POLITECNICO DI TORINO

Degree Course in Aerospace Engineering

Master’s Thesis in System Engineering

DEPENDABLE DESIGN OF AN EDUCATIONAL CUBESAT

Supervisors: Fabrizio Stesina
Sabrina Corpino

Candidate: Luisa Iossa

Academic Year 2021-2022

Index

Index of Figures

Index of Tables

List of Acronyms

ADC	Analog to Digital Converter
ADCS	Attitude and Determination Control System
BCR	Battery Charge Regulator
CAN	Controller Area Network
CIL	Critical Items List
CN	Critical Number
COMMSYS	Communication System
COTS	Commercial Off The Shelf
ECSS	European Cooperation for Space Standardization
EEE	Electrical, Electronic and Electro-mechanical
EPS	Electrical Power System
FDIR	Fault Detection Identification and Recovery
FM	Function Manager
FMEA/FMECA	Failure Modes Effects Analysis/Failure Modes Effects and Criticality Analysis
FTA	Fault Tree Analysis
FT	Fault Tree
GRVI	Green-Red Vegetation Index
IMU	Inertial Measurements Units
MLVDS	Multi Low-Voltage Differential Signaling
OBC	OnBoard Computer
PN	Probability Number
PU	Processing Unit
RAMS	Reliability Availability Maintenability Safety
RBD	Reliability Block Diagrams
RBF	Remove Before Flight
RGB	Red Green Blue
RM	Resource Module
RW	Reaction Wheel

SILVA	Satellite based Innovative Land and Vegetation Analysis
SN	Severity Number
SRR	Super Resolution Reconstruction
SS	Sun Sensor
TCS	Thermal Control System

1 Introduction

This thesis was developed in the CubeSat team Polito, and its purpose is to define and apply effective methods for the design of a dependable CubeSat in an academic context.

The heritage of launched educational missions involving CubeSats shows a non-negligible number of failures that causes low level of success of these missions. The workforce is generally inexperienced, the budget is limited, short development time, the use of components off the shelf (with high performance but not designed for hostile operative environment) and reduced and inadequate verification campaigns are the main root causes of this unsuccessful trend.

All these factors contribute to a high percentage of dead-on-arrival spacecrafts: 20% of launched CubeSats have never been operative, not even for the first contact with a ground station. Moreover, the infant mortality is relevant. Actually, failures do not affect only the educational CubeSats: 34% of CubeSats developers do not perform any kind of failure or risk analysis. As a result, about 65% of CubeSats' missions do not expect to be able to fulfill all their mission objectives. To mitigate the problems, CubeSat developers and integrators have worked on the quality of components and the improvement of the activities made in any phase of the product life cycle. At system level, the trend is to adopt high quality EEE elements, with higher reliability but higher cost. However, high cost, sophisticated instrumentation and tools and long environmental test campaigns are enemy of the educational programs.

One of the solutions to maintain COTS based project, with low budget and fast delivery is to adopt, at system level, dependable architectures. It means introducing redundancies at hardware, data, software level in the design phase and tailoring the procedures and rules for the testing phase.

The thesis aims at proposing a set of tools and methods that favour the design and verification of a dependable CubeSat, showing the effectiveness of this solution through a real case study, the new CubeSat 3U developed by the CubeSat team of Politecnico di Torino.

The result is an effective process that can be applied even by students to enhance the reliability of their CubeSats.

The first guideline is to integrate dependability activities in the early phases of a mission, as they can support the design and required trade-offs.

As soon as the system functional analysis is complete and a first architecture is defined, an FMEA (Failure Modes and Effects Analysis) analysis can be performed. The FMEA's purpose is to identify the main ways the system can fail, define the degree of severity of such failures, and assert detection methods and compensating measures for them.

The FMEA should help developers to identify the critical functions that the system shall perform to fulfill its mission objectives. The major FMEA drawback is the impossibility to evaluate the effect of combinations of failures. Then, a Fault Tree Analysis (FTA) should be executed. The FTA helps identify the minimum set of combined failures needed to make an undesirable event (such as the loss of a critical function) happen.

