at least one (1) propulsion units.
HLR-A07	The avionics shall gather the analogue and digital housekeeping telemetry from the propulsion unit (temperature, current, voltage, digital status, etc.).
HLR-A08	The avionics shall interface with a GNSS receiver.
HLR-A09	The avionics shall acquire and distribute accurate knowledge of time from a GNSS signal to peripherals and inside the avionics unit.

Payload	
HLR-P01	The avionics shall cope with at least two (2) hosted payloads.
HLR-P02	The avionics shall independently and simultaneously control each of the hosted payloads directly from their back-end electronics.

HLR-P03	The avionics shall gather the analogue and digital housekeeping telemetry from hosted payloads (temperature, current, voltage, status, etc.)
HLR-P04	The avionics shall simultaneously receive and locally store telemetry (housekeeping and science data) from the hosted payloads. *NOTE: the purpose is to reduce the buffering requirements in their back-end electronics.*
HLR-P05	The avionics shall handle bandwidths in the payload data interfaces up 2Gbps.
HLR-P06	The avionics shall locally store at least 64Gbyte of observation data from the payloads on a non-volatile memory.

TM/TC	
HLR-T01	The avionics shall apply CCSDS standards for TM/TC.
HLR-T02	The avionics shall interface with nominal and redundant RF units.
HLR-T03	The avionics shall receive digital uplink data packets from an RF unit.
HLR-T04	The avionics shall send digital downlink data packets to an RF unit.
HLR-T05	The avionics shall collect all S/C generated downlink data.
HLR-T06	The avionics shall distribute uplink data packets to the appropriate units or subsystems.
HLR-T07	All TM/TC coding and decoding of data packets shall be implemented in hardware.

Table C.1: High level functional requirements. The methodology for creating the requirements ID can be consulted in annex C.

C.2.2. Non-functional requirements

ID	**Requirement Description**
	Interfaces
HLR-I01	The avionics shall interface with the the satellite's hosted payloads, power distribution unit, analog radio units, AOCS components and other peripherals.
HLR-I02	The avionics shall develop all the following interfaces with S/C peripherals: • 2x Solar Array Step Motors I/F (22-38V, 290Ω, 260mH) • x2 SpaceWire • x2 CAN • x10 Analog Telemetry • x5 RS-422 (TM/TC) • x6 Discrete Commands
HLR-I03	The avionics shall develop all the following interfaces with the AOCS elements: • x3 Magnetorquers I/F (L=2.7H; R=66Ω) • x2 SpaceWire (Star Trackers) • x3 RS-422 (Gyros) • x2 CAN (Reaction Wheels) • x10 Analog Telemetry (Sun Sensors) *NOTE: All these interfaces are found in current AOCS COTS peripherals.*
HLR-I04	The avionics shall develop at least four (4) low-voltage differential signaling (LVDS) interfaces with the payloads.
HLR-I05	The avionics shall develop two (2) serial interfaces to telemetry RF units *NOTE: The purpose is to provide an interface to a nominal and a redundant radio unit.*
HLR-I06	The avionics shall develop three (3) serial interfaces to telecommand RF units *NOTE: The purpose is to provide an interface to a nominal and two redundant radio units.*
HLR-I07	The avionics shall provide over-voltage and over-current protection on all interfaces.

RAMS	
HLR-R01	A reliability analysis of the avionics shall be calculated for the reference mission.
HLR-R03	The reliability figure and drivers for extended or longer missions should be calculated for 7 and 10 years mission lifetimes.
HLR-R04	The avionics shall guarantee an availability of 99.9% or better throughout the entire course of a nominal mission.

HLR-R05	The avionics shall operate without significant performance and functional degradation for a minimum 5 years in LEO.

SWaP	
HLR-S01	The envelope volume shall be approximately 200 x 200 x 200 mm.
HLR-S02	The avionics and casing(s) shall have a combined weight of less than 5 kg.
HLR-S03	The maximum power consumption of the avionics shall be less than 40 Watts considering the worst case end-of-life condition.
HLR-S04	The nominal operating power should be less than 20W.

Environment	
HLR-E01	The avionics shall withstand a mission lifetime of five (5) years.
HLR-E02	The avionics should withstand a mission lifetime of ten (7) years.
HLR-E03	The avionics shall be designed to ensure that nominal performances and functionality are maintained without significant degradation in presence of radiation. Effects as: • Total Ionizing radiation dose (TID), including NIEL damage. • Single Event Latch-up (SEL) • Single Event Upset (SEU) • Burn-out • Single Event Gate Rupture (SEGR) • Single Event Transient (SET) • Single Event Functional Interrupt (SEFI) shall be considered for a LEO (300km to 1300km) during the design and analysis phases.
HLR-E04	The avionics power consumption shall not be significantly increased by TID effects during 5 years in LEO (300km to 1300km)
HLR-E05	The avionics design shall include mitigation techniques for non-correctable SEE.
HLR-E06	The stored data shall not be permanently corrupted by radiation affects.
HLR-E07	The avionics availability shall not be significantly reduced by SEE.
HLR-E08	The avionics shall be design to sustain an operating temperature range of -30 ºC to +60ºC

Others	
HLR-O01	The components of the avionics shall not be subject of third party access restrictions (such as ITAR).
HLR-O02	The avionics shall easily integrate with the S/C.
HLR-O03	The baseline avionics architecture should handle all imaging EO applications for satellites between 50kg and 200kg without requiring significant changes to its design.
HLR-O04	The avionics shall make use of COTS parts as much as possible.
HLR-O05	The avionics shall be design in order to be through-bolted on a S/C panel using M5 bolts.
HLR-O06	The hardware shall be designed to sustain the loads generated by the following events: • Manufacturing, assembly, ground handling and transportation loads • Test Loads • Launch loads: quasi static, vibration (including shock), thermal and pressure loads • Operational loads : including thermal, mechanism induced and pressure loads
HLR-W01	The avionics shall be cost competitive to related competitors.

Table C.2: High level non-functional requirements. The methodology for creating the requirements ID can be consulted in annex C.

C.3. System requirements

C.3.1. Functional requirements

ID	Requirement Description	Traceability [1]	Compliance
AOCS			
SR-A01	The system shall control the S/C attitude by interfacing with AOCS peripherals and providing computational resources.	A.1-01, A.1-07	Yes (review)
SR-A02	The system shall handle active and redundant AOCS peripherals.	HLR-A01	Yes (review)
SR-A03	The system shall be able to reconfigure its active and redundant AOCS peripherals.	HLR-A01	Yes (review)
SR-A04	The system shall generate sufficient data for the configuration, health and operation of the AOCS subsystem to be monitored.	HLR-A04	Yes (similarity)
SR-A05	A computational unit shall provide the capability to run attitude control algorithms.	A.1-07	Yes (similarity)
SR-A06	All the data from AOCS sensors and actuators shall be gathered in a single computational unit.	A.1-07	Yes (review)
SR-A07	All commands to AOCS peripherals shall be generated by a single computational unit.	A.1-07	Yes (review)
SR-A08	The AOCS health and operational monitoring data of the previous 48 hours shall be stored non-volatile memory.	A.1-04, A.1-06	Yes (similarity)
SR-A09	All AOCS functions shall be maintained with full performance after a single failure.	HLR-R05	Yes in redundant configuration (review)
SR-A10	The system shall cope with AOCS peripherals with different update rates.	7.1	Yes (similarity)
SR-A11	The system shall provide AOCS peripherals with power in the case they required regulated voltages. *NOTE: Some COTS AOCS peripherals require low-voltage regulated power supply.*	HLR-A03	Not designed
SR-A12	The system shall monitor the current flowing to the AOCS peripherals it powers. *NOTE: Some COTS AOCS peripherals already provide current monitoring and limiting capabilities.*	HLR-A04	Not designed
Peripherals			
Sun Sensor			
SR-A13	The system shall cope with four (4) external sun sensors.	7.1	Yes (review)
SR-A14	The system shall develop analog interfaces (0V to 5V) with the sun sensors.	7.1	Yes (review)
SR-A15	The system shall simultaneously receive and convert five (5) analog signals (0V to 5V) from a single sun sensor into digital signals. *NOTE: Each sun sensor has four photo-detectors and one thermistor outputs.*	7.1	Yes (review)
SR-A16	The converted digital signal from the sun sensors shall be connected to a processing unit.	7.1	Yes (review)
SR-A17	The system shall provide a 5V regulated power input and return to each sun-sensor.	7.1	Not designed
SR-A18	The system shall provide a common ground to each sun sensor.	7.1	Not designed
Star Tracker			
SR-A19	The system shall cope with two (2) star trackers.	7.1	Yes (review)
SR-A20	The system shall develop bi-directional SpaceWire interfaces with the star trackers.	7.1	Yes (review)

[1] Referring to figure 7.1 and high level requirements C.2.

SR-A22	The system shall, if necessary, provide means to convert the SpaceWire link to an interface standard supported by the processing unit. *NOTE: Commercial SoC often do not natively support SpW.*	7.1	Yes (review)
SR-A23	The system shall cope with SpaceWire signal rates higher than 80MHz.	7.1	Yes (similarity)
SR-A24	The system shall independently control each star tracker via the SpaceWire interface.	7.1	Yes (review)
SR-A25	The system shall gather telemetry and housekeeping data from each star tracker via the Spacewire interface.	7.1	Yes (review)
SR-A26	The system shall support an update rate of the star trackers of 10 Hz.	7.1	Yes (similarity)
SR-A27	The system shall be able to perform initial attitude determination and continuing attitude determination update from the star tracker when no autonomous operation of the star tracker is available. *NOTE: Star Tracker with both optical heads or optical head with electronics unit are expected.*	7.1	Yes (similarity)
SR-A28	The system shall provide a 5V regulated power supply to each star tracker.	7.1	Not designed
Reaction Wheel			
SR-A29	The system shall cope with 4 reaction wheels.	7.1	Yes (review)
SR-A31	The system shall develop two (2) RS-485 interfaces to each reaction wheel. *NOTE: As per ICD.*	7.1	Yes (review)
SR-A30	The system should support a CAN interface to the reaction wheels.	7.1	Yes (review)
SR-A32	The system shall be able to individually control each reaction wheel by sending telecommands via the assigned interfaces.	7.1	Yes (review)
SR-A32	The system shall be able to gather telemetry and housekeeping data from each reaction wheel via the assigned interfaced.	7.1	Yes (review)
GNSS			
SR-A33	The system shall cope with one nominal and redundant GNSS units.		Yes (review)
SR-A34	The system shall develop one RS-422 interface to the GNSS units		Yes (review)
SR-A35	The system shall support the input and distribution of PPS signals from a GNSS unit.		Yes (review)
SR-A36	The system shall develop LVTTL outputs to reset the GNSS units.		Yes (review)
SR-A37	The system shall be able to determine positioning and time data from the outputs of the GNSS units.		Yes (review)
SR-A38	The system shall be able to distribute the time data from the outputs of the GNSS units.		Yes (review)
Magnetorquers			
SR-A39	The system shall cope with 3 magnetorquers.	7.1	Not designed
SR-A40	The system shall develop independent analog interfaces with each magnetorquer.	7.1	Not designed
SR-A41	The system shall control the current flowing to each individual magnetorquer via a driving circuit (28Ω).	7.1	Not designed
SR-A42	The magnetorquer's driving circuit shall generate an individual output analog signal (-28 to +28 V) to each magnetorquer.	7.1	Not designed
SR-A43	The magnetorquer's driving circuit shall individually control each magnetorquer via a PWM signal from a processing unit.	7.1	Not designed
SR-A44	The current flowing to each magnetorquers shall be individually measured.	7.1	Not designed
SR-A45	The system shall be able to gather analog or digital housekeeping information from the magnetorquers.	7.1	Not designed
Magnetometers			

SR-A46	The system shall cope with one nominal and redundant magnetometers.		Yes (review)
SR-A47	The system shall develop one RS-422 interface to the magnetomer units.		Yes (review)
SR-A48	The system shall control the magnetometer units via the RS-422 interface		Yes (review)
Gyroscope			
SR-A49	The system shall cope with three nominal and one redundant gyroscope.		Yes (review)
SR-A50	The system shall develop one RS-422 interface to the gyroscope units.		Yes (review)
SR-A51	The system shall receive angular velocity measurements via the RS-422 interface		Yes (review)

Table C.3: System requirements related to AOCS functions.

ID	**Requirement Description**	**Traceability** [2]	**Compliance**
TM/TC			
SR-T01	The system shall interface with RF front-end equipment.	HLR-T02	Yes (review)
SR-T02	The system shall apply CCSDS Data link layer protocols to inflowing and outflowing data. *NOTE: As described in the CCSDS Blue Books of recommended standards*	HLR-T01	Yes (review)
SR-T03	The system shall cope with simultaneous data transmission and reception.		Yes (review)
SR-T04	The system shall collect health and housekeeping data from the RF front-end equipment.		Yes (review)
Telemetry			
SR-T05	The system shall develop redundant data interfaces to an RF transmitter.	T.1-07	Yes (review)
SR-T05	All S/C telemetry shall be collected for downlink.	T.1-01	Yes (review)
SR-T06	CCSDS data link layer protocols shall be applied to the telemetry data.	T.1-04, T.1-05	Yes (review)
SR-T07	The system shall cope with real-time CCSDS data link layer processing of outflowing telemetry data.		Yes (similarity)
SR-T08	The system shall be able to buffer TBD (size) telemetry data.	T.1-03	Yes (similarity)
SR-T09	The system shall be able to store TBD (size) downlink data before being sent to an RF unit. *NOTE: The goal is to allow layer 2 protocols to be applied in advance to downlink window and improve processor task scheduling.*	T.1-08	Yes (similarity)
SR-T10	The system shall develop 2 serial interfaces with RF transmitters.	T.1-07	Yes (review)
SR-T11	The system shall collect health and housekeeping data from the RF transmitters.		Yes (review)
SR-T12	The system shall handle TBD bandwidth to the RF transmitter.		Yes (review)
SR-T13	The system shall be able to collect and send telemetry data directly to the RF receiver without applying decoding protocols.	T.1-07	Yes (review)
Telecommand			
SR-T14	The system shall develop redundant data interfaces to an RF receiver.	T.2-01	Yes (review)
SR-T15	Uplink data coming from the RF receiver shall be collected.	T.2-01	Yes (review)

[2]Referring to figures 7.2 and 7.3 and high level requirements in table C.2.