At this point, the developers can decide which mitigation strategies to apply to reduce the severity and probability of these failures. For COTS, the probability of failure occurrence shall be estimated by experience. Then, it is possible to build risk matrices for the system before and after the mitigation strategies. Reliability Block Diagrams (RBD) are another way to assess the mitigation strategies' impact, and to prove the increased system reliability by estimating the reliability of the system before and after applying mitigation strategies.

This method was applied to the mission under development in the CubeSat team Polito, SILVA.

SILVA is an Earth observation mission that aims to assess the health status of vegetation to study desertification and climate change-related phenomena. SILVA payload is an optical camera, whose images' resolution will be enhanced by onboard data processing. The CubeSat's critical functions are the ability to take clear pictures (thus, the ADCS system is critical) and to process them (thus, it was considered crucial that onboard processors would not fail). To preserve these functions, it was created a distributed architecture of three processors, that can reallocate ADCS, OBC, and mission data processing functions as needed if failures occur in one of them. Each processor continuously assesses the health status of the other ones and can operate critical hardware through two CAN buses.

These strategies increased the overall system reliability.

Chapter 2 presents more data about the current success rate of CubeSats missions.

Chapter 3 explains extensively the methodology used to design SILVA’s CubeSat.

Chapter 4 presents the SILVA mission and system.

Chapter 5 covers the executed analysis and the mitigation strategies proposed.

2 General CubeSat Reliability

A CubeSat is a class of miniaturized satellites based on a form factor consisting in 10 cm cubes, each unit weights 2 kg. The CubeSat Design Specifications was formulated in 1999 by a professor at Stanford University to promote and develop the skills required by the students to design, manufacture, and test a satellite able to work in Low Earth Orbit. Therefore, CubeSats were thought specifically to be used as a training tool in academic contexts.

Academia accounted for the majority of CubeSats launches until 2013, when more than half of launches were for non-academic purposes. By August 2021, more than 1600 CubeSats have been launched.

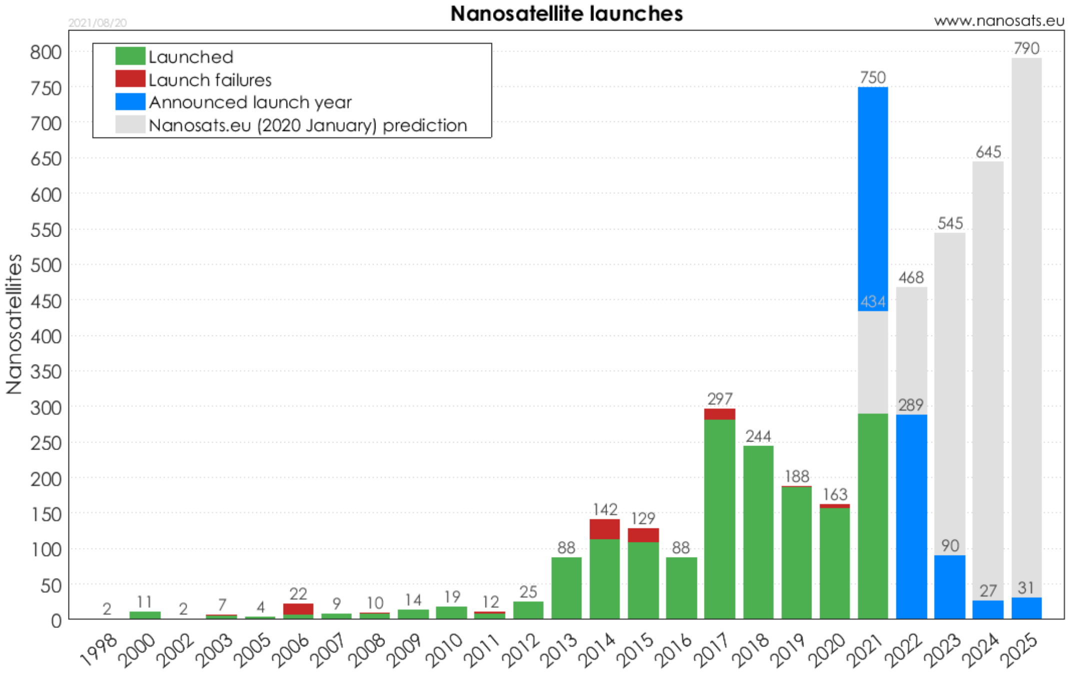


Figure 1 Nanosatellites launched (and planned) by year

The heritage of CubeSats educational missions shows a non-negligible level of low success.

CubeSats are developed as fast, cheap projects: the short development time often leads to inadequate and ineffective verification campaigns, while low budget makes integrate space-rated components not a viable option. Therefore, most CubeSats use commercial-off-the-shelf (COTS) components, that have high performances but are not designed to survive the hostile space environment. Moreover, in educational projects the workforce is inexperienced and there is a constant turnover of the operators involved in the mission. All these factors significantly increase the failure rate of these missions.

In non-educational context, CubeSats are often used to demonstrate spacecraft technologies intended for bigger satellites, when their feasibility seems questionable enough. Since CubeSats are quite inexpensive, their low cost justifies higher risks. However, it is always more common for

CubeSats to be destined to actual commercial and scientific purposes. In these missions, high risks are no longer tolerated. That justify the interest to decrease CubeSats' failures rate.

Several statistical analyses have been conducted to gather data and lessons learned about CubeSats' failures. Here, the results of a questionnaire carried in 2014 by Martin Langer and Eberhard Gill are covered.

The questionnaire is divided into three sections: the first one addresses general reliability aspects of CubeSats, the second one is focused on the CubeSats' interfaces, while the last one addresses the experts' insights of overall failure rates and causes for CubeSats. The questionnaire was completed by 138 participants, and the answers regarded 60 launched CubeSats and 44 under development ones.

CubeSats' mission objectives are divided into three groups: educational, technology demonstration, and operational mission (science, commercial, civil purposes). A single CubeSat might have mission objectives that fall in more than one category (for example, the combination of educational and technology demonstration is quite common). Participants were asked to assess the current success rate of their mission (Figure 2) and the expected one based on the current status of the project (Figure 3). 80% of educational launched CubeSats are considered successful; however, many teams consider a successful launch and limited operations by their satellite as a fulfillment of educational mission objectives, regardless of the functionality demonstrated by the spacecraft. For technology demonstration purposes, a minimum functionality of the CubeSat in orbit is required, and the success rate falls to 39%. The success rate decreases even further to 30% for operational missions, where the system actually has to provide a service according to its specifications.

Figure 4 shows the operational status of CubeSats after a selected set of months since launch. It is worth noticing that among CubeSats that have lost contact, 20% of the total have not been operational for their entire mission (dead-on-arrival satellites). Furthermore, the percentage of operational CubeSats drops from 90% to 65% within the first three months: this high infant mortality rate is quite typical for systems that are not extensively tested because it is more likely to have undetected defects.