SR-T16	CCSDS data link layer protocols shall be applied to the collected uplink data.	T.2-04, T.2-05	Yes (review)
SR-T17	Telecommands shall be sent to the appropriate components or subsystems.	T.2-07	Yes (review)
SR-T18	The system shall cope with real-time CCSDS data link layer processing of inflowing uplink data.		Yes (similarity)
SR-T19	The system shall be able to store TBD (size) telecommand data.	T.2-08	Yes (review)
SR-T20	The system shall be able to buffer TBD (size) inflowing uplink data before being sent for decoding.	T.2-03	Yes (review)
SR-T21	The system shall develop 3 serial interfaces with RF receiver.	T.2-01	Yes (review)
SR-T22	The system shall collect health and housekeeping data from the RF receivers.		Yes (review)
SR-T23	The system shall handle TBD (bandwidth) from the RF receiver.		Yes (review)
SR-T24	The system shall be able to collect and store telecommand data directly from the RF receiver without applying decoding protocols.	T.2-07	Yes (review)

Table C.4: System requirements related to TM/TC functions. TBD: to be determined

ID	Requirement Description	Traceability [3]	Compliance
	Payload		
SR-P01	The system shall interface with at least two (2) hosted payloads.	HLR-P01	Yes (review)
SR-P02	The system shall be able to independently and simultaneously control each of the hosted payloads directly from their back-end electronics.	HLR-P013	Yes (review)
SR-P03	A processing unit shall calculate and generate command signals for the payloads.	P.1-07, P.1-08	Yes (review)
SR-P04	A processing unit shall be capable of processing housekeeping data from the payloads.	P.1-04	Yes (review)
SR-P05	A processing unit shall process the raw science data from the payloads.	P.2-04	Yes (similarity)
SR-P06	A processing unit should process the raw science data from the payloads in real time.	P.2-04	Yes (similarity)
SR-P07	The system shall perform at least the following level of processing of the raw-data from the payload electronics: • Packetisation with temporal storage following CCSDS standards. • Buffering and pre-processing of raw payload data. • Lossless data compression. *NOTE: the purpose is to reduce the downlink data bandwidth required and therefore increasing the volume of usable, processed data to be downlinked, or trade-off the lower data-rate to relax the downlink requirements*	P.2-05	Yes (similarity)
SR-P08	The system shall establish at least three (3) LVDS science data interfaces with the payloads	P.2-01	Yes (review)
SR-P09	The system shall establish a CAN bus for control and housekeeping with the payloads	P.1-01, P.1-11	Yes (review)
SR-P10	The system shall cope with both analog and digital housekeeping telemetry from the payloads.	P.1-02, P.1-03	Yes (review)
SR-P11	The system shall cope with both analog and digital commands to the payloads.	P.1-09, P.1-10	Yes (review)
SR-P12	The system shall handle bandwidths in the payload data interfaces from 50Mbps up to 2Gbps.	P.2-01	Yes (similarity)

[3] Referring to figures 7.4 and 7.5 and high level requirements in table C.2.

SR-P13	The system shall be able to buffer TBD (size) payload telemetry (housekeeping and science data) before it is sent for processing.	P.1-05. P.2-06	Yes (review)
SR-P14	The system shall simultaneously receive and locally store telemetry (housekeeping and science data) from the hosted payloads. *NOTE: the purpose is to reduce the buffering requirements in their back-end electronics.*	P.1-06	Yes (review)
SR-P15	The system shall locally store at least 256Gbyte of observation data from the payloads on non-volatile memory.	P.2-07	Yes (review)

Table C.5: System requirements related to payload functions.

ID	Requirement Description	Traceability [4]	Compliance
	C&DH		
SR-C01	The system shall provide general processing capability to operate the spacecraft and achieve the aims of the mission.		Yes (similarity)
SR-C02	The system shall be able to run a Real Time Operating System (RTOS).		Yes (similarity)
SR-C03	The system shall be able to forward telecommands for execution on target components or sub-systems at a defined time or position in space.	HLR-C05	Yes (similarity)
SR-C04	The system shall be able to store telecommands before being forward to the target component or subsystems.	HLR-C03	Yes (review)
SR-C05	The system shall be able to manage and distribute multiple time signals to target component or subsystems.	HLR-C05	Yes (review)
SR-C06	The system shall be able to monitor the status of its internal components and subsystems.	HLR-C02	Yes (review)
SR-C07	The system shall collect discrete internal values such as voltages, temperatures and other values useful for system characterization and mission success.	HLR-C02	Yes (review)
SR-C08	The system shall be able to centrally collect all housekeeping telemetry generated inside the system as well as by other S/C systems.	HLR-C02	Yes (review)
SR-C09	The system shall be able process, in real-time, all housekeeping telemetry generated inside the system as well as by other S/C systems.	HLR-C01	Yes (similarity)
SR-C10	The system shall be able to buffer TBD (size) housekeeping data before it is processed.	HLR-C03	Yes (similarity)
SR-C11	The system shall be able to store four (4) Gbytes of housekeeping data.	HLR-C03	Yes (review)
SR-C12	The system shall store TBD (size) configuration data in a non-corruptible memory.		Yes (review)
SR-C13	The system shall be able to configure itself by means of non-corruptible configuration data.		Yes (review)
SR-C14	The system shall be able to reconfigure itself by means of telecommands.		Yes (review)
SR-C15	The system shall provide means for the on-board software to control components and sub-system both internal and external to the avionics.		Yes (review)
SR-C16	The system shall develop 5 analog interfaces with peripherals.	HLR-C04	Yes (review)
SR-C17	The system shall convert the analog signals to digital signals to be accessible by a processing unit.	HLR-C04	Yes (review)
SR-C18	The system shall develop 2 digital interface with peripherals.	HLR-C04	Yes (review)
SR-C19	The digital interfaces with peripherals shall be accessible by a processing unit.	HLR-C04	Yes (review)
SR-C20	The system shall be controllable by electrical ground support equipment (EGSE).		Yes (similarity)

Table C.6: System requirements related to C&DH functions. TBD: to be determined

[4] Referring to high level requirements in table C.2.

ID	Requirement Description	Traceability [5]	Compliance
Supervisor			
SR-SP01	The system shall develop supervisor functions in one of its subsystems.		Yes (review)
SR-SP02	The supervisor shall be mainly composed of space qualified components. *NOTE: The supervisor is not expected to fail in order to avoid the "who supervises the supervisor?" question.*		Yes (review)
SR-SP03	The supervisor shall receive periodic health status telemetry from the multiple subsystems. *NOTE: To allow for fault detection.*	R.1-01	Yes (review)
SR-SP04	The supervisor shall receive periodic context telemetry from the multiple subsystems. *NOTE: To expedite task restoration in a new configuration.*	R.1-01	Yes (review)
SR-SP05	The supervisor shall monitor the current flowing to each of the system's internal boards.	R.1-02	Yes (review)
SR-SP06	The supervisor shall be controllable by telecommands directly from the RF front end.	R.1-03	Yes (review)
SR-SP07	The supervisor shall provide computational power to operate FDIR software.	R.1-04	Yes (review)
SR-SP08	The supervisor shall be able to control the electric power supplied to each board	R.1-05	Not designed
SR-SP09	The supervisor shall store TBD (size) of system restoration and context data.	R.1-09	Yes (review)
SR-SP10	The supervisor shall be able to change the configuration of active and redundant boards.	R.1-10	Yes (review)
SR-SP11	The supervisor shall be able to periodically match task context between active and redundant boards.	R.1-10	Yes (review)
SR-SP12	The supervisor shall be able to independently control and monitor each board of the system.	R.1-07	Yes (review)
SR-SP13	The supervisor shall be physically located in the same board(s) as the PSDU.	R.1-07	Not designed

Table C.7: System requirements related to supervisor functions. TBD: to be determined

C.3.2. Non-functional requirements

ID	Requirement Description	Traceability [6]	Compliance
RAMS			
SR-R01	A reliability analysis of the system shall be calculated for the reference mission.	HLR-R01	Yes
SR-R02	The reliability figure for the system shall be at least 950 FIT (FIDES Standard) [7] for a mission lifetime of 5 years according to the definition of the reference mission.	HLR-R02	Not performed
SR-R03	The reliability figure and drivers for extended or longer missions shall be calculated for 7 and 10 years mission lifetimes.	HLR-R03	Not performed
SR-R04	The system shall guarantee an availability of 99.9% or better throughout the entire course of a nominal mission.	HLR-R04	Yes (analysis)
SR-R05	The system shall operate without significant performance and functional degradation for a minimum 5 years in LEO.	HLR-R05	Yes (analysis)
SWaP			

[5] Referring to figure 7.6 and section 6.3.
[6] Referring to the high level requirements in table C.2 and concept in section 6.3.
[7] The Failures In Time (FIT) rate of a device is the number of failures that can be expected in one billion (10^9) device-hours of operation

SR-S01	The envelope volume shall be approximately 200 x 200 x 200 mm.	HLR-S01	Yes (review)
SR-S02	The system and casing(s) shall have a combined weight of less than 5 kg.	HLR-03-S02	Yes (similarity)
SR-S03	The maximum power consumption of the system shall be less than 60 Watts considering the worst case end-of-life condition.	HLR-03-S03	Yes (similarity)
SR-S04	The nominal operating power shall be no more than 50 Watts.	HLR-03-S04	Yes (similarity)

Environment			
SR-E01	The system shall withstand a mission lifetime of five (5) years.	HLR-E01	Yes (similarity; analysis)
SR-E02	The system should withstand a mission lifetime of ten (7) years.	HLR-E02	Not calculated
SR-E03	The system shall be designed to ensure that nominal performances are maintained without degradation in presence of radiation. Effects as: • Total Ionizing radiation dose (TID), including NIEL damage. • Single Event Latch-up (SEL) • Single Event Upset (SEU) • Burn-out • Single Event Gate Rupture (SEGR) • Single Event Transient (SET) • Single Event Functional Interrupt (SEFI) shall be considered for a LEO (300km to 1300km) during the design and analysis phases.	HLR-E03	Yes (analysis)
SR-E04	The system power consumption shall not be significantly increased by TID effects during 5 years in LEO (300km to 1300km)	HLR-E04	Yes (analysis)
SR-E05	The system design shall include mitigation techniques for non-correctable SEE.	HLR-E05	Yes (analysis)
SR-E06	The stored data shall not be permanently corrupted by radiation affects.	HLR-E06	Yes (analysis)
SR-E07	The system availability shall not be significantly reduced by SEE.	HLR-E07	Yes (analysis)
SR-E08	The system shall be design to sustain an operating temperature range of -30 ºC to +60ºC	HLR-E08	Yes (review)

Others			
SR-O01	The system shall be composed of a single unit.	HLR-D01	Yes (review)
SR-O02	The system shall be composed of redundant embedded system boards.	6.3	Yes (review)
SR-O03	The boards shall all be of a single form factor.	6.3	Yes (review)
SR-O04	The boards shall all be mounted on a common backplane.	6.3	Yes (review)
SR-O05	The system shall allow discrete connections between boards.	6.3	Yes (review)
SR-O06	All board shall be connected to the PSDU.	6.3	Not designed
SR-O07	Failures shall be contained to the board of origin.	6.3	Yes (similarity)
SR-O08	The system shall allow multiple combinations of active and standby boards.	6.3	Yes (review)
SR-O09	The components of the system shall not be subject of third party access restrictions (such as ITAR).	HLR-03-O01	Yes (review)

SR-O10	The system shall easily integrate with the S/C.	HLR-O02	Yes (similarity)
SR-O11	The baseline system architecture shall handle all expected EO (imaging and SAR) applications for satellites between 50kg and 200kg without requiring significant changes to it's design.	HLR-O03	Yes (review)
SR-O12	The system shall make use of COTS parts as much as possible.	HLR-O04	Yes (review)
SR-O13	The system shall be design in order to be through-bolted on a S/C panel using M5 bolts.	HLR-O05	Not designed
SR-O14	The hardware shall be designed to sustain the loads generated by the following events: • Manufacturing, assembly, ground handling and transportation loads • Test Loads • Launch loads: quasi static, vibration (including shock), thermal and pressure loads • Operational loads : including thermal, mechanism induced and pressure loads	HLR-O06	Not analysed
SR-O15	The system shall be cost competitive to related competitors.	HLR-W01	Yes (review)

Table C.8: System non-functional requirements.

Bibliography

[1] S. Duzellier, *Radiation effects on electronic devices in space,* Aerospace Science and Technology **9**, 93 (2005).

[2] Union of Concerned Scientists, *UCS Satellite Database,* (2018).

[3] G. D. Krebs, *Description of SkySat satellites,* https://space.skyrocket.de/doc_sdat/skysat-3.htm (2019), web article.

[4] S. Curiel, A. Cawthorne, J. Penson, and M. Sweeting, *Production engineering a low cost video imaging constellation,* Proceeding of the IAA Symposium on Small Satellites for Earth Observation (2015).

[5] OHB Sweden, *InnoSat Platform,* (2018), brochure.

[6] A. O. Erlank and C. P. Bridges, *A multicellular architecture towards low-cost satellite reliability,* 2015 NASA/ESA Conference on Adaptive Hardware and Systems, AHS 2015 , 1 (2015).

[7] A. O. Erlank and C. P. Bridges, *Satellite stem cells: The benefits & overheads of reliable, multi-cellular architectures,* IEEE Aerospace Conference Proceedings , 1 (2017).

[8] S. Parkes, *SpaceWire User's Guide,* (2012).

[9] S. S. Centre, *System-Level Mitigation of SEFIs in Data Handling Architectures , A Solution for Small Satellites,* (2005).

[10] C. Mitchell, J. Rexroat, S. A. Rawashdeh, and J. Lumpp, *Development of a modular command and data handling architecture for the KySat-2 CubeSat,* IEEE Aerospace Conference Proceedings , 1 (2014).

[11] T. Helfers, G. Vives, A. Defence, S. Gmbh, and C. Papadas, *HPDP-40 High Performance Data Processor – A New Generation Space Processor in Demonstration,* (2019).

[12] M. Suess, J. Ilstad, and W. Gasti, *Galvanic Isolation of SpaceWire Links Requirements , Design Options and Limitations,* (2009).

[13] R. Ecoffet, *Overview of In-Orbit Radiation Induced Spacecraft Anomalies,* IEEE Transactions on Nuclear Science **60**, 1791 (2013).

[14] G. Furano and A. Menicucci, *Roadmap for On-Board Processing and Data Handling Systems in Space,* in *Dependable Multicore Architectures at Nanoscale*, edited by M. Ottavi, D. Gizopoulos, and S. Pontarelli (Springer International Publishing, Cham, 2018) pp. 253–281.

[15] C. Inguimbert, S. Duzellier, R. Ecoffet, L. Guibert, J. Barak, and M. Chabot, *Using a carbon beam as a probe to extract the thickness of sensitive volumes,* IEEE Transactions on Nuclear Science **47**, 551 (2000).

[16] R. C. Amorim, *Literature Study: Radiation Hardness Assurance on Microcontrollers for Deep Space CubeSats*, Tech. Rep. (TU Delft, Delft, 2019).

[17] J. Whalen, D. McKinney, R. Wray, and W. Mackey, *System Engineering Handbook,* (2000).