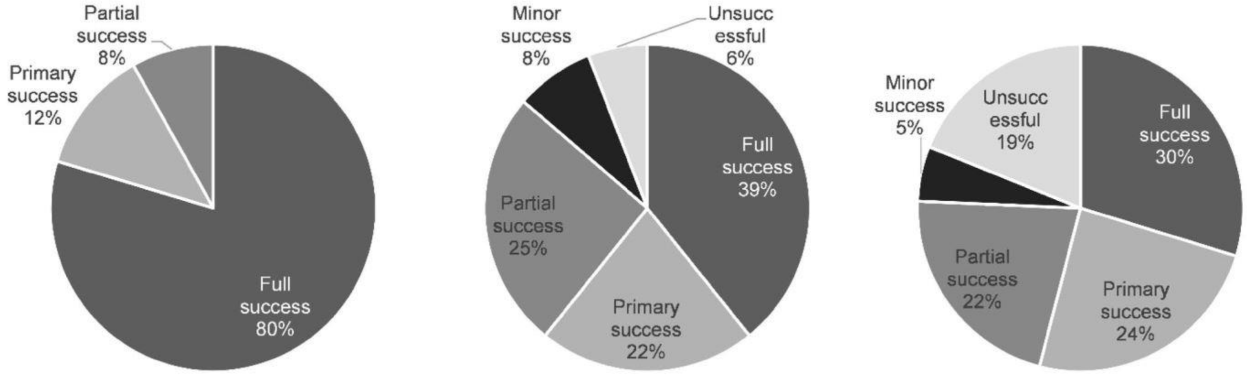


Figure 2 Current success rates of launched CubeSats for education (left, n = 49), technology demonstration (middle, n = 51), and operational mission (right, n = 32) objectives

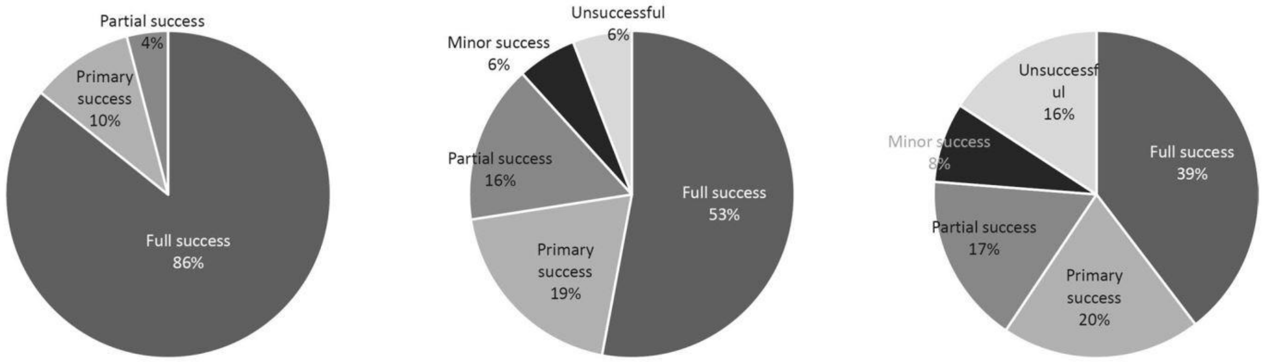


Figure 3 Expected final success rates for launched CubeSats for education (left, n = 49), technology demonstration (middle, n = 51), and operational mission (right, n = 32) objectives