[18] R. H. Maurer, M. E. Fraeman, M. N. Martin, and D. R. Roth, *Space Radiation Environment, Effects, and Mitigation,* in *Johns Hopkins APL Technical Digest*, Vol. 28 (Johns Hopkins APL, 2008) pp. 17–29.

[19] D. V. Reames, *The two sources of solar energetic particles,* Space Science Reviews **175**, 53 (2013), arXiv:1306.3608 .

[20] A. Asrronau, G. Britain, A. Medicine, and C. Medicine, *RADIATION PROTECTION IN SPACE,* Acta Astronautica **35** (1995).

[21] J.-C. Boudenot, *Radiation Space Environment,* in *Radiation Effects on Embedded Systems* (Springer Netherlands, Dordrecht, 2007) pp. 1–9.

[22] Insoo Jun and W. McAlpine, *Displacement damage in silicon due to secondary neutrons, pions, deuterons, and alphas from proton interactions with materials,* IEEE Transactions on Nuclear Science **48**, 2034 (2001).

[23] C. Poivey, *Radiation Hardness Assurance (RHA) for Space Systems,* EPFL Space Center , 1 (2009).

[24] R. D. Schrimpf, *Radiation Effects in Microelectronics,* in *Radiation Effects on Embedded Systems*, edited by R. VELAZCO, P. FOUILLAT, and R. REIS (Springer Netherlands, Dordrecht, 2007) pp. 11–29.

[25] M. A. Silveira, K. H. Cirne, R. B. Santos, S. P. Gimenez, N. H. Medina, N. Added, M. H. Tabacniks, M. D. Barbosa, L. E. Seixas, W. Melo, and J. A. De Lima, *Performance of electronic devices submitted to X-rays and high energy proton beams,* in *Nuclear Instruments and Methods in Physics Research, Section B: Beam Interactions with Materials and Atoms*, Vol. 273 (Elsevier B.V., 2012) pp. 135–138.

[26] ECSS, *Single Event Effects Test Method and Guidelines, ESCC Basic Specification No.25100* (ESCC, 2002).

[27] ECSS, *Total Dose Steady-State Irradiation Test Method, ESCC Basic Specification No. 22900* (2007).

[28] R. Velazco, P. Fouillat, and R. Reis, *Radiation Effects on Embedded Systems*, edited by R. VELAZCO, P. FOUILLAT, and R. REIS (Springer Netherlands, Dordrecht, 2007).

[29] NASA Ames Research Center, *Small Spacecraft Technology State of the Art 2016*, Tech. Rep. December (2015).

[30] D. S. Lee, M. Wirthlin, G. Swift, and A. C. Le, *Single-Event Characterization of the 28 nm Xilinx Kintex-7 Field-Programmable Gate Array under Heavy Ion Irradiation,* 2014 IEEE Radiation Effects Data Workshop (REDW) **90245**, 1 (2014).

[31] J. Cruz-Colon, V. Narayanan, W. N. Vonbergen, R. G. Roybal, and R. C. Baumann, *Radiation Evaluation of the HVD233-SP CAN Transceiver,* 2018 IEEE Nuclear and Space Radiation Effects Conference, NSREC 2018 , 1 (2018).

[32] M. Ottavi, D. Gizopoulos, and S. Pontarelli, *Dependable Multicore Architectures at Nanoscale*, edited by M. Ottavi, D. Gizopoulos, and S. Pontarelli (Springer International Publishing, Cham, 2018) pp. 1–281.

[33] M. Yang, G. Hua, Y. Feng, and J. Gong, *Fault-Tolerance Techniques for Spacecraft Control Computers* (John Wiley & Sons Singapore Pte. Ltd, Singapore, 2017).

[34] B. Lal, *Global Trends in Small Satellites*, Tech. Rep. (IDA Science and Technology Policy Institute, 2018).

[35] M. Tipaldi and B. Bruenjes, *Survey on Fault Detection, Isolation, and Recovery Strategies in the Space Domain,* Journal of Aerospace Information Systems **12**, 235 (2015).

[36] J. R. Schwank, M. R. Shaneyfelt, and P. E. Dodd, *Radiation hardness assurance testing of microelectronic devices and integrated circuits: Test guideline for proton and heavy ion single-event effects,* IEEE Transactions on Nuclear Science **60**, 2101 (2013).

[37] James Richard Wertz; David F Everett; Jeffery John Puschell, *Space mission engineering : the new SMAD* (Hawthorne, CA : Microcosm Press : Sold and distributed worldwide by Microcosm Astronautics Books, ©2011, 2011).

[38] NASA Ames Research Center, *Small Spacecraft Technology State of the Art*, Tech. Rep. February (2018).

[39] R. Ginosar, *Survey of processors for space,* in *Proceedings of DASIA 2012 Data Systems in Aerospace* (2012) pp. 1–5.

[40] G. Lentaris, K. Maragos, I. Stratakos, L. Papadopoulos, O. Papanikolaou, D. Soudris, M. Lourakis, X. Zabulis, D. Gonzalez-Arjona, and G. Furano, *High-Performance Embedded Computing in Space: Evaluation of Platforms for Vision-Based Navigation,* Journal of Aerospace Information Systems **15**, 178 (2018).

[41] S. Guertin, *March 2012 P2020 Dual Core SEE Test Report*, Tech. Rep. March 2012 (NASA Electronic Parts and Packaging Program, 2013).

[42] A. Leach, *NASA's $2.5bn Curiosity rover: An Apple PowerBook on wheels,* (2012), Web article.

[43] T. Giagnacovo and E. Petritoli, *Rad-hard, in-flight, reprogrammable field FPGA architecture for satellite computers,* in *Proceedings of Italian Association of Aeronautics and Astronautics XXII Conference*, September 2013 (2013).

[44] A. Bernie, S. Curiel, N. Antoniu, L. Gomes, R. Goddard, J. Friend, and S. M. Sweeting, *Thinking Outside the " Cube ",* (2018).

[45] E. F. Hitt, *Fault-tolerant avionics,* Digital Avionics Handbook, Third Edition (2017), 10.1201/b17545.

[46] Technology Harmonisation Advisory Group, *Big Data from Space,* (2019), Draft technical note.

[47] C. Henry, *OneWeb's first six satellites in orbit following Soyuz launch,* spacenews.com/first-six-oneweb-satellites-launch-on-soyuz-rocket/ (2019), Web article.

[48] SpaceNews Staff, *Why OneWeb is Eager To Be the 'Clean-up Crew of Connectivity,* spacenews.com/in-conversation-with-oneweb-founder-greg-wyler (2015), web article.

[49] J. Barna, *Launch Approach, Spire Global,* (2015), presentation.

[50] G. D. Krebs, *Description of Lemur-2,* (2019), web article.

[51] G. D. Krebs, *Pearl 1,* https://space.skyrocket.de/doc_sdat/pearl.htm (2019), web article.

[52] Aistech Space, *Aistech Fleet,* aistechspace.com/fleet (2019), webpage.

[53] D. Wener, *Helios Wire sees a hidden fortune in finding lost assets,* (2018).

[54] Ecole Polytechnique Federale de Lausanne, *Astrocast successfully launches its first satellite,* (2018).

[55] G. D. Krebs, *Astrocast 0.1, 0.2,* https://space.skyrocket.de/doc_sdat/astrocast-0.htm (2019), web article.

[56] Earth Observation Portal, *SkySat,* (2019).

[57] Euroconsult, *Prospects for the small satellite market*, Tech. Rep. (2018).

[58] Earth Observation Portal, *SkySat constellation of Terra Bella,* (2019).

[59] D. Wener, *ICEYE achieves the 'impossible' with miniature radar satellite,* (2018).

[60] Airbus Defense and Space, *OneWeb Arrow Platform,* (2018).

[61] J. Amos, *OneWeb satellite operator eyes huge rocket campaign,* (2015).

[62] R. Sandau, H.-P. Roeser, and A. Valenzuela, eds., *Small Satellite Missions for Earth Observation* (Springer Berlin Heidelberg, Berlin, Heidelberg, 2010).

[63] P. Blau, *Flying Laptop,* (2019).

[64] OHB Sweden, *InnoSat and MATS,* .

[65] OneWeb, *ARROW,* (2019).

[66] F. Doengi, W. Engel, A. Pillukat, and S. Kirschstein, *JSS MULTISPECTRAL IMAGERS FOR EARTH OBSERVATION MISSIONS,* in *Small Satellites for Earth Observation* (DE GRUYTER, Berlin, Boston, 2012) pp. 10–13.

[67] P. Luquet, L. Brouard, and E. Chinal, *NAOMI instrument: a product line of compact and versatile cameras designed for HR and VHR missions in Earth observation,* **10566**, 147 (2017).

[68] F. M. Pranajaya, R. E. Zee, and S. C. O. Grocott, *NEMO-HD: HIGH-RESOLUTION MICROSATELLITE FOR EARTH MONITORING AND OBSERVATION,* .

[69] G. Bianucci, *A Reactive Multispectral Optical Payload for Small Satellites,* (2016).

[70] A. Seelin, K. Kumar, D. Rama, and M. Samudraiah, *Optical Payloads for Space Missions*, edited by S.-E. Qian (John Wiley & Sons, Ltd, Chichester, UK, 2015).

[71] F. E. Ivan Ferrario, Massimiliano Rossi, Antonio Ritucci, Marco Terraneo and Zocch, *HYPERSTREEGO: REACTIVE PAYLOAD,* in *The 4S Symposium 2016* (2016).

[72] R. Hoogeveen, J. de Vries, R. Voors, Q. Kleipool, I. Aben, P. Veefkind, N. C. J. van der Valk, I. Bhatti, and D. M. Woods, *The TROPOMI instrument: first H/W results,* Sensors, Systems, and Next-Generation Satellites XVII **8889**, 88890Q (2013).

[73] J. Lifshits, L. Stras, S. C. O. Grocott, F. M. Pranajaya, and R. E. Zee, *Next-generation for Earth Monitoring and Observation - High Definition Imaging and Video of Earth,* in *Optical Payloads for Space Missions* (John Wiley & Sons, Ltd, Chichester, UK, 2015) pp. 895–903.

[74] H. Saito, *Engineering-Model Results of X-band Synthetic Aperture Radar for Small Satellite and Its Application to Constellation Mission,* 32nd Annual Small Satellite conference , 1 (2018).

[75] M. Inggs, *Potential Synthetic Aperture Radar applications of small satellites Aspects of SAR Operation,* (2017).

[76] A. Aguasca, A. Broquetas, X. Fàbregas, A. G. Mondéjar, P. L. Dekker, C. L. Martínez, and J. J. Mallorqui, *Feasibility Study on SAR Systems on Small Satellites,* Communications , 1 (2009).

[77] T. Obata, T. Tohara, S. Nakamura, K. Hirako, H. Saito, S. Shirasaka, and S. Nakasuka, *Development of small satellite for X-Band compact synthetic aperture radar,* Journal of Physics: Conference Series **1130**, 012013 (2018).

[78] I. Opinions and M. Support, *Next Generation Processor for On-board Payload Data Processing Application ESA Round Table,* Round Table, The , 1 (2007).

[79] M. T. L'Abbate, *Compact Sar and Micro Satellite Solutions for Earth Observation,* 31st Space Symposium , 1 (2015).

[80] J. Y.-C. Yaung, S.-J. Chung, Y.-J. Lee, I. Y. Tarn, B.-H. Wu, C.-L. Chang, H.-C. Chang, and S.-J. Yu, *A Low Cost C-band SAR Small Satellite Definition for Disasters Management,* EUSAR 2014; 10th European Conference on Synthetic Aperture Radar; Proceedings of , 1 (2014).

[81] H. Saito, A. Tomiki, P. Akbar, T. Ohtani, K. Nishijo, J. Hirokawa, and M. Ando, *Synthetic aperture radar compatible with 100kg class piggy-back satellite,* Conference Proceedings of 2013 Asia-Pacific Conference on Synthetic Aperture Radar (APSAR) , 88 (2013).

[82] L. Jiang, P. Xu, F. Zhan, X. Fang, and M. Xin, *Research and development of integrated avionics for quick responsive micro-satellites,* Proceedings - 2016 6th International Conference on Instrumentation and Measurement, Computer, Communication and Control, IMCCC 2016 , 504 (2016).

[83] Y. Kobayashi, N. Gouda, T. Tsujimoto, T. Yano, M. Suganuma, M. Yamauchi, N. Takato, S. Miyazaki, Y. Yamada, N. Sako, and S. Nakasuka, *Nano-JASMINE: a 10-kilogram satellite for space astrometry,* Space Telescopes and Instrumentation I: Optical, Infrared, and Millimeter **6265**, 626544 (2006).

[84] J. Eickhoff, *Onboard Computers, Onboard Software and Satellite Operations*, Springer Aerospace Technology (Springer Berlin Heidelberg, Berlin, Heidelberg, 2012) p. 282.

[85] M. Authors, D. Version, and M. Authors, *Delft University of Technology LUMIO: a CubeSat at Earth-Moon L2,* (2018).

[86] S. Maqbool, *A System-level Supervisory Approach to Mitigate Single Event Functional Interrupts in Data Handling Architectures*, Ph.D. thesis, Universit of Surrey (2006).

[87] Solar MEMS, *SSOC-A60 - Technical Specification, Interfaces & Operation Page:,* (2015).

[88] Terma-Space, *T1 & T2 Star Trackers Specifications,* (2018).

[89] D. Sinclair, *RW-3 Interface Control Document,* (2016).

[90] SpaceQuest, *GPS-601 Satellite GNSS Receiver,* (2019), brochure.

[91] S. Interplanetary, *Microsatellite Torque Rods,* .

[92] U. S. Patent, *GG1320AN User's Manual,* (2015).

[93] CCSDS, *TM Synchronization and Channel Coding,* Ccsds 131.0-B-1 (2017).

[94] SAVOIR Advisory Group, *Introduction and Status of SAVOIR,* (2015).

[95] S. Yoon, Y. Shin, J. Jeon, Y. Seo, J. Jeon, J. Woo, and J. Seon, *Analysis of the charged particle radiation effect for a CubeSat transiting from Earth to Mars,* Current Applied Physics **14**, 575 (2014).

[96] P. Kotiranta, I. Kelander, M. Rouvala, and J. Takaneva, *Characterization of flexible interconnects in mobile devices,* Proceedings - 11th IEEE Workshop on Signal Propagation on Interconnects, SPI 2007 , 113 (2007).

[97] P. Kotiranta, I. Kelander, and M. Rouvala, *SPI Proceedings: Analysis of High-Speed Digital Interfaces in Flexible Interconnections,* in *2006 IEEE Workship on Signal Propagation on Interconnects* (IEEE, 2006) pp. 231–234.

[98] R. York, *Benchmarking in context: Dhrystone,* ARM, March (2002).