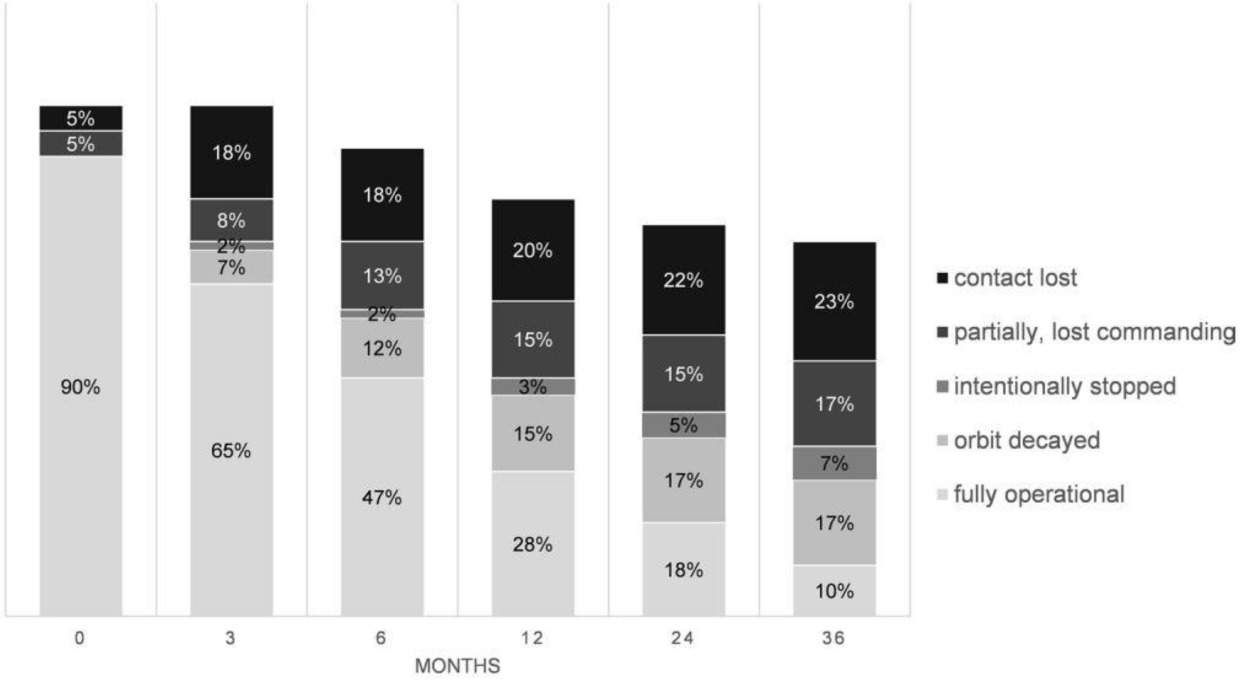


Figure 4 Operational status of CubeSats missions after launch

The results of a root cause allocation to subsystem are shown in Figure 5. The most critical subsystems are considered the ADCS, EPS, and Communication system; though, a significant percentage of failures are not clearly linked to any subsystem. The last point that this questionnaire highlights is that at least 34% of CubeSat developers do not perform a failure or risk analysis, even if most of them have knowledge and experience in these techniques (Figure 6). That is most likely caused by how time-consuming risk management tasks can be. Therefore, it is required to tailor standard dependability practices to suit the fast-paced development of a CubeSat.

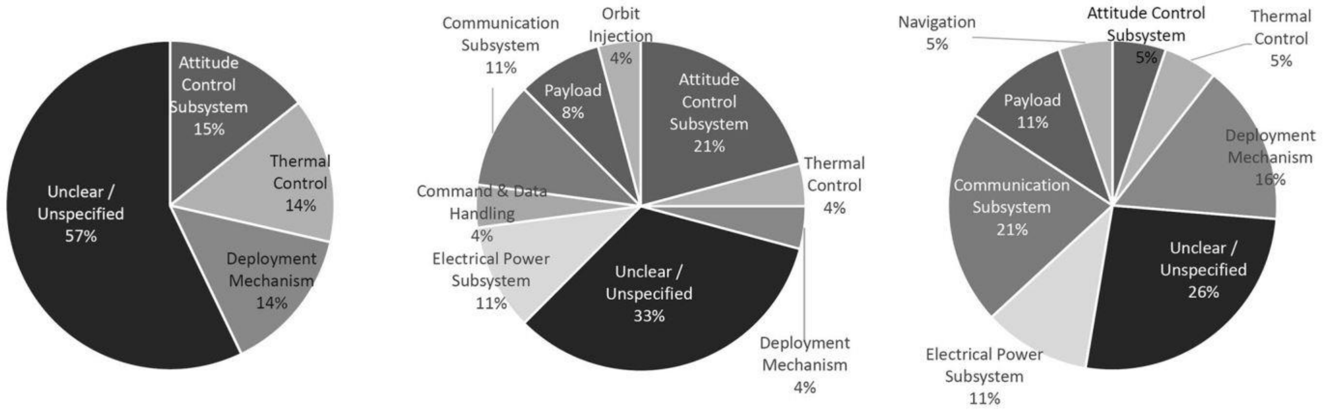


Figure 5 Root cause allocation for not achieving full success for education (left, n = 7), technology demonstration (middle, n = 24), and operational mission (right, n = 19) objectives