[99] DSPACE Project, *DSP for Space Applications,* in *2nd Seventh Framewrok Programme Space Conference* (2012).

[100] R. Trautner, J. Both, D. Merodio, R. Jansen, and R. Weigand, *DSP and FPGA – Competition , Synergy , and Future Integration,* (2016).

[101] Tsvika Israeli, *RC64 - Rad-hard high-performance DSP manycore,* (2017).

[102] M. A. Syed and E. Schueler, *High Performance Data Processor (HPDP),* Proceedings of the 2008 NASA/ESA Conference on Adaptive Hardware and Systems, AHS 2008 , 178 (2008).

[103] Ramonchips, *RC64 Many-Core DSP,* (2019).

[104] 1-CORE Technologies, *SRAM Based FPGA Architectures Overview,* .

[105] D. S. Lee, *Commercial Field-Programmable Gate Arrays for Space Processing Applications,* (2017).

[106] R. Glein, F. Rittner, A. Becher, D. Ziener, J. Frickel, J. Teich, and A. Heuberger, *Reliability of space-grade vs. COTS SRAM-based FPGA in N-modular redundancy,* 2015 NASA/ESA Conference on Adaptive Hardware and Systems, AHS 2015 (2015), 10.1109/AHS.2015.7231159.

[107] I. Troxel, *Memory Technology for Space,* (2009).

[108] B. De Salvo and L. Baldi, *Memory Technologies,* in *Nanoelectronics: Materials, Devices, Applications*, Vol. 1 (Wiley-VCH Verlag GmbH & Co. KGaA, Weinheim, Germany, 2017) pp. 113–136.

[109] E. J. Wyrwas, *DDR Memories NASA Electronic Parts and Packaging Program*, Tech. Rep. (2017).

[110] A. Zadeh, J. Ilstad, G. Furano, and D. Thurnes, *ESA UNCLASSIFIED-For Official Use Mass Memory Storage and the use of Commercial Off the Shelf (COTS) EEE Components. Workshop on High End Digital Processing Technologies and EEE Components for Future Space Missions*, Tech. Rep. (2018).

[111] F. Irom and D. N. Nguyen, *Radiation Tests of Highly Scaled, High-Density, Commercial, Non-volatile NAND Flash Memories— Update 2010,* (2010).

[112] Micron, *Selecting a Flash Memory Solution for Embedded Applications*, Tech. Rep. (2019).

[113] C. Sansoe and M. Tranchero, *Use of FRAM Memories in Spacecrafts,* in *Ferroelectrics - Applications* (InTech, 2011).

[114] M. Bagatin, S. Gerardin, and A. Paccagnella, *Space and terrestrial radiation effects in flash memories,* Semiconductor Science and Technology **32**, 033003 (2017).

[115] A. Tal, *NAND vs. NOR flash technology,* Electronic Products (Garden City, New York) **44**, 25 (2002).

[116] Xilinx, *Zynq-7000 SoC Technical Reference Manual,* Xilinx.Com **585** (2018).

[117] J. Bouwmeester, M. Langer, and E. Gill, *Survey on the implementation and reliability of CubeSat electrical bus interfaces,* CEAS Space Journal **9**, 163 (2017).

[118] J. Mellon and N. College, *Where and When Can We Use Google,* PS: Political Science & Politics **46**, 280 (2012).

[119] A. Valverde, L. Bolognino, and G. Furano, *CAN activities @ ESA,* (2017).

[120] G. Rouchaud and M. Jakob, *Mass reduction and higher data rate transmission with copper based components , Short Paper,* .

[121] D. Jameux, *SpaceWire evolutions and standard revision,* Discovery (2010).

[122] D. Selčan, G. Kirbiš, and I. Kramberger, *Nanosatellites in LEO and beyond: Advanced Radiation protection techniques for COTS-based spacecraft,* Acta Astronautica **131**, 131 (2017).

[123] F. Irom and M. Amrbar, *Heavy Ion Single Event Effects Measurements of Xilinx Zynq-7000 FPGA,* in *2015 IEEE Radiation Effects Data Workshop (REDW)*, Vol. 2015-Novem (IEEE, 2015) pp. 1–6.

[124] S. Parkes and C. Carrie, *SpaceWire 2016,* in *Proceedings of the 7th International SpaceWire Conference* (Space Technology Center, Universy of Dundee, 2016) p. 372.

[125] Texas Instruments and T. Kugelstadt, *RS-485 : Passive failsafe for an idle bus,* Analog Applications Journal , 22 (2009).

[126] D. L. Hansen, R. Hillman, F. Meraz, J. Montoya, and G. Williamson, *Architectural consequences of radiation performance in a flash NAND device,* IEEE Radiation Effects Data Workshop **2017-July** (2017), 10.1109/NSREC.2017.8115485.

[127] S. Mittal and M. S. Inukonda, *A survey of techniques for improving error-resilience of DRAM,* Journal of Systems Architecture **91**, 11 (2018).

[128] P. Dipartimento, A. M. Bagatin, S. Gerardin, A. Paccagnella, and U. Padova, *TID and SEE Report on Micron MT29F16G08ABABA Single-Level-Cell NAND Flash Memory,* , 1 (2013).

[129] P. Dipartimento, A. M. Bagatin, S. Gerardin, A. Paccagnella, and U. Padova, *TID and SEE Report on Micron MT29F32G08CBACA Multi-Level-Cell Single-Level-Cell NAND Flash Memory,* , 1 (2013).

[130] J. Heidecker, M. White, M. Cooper, D. Sheldon, F. Irom, and D. Nguyen, *Qualification of 128 Gb MLC NAND flash for SMAP space mission,* IEEE International Integrated Reliability Workshop Final Report , 145 (2010).

[131] M. Fabiano and G. Furano, *NAND flash storage technology for mission-critical space applications,* IEEE Aerospace and Electronic Systems Magazine **28**, 30 (2013).

[132] L. Huang, H. Zhang, R. Li, Y. Ge, and J. Wang, *AI Coding: Learning to Construct Error Correction Codes,* , 1 (2019), arXiv:1901.05719 .

[133] M. Berg, C. Poivey, D. Petrick, D. Espinosa, A. Lesea, K. A. LaBel, M. Friendlich, H. Kim, and A. Phan, *Effectiveness of internal versus external SEU scrubbing mitigation strategies in a Xilinx FPGA: Design, test, and analysis,* IEEE Transactions on Nuclear Science **55**, 2259 (2008).

[134] M. Amrbar, F. Irom, S. M. Guertin, and G. Allen, *Heavy ion single event effects measurements of Xilinx Zynq-7000 FPGA,* IEEE Radiation Effects Data Workshop **2015-Novem**, 1 (2015).

[135] A. Stoddard, A. Gruwell, P. Zabriskie, and M. Wirthlin, *High-speed PCAP configuration scrubbing on Zynq-7000 All Programmable SoCs,* FPL 2016 - 26th International Conference on Field-Programmable Logic and Applications , 1 (2016).

[136] J. Beningo, *A Review of Watchdog Architectures and their Application to Cubesats,* (2010).

[137] Spenvis Team, *Spenvis help guide,* spenvis.oma.be (2019), guide.

[138] S. Bourdarie, C. Inguimbert, J. R. Vaillé, P. Calvel, A. Sicard-Piet, D. Falguere, E. Lorfevre, R. Ecoffet, and C. Poivey, *Benchmarking ionizing space environment models,* Proceedings of the European Conference on Radiation and its Effects on Components and Systems, RADECS **2016-Septe**, 1 (2017).