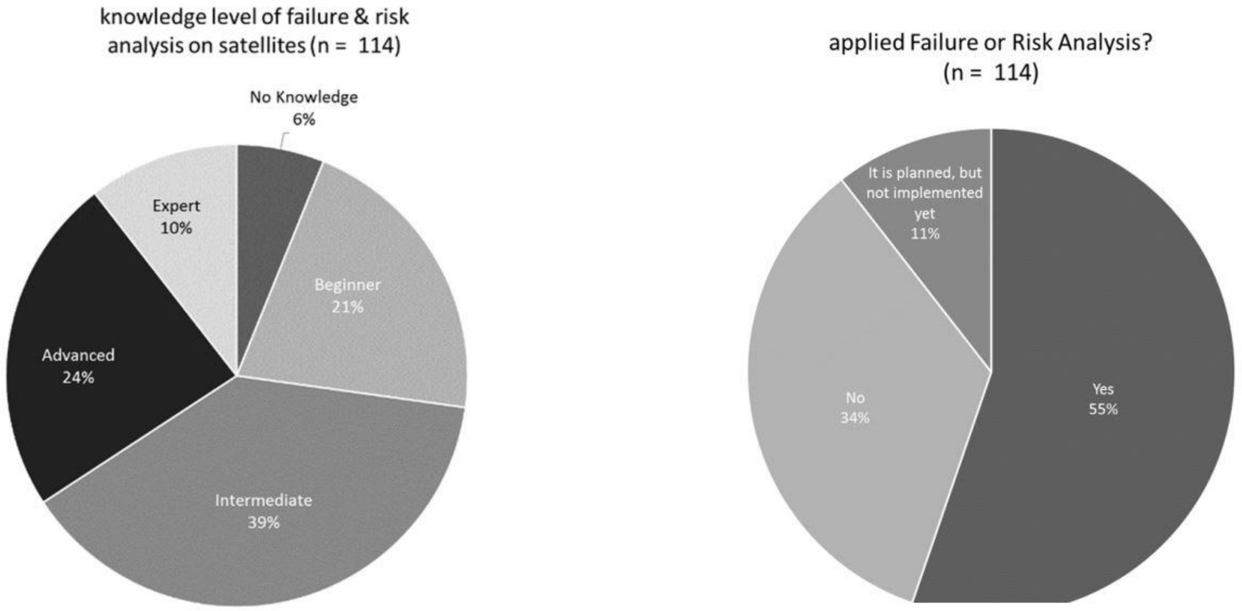


Figure 6 Knowledge level of failure and risk analysis (left); Missions where failure or risk analysis are performed (right)

3 Dependability

3.1 Basics of Dependability

A system dependability is defined as the extent to which the fulfilment of a required function can be justifiable trusted. Dependability includes different attributes of the system:

- Reliability: the ability of an item to perform a required function under given conditions for a given time interval. It is generally assumed that the item is in a state to perform this required function at the beginning of the time interval. Reliability is a measure of the system ability to deliver continuous and correct service.
- Availability: ability of an item to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided.
- Maintainability: ease of performing maintenance on a product.

Dependability should always be considered paired with safety, that is a system state where an acceptable level of risk is not exceeded. Risks are undesirable situations or circumstances that have both a likelihood of occurrence and a potential negative consequence on a project. Safety is affected by risks related to fatality, injuries, damage to infrastructures and pollution on environments external to the system.

There are several events that can decrease a system dependability:

- A fault is a physical defect, imperfection, or flaw that occurs in some hardware or software components. A fault can cause a failure and can be the result of a failure but can also exist without a prior failure.
- A failure is an event resulting in the system being no longer able to perform its required function. A system fails when its provided service is not compliant with the system specifications.
- An error is a deviation from correctness or accuracy in computation. It usually occurs as a result of a fault, as it is associated with incorrect values in the system state. It can also happen when the timing in computational operations is not accurately synchronized among different software functions.

3.2 Dependability approaches

The most efficient way to design a dependable system is to include dependability evaluations early in the project. If the system does not comply with dependable requirements, it is cheaper to alter the design before the manufacturing process has been initiated.

There are several techniques that help reaching the desired dependability levels: fault prevention, fault forecasting, fault removal, and fault tolerance.

Fault prevention, or fault avoidance, consists in the attempt to prevent the introduction of faults in the system altogether. Fault prevention is achieved through rigorous design and high-quality control standards during the manufacture phase. In the space industry, that translates in adopting space rated and radiation hardened hardware, which assures high reliability and robustness to the space environment's threats.

Fault forecasting has the purpose of estimating the number of faults present in the system, their probability of occurrence and their consequences to the system. It is carried by evaluation on the system functionalities, and it can provide qualitative or quantitative information on the system failures possibilities. This kind of activity is usually performed throughout the design process.

Fault removal aims at the reduction of the number of faults present in the system. In the space industry, fault removal is performed during the verification process. During the verification phase, the system is proved to be compliant with its requirements; if that does not happen, the faults that cause the non-compliance are identified and corrected. Fault removal is achieved through an extensive and accurate verification campaign that include several tests at subsystem and system level.

Fault tolerance is a design strategy that aims at obtaining a system that can recover from a failure and continue to operate correctly, possibly with lower performances. It is assumed that failures will happen, and the purpose is to reduce their impact on the system functionality.

This design method heavily relies on redundancies, that can be classified in three categories: hardware redundancy, information redundancy, and time redundancy.

The principle of implementing hardware redundancy is to have more hardware than needed to mitigate faults. Different design choices can be implemented:

- Passive redundancy: the redundant hardware is replicated at least three times. The same input is given to each unit, and a voter evaluates the output produced by each piece of hardware. If one result is significantly different from those produced by the other units, the voter isolates the faulty hardware and excludes its output from further calculations. This technique allows the system to ignore the fault without interrupting its service (it is called "masking"), but it works only if the voter is faulty-free and if the same fault is not present in all the different pieces of hardware.
- Active redundancy: the recovery from a fault passes through the detection, location, and containment of the fault. Once the faulty item is recognized, the system isolates it and reconfigures itself to activate the spare hardware instead of the faulty one.
- Hybrid redundancy: it is a combination of active and passive redundancy. A certain number N of modules are available, as well as M spare modules. A voter evaluates the output of the primary modules and, if a fault is detected from one of them, the faulty unit is replaced by one of the spares.

3.3 System response to failures

When a failure occurs, a redundant system responds to it in a manner that should be planned by the system designer. Generally, the system response to failures is articulated in the following phases:

- Fault confinement (or containment): the fault is restrained in the area it was originated in, and the fault propagation to other system parts is avoided. That can be achieved by introducing fault-detection circuits or by executing consistency checks before performing a function or using some data. These strategies can be designed both on hardware and software.
- Fault detection: in this phase the system recognizes something unexpected has happened. There are off-line detection techniques, like diagnostic programs, that can identify faults only when the system is not operating, while on-line detection techniques, like parity and duplication, can be performed during operations too.
- Diagnosis: a further phase that provides additional information about failure locations and properties.
- Reconfiguration: if a permanent failure is located, the system might reconfigure itself by replacing the faulty components with spare ones or by excluding the faulty components from the operations. After the reconfiguration, the system might operate with lower performances, and this process is called graceful degradation.
- Recovery: this phase aims at eliminating the effects of failure. If a fault is temporary, a retry attempt can be executed. The system is restored to a safe status before the faults occurred, and operations are restarted from that point. Another strategy is masking, where in the system redundant information are available to substitute the incorrect one during the calculations. That allows the system to keep operating without being affected by the failure.
- Restart: this process occurs after the recovery of damaged information. It can regard all operations from the point of fault detection without loss ("hot" restart), part of the operations ("warm" restart), or it can be a complete reload of the system ("cold" restart).
- Repair: the components that have failed are replaced. This procedure is not applicable to space systems in most of the cases.
- Reintegration: the repaired module must be integrated into the system and re-initialized to reflect the state of the rest of the functioning modules.