[139] N. Ya'acob, A. Zainudin, R. Magdugal, and N. F. Naim, *Mitigation of space radiation effects on satellites at Low Earth Orbit (LEO),* in *2016 6th IEEE International Conference on Control System, Computing and Engineering (ICCSCE)*, November (IEEE, 2016) pp. 56–61.

[140] J. J. Likar, A. L. Bogorad, R. E. Lombardi, S. E. Stone, and R. Herschitz, *On-orbit SEU rates of UC1864 PWM: Comparison of ground based rate calculations and observed performance,* IEEE Transactions on Nuclear Science **59**, 3148 (2012).

[141] L. Scheick, *Testing Guideline for Single Event Gate Rupture (SEGR) of Power MOSFETs,* Jet Propulsion Laboratory (2008).

[142] F. Sturesson, J. Gaisler, R. Ginosar, and T. Liran, *Radiation characterization of a dual core LEON3-FT processor,* Proceedings of the European Conference on Radiation and its Effects on Components and Systems, RADECS , 938 (2011).

[143] R. Koga, S. Davis, and J. George, *Heavy Ion and Proton Induced Radiation Effects on Differential Bus Transceiver Microcircuits,* in *2017 IEEE Radiation Effects Data Workshop (REDW)*, Vol. 2017-July (IEEE, 2017) pp. 1–6.

[144] D. M. Hiemstra and V. Kirischian, *Single Event Upset Characterization of the Zynq-7000 ARM® Cortex™-A9 Processor Unit Using Proton Irradiation,* in *2015 IEEE Radiation Effects Data Workshop (REDW)*, Vol. 2015-Novem (IEEE, 2015) pp. 1–3.

[145] X. Du, S. Liu, D. Luo, Y. Zhang, X. Du, C. He, X. Ren, W. Yang, and Y. Yuan, *Single event effects sensitivity of low energy proton in Xilinx Zynq-7010 system-on chip,* Microelectronics Reliability **71**, 65 (2017).

[146] D. Chen, E. Wilcox, R. L. Ladbury, H. Kim, A. Phan, C. Seidleck, and K. A. Label, *Heavy Ion Irradiation Fluence Dependence for Single-Event Upsets in a NAND Flash Memory,* IEEE Transactions on Nuclear Science **64**, 332 (2017).

[147] L. A. Tambara, A. Akhmetov, D. V. Bobrovsky, and F. L. Kastensmidt, *On the characterization of embedded memories of Zynq-7000 all programmable SoC under single event upsets induced by heavy ions and protons,* Proceedings of the European Conference on Radiation and its Effects on Components and Systems, RADECS **2015-Decem**, 1 (2015).

[148] R. L. Nasa-gsfc, H. Kim, and M. Engineering, *Heavy Ion SEE Test Report for the MT29F2G08B Micron NAND Flash Memory,* (2012).

[149] T. R. Oldham, M. R. Friendlich, A. B. Sanders, C. M. Seidleck, H. S. Kim, M. D. Berg, and K. A. LaBel, *TID and SEE response of advanced Samsung and Micron 4G NAND flash memories for the NASA MMS mission,* IEEE Radiation Effects Data Workshop **20771**, 114 (2009).

[150] H. Schmidt, M. Hermann, and F. Gliem, *Radiation Hard Memory-Radiation Testing of Candidate Memory Devices for Laplace Mission,* in *CNES/ESA Radiation Effections Final Presentation Days*, March 10, (2015).

[151] L. A. Tambara, *Analyzing the Impact of Radiation-induced Failures in All Programmable System-on-Chip Devices,* (2017).

[152] X. Du, S. Liu, C. He, X. Du, Y. Li, Y. Zhang, W. Chen, X. Liu, and D. He, *Single event effects testing of Xilinx Zynq-7010 SoC with ²³⁹Pu alpha irradiation,* Applied Mechanics and Materials **678**, 268 (2014).

[153] V. Malherbe, G. Gasiot, D. Soussan, J. L. Autran, and P. Roche, *On-Orbit Upset Rate Prediction at Advanced Technology Nodes: A 28 nm FD-SOI Case Study,* IEEE Transactions on Nuclear Science **64**, 449 (2017).

[154] N. A. Dodds, J. R. Schwank, M. R. Shaneyfelt, P. E. Dodd, B. L. Doyle, M. Trinczek, E. W. Blackmore, K. P. Rodbell, M. S. Gordon, R. A. Reed, J. A. Pellish, K. A. LaBel, P. W. Marshall, S. E. Swanson, G. Vizkelethy, S. Van Deusen, F. W. Sexton, and M. J. Martinez, *Hardness assurance for proton direct ionization-induced SEEs using a high-energy proton beam,* IEEE Transactions on Nuclear Science **61**, 2904 (2014).

[155] J. A. Pellish, P. W. Marshall, K. P. Rodbell, M. S. Gordon, K. A. LaBel, J. R. Schwank, N. A. Dodds, C. M. Castaneda, M. D. Berg, H. S. Kim, A. M. Phan, and C. M. Seidleck, *Criticality of Low-Energy Protons in Single-Event Effects Testing of Highly-Scaled Technologies,* IEEE Transactions on Nuclear Science **61**, 2896 (2014).

[156] P. Dipartimento, A. M. Bagatin, S. Gerardin, A. Paccagnella, and U. Padova, *TID and SEE Report on Micron MT29F16G08ABABA Single-Level-Cell NAND Flash Memory,* , 1 (2013).

[157] N. A. McGirl, L. A. Castellanos, A. P. Srikrishna, L. Heilbronn, C. L. Tessa, A. Rusek, M. Sivertz, S. Blattnig, M. Clowdsley, T. Slaba, and C. Zeitlin, *Accelerator-based measurements relevant for shielding design in space,* IEEE Aerospace Conference Proceedings **2016-June** (2016), 10.1109/AERO.2016.7500858.

[158] B. Lussier, R. Chatila, F. Ingrand, M.-o. Killijian, and D. Powell, *On Fault Tolerance and Robustness in Autonomous Systems,* IARP/IEEE-RAS Joint Workshop on Technical Challenge for Dependable Robots in Human Environments , 1 (2004).

[159] G. O. Rabasa, *Methods for dependability analysis of small-satellite missions*, Ph.D. thesis (2019).

[160] K. A. Hoque, O. A. Mohamed, and Y. Savaria, *Towards an accurate reliability, availability and maintainability analysis approach for satellite systems based on probabilistic model checking,* in *Proceedings -Design, Automation and Test in Europe, DATE*, Vol. 2015-April (2015) pp. 1635–1640.

[161] C. Avionics, *Space Equipment PureLine Amethyst,* **20**.

[162] J. McHale, *Reduced SWaP , COTS in space , and budget constraints in the rad-hard world,* Mil-embedded.com (2015).

[163] T. M. Lovelly and A. D. George, *Comparative Analysis of Present and Future Space-Grade Processors with Device Metrics,* Journal of Aerospace Information Systems **14**, 184 (2017).

[164] T. Imken, J. Castillo-Rogez, Y. He, J. Baker, and A. Marinan, *CubeSat flight system development for enabling deep space science,* in *IEEE Aerospace Conference Proceedings* (IEEE, 2017) pp. 1–14.

[165] D. Rudolph, C. Wilson, J. Stewart, P. Gauvin, A. George, H. Lam, G. Crum, M. Wirthlin, A. Wilson, and A. Stoddard, *SSC14-III-3 CSP: A Multifaceted Hybrid Architecture for Space Computing,* 28th Annual AIAA/USU Conference on Small Satellites , 1 (2014).