3.4 Basic reliability model

Among all the dependability aspects, this thesis focuses on reliability.

The most important parameter used to measure a system's reliability is the failure rate.

Failure rate, indicated by λ, is the expected number of failures per unit of time. It is usually expressed as [number of failures/hour]. It is a function of time, and in literature there are different distributions available. Most of the systems follows the trend shown in Figure 7 and generally known as bathtub curve. At the beginning of the operation life the failure rate is quite high because of non-qualitative enough components. As soon as these components fail and are removed from the system, the failure rate decreases to a constant value that characterize the system for its operative life. When components reach the end of their design life, the failure rate increases again because of wear out. Not all the class of components follow this trend: for example, electronic and electrical equipment generally do not present a wear out region.

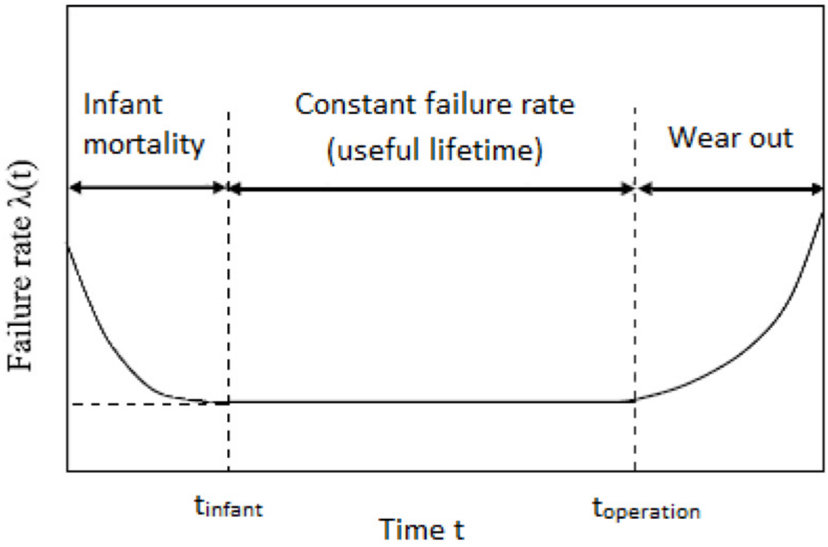


Figure 7 Distribution of failure rate over time

CubeSats as a system respect the bathtub curve quite well: at the beginning of their mission the failure rate is quite high because the faults that were not detected during the verification process manifest themselves, then the failure rate becomes a constant determined by the random failure that can happen, at last onboard equipment is always more unreliable as they reach the end of their design life and degrade.

3.5 Dependability methods

Dependability risk assessment and control are part of the risk management process, and their purpose is to identify and report dependability associated risks.

As stated in ECSS-Q-ST-30C, dependability risk analysis reduction and control shall include the following steps:

- identification and classification of undesirable events according to the severity of their consequences;
- analysis of failure scenarios, determination of related failure modes, failure origins or causes;
- classification of the criticality of the functions and associated products according to the severity of relevant failure consequences;
- definition of actions and recommendations for detailed risk assessment, risk elimination, or risk reduction and control to an acceptable level;
- status of risk reduction and risk acceptance;
- implementation of risk reduction;

- verification of risk reduction and assessment of residual risks.

Risk reduction measures that are proposed for dependability shall be assessed at system level in order to select the optimum solution to reduce the system level risk.

The process of risk identification and assessment can include both qualitative and quantitative approaches; when dealing with CubeSats it is usually preferable following a qualitative approach. As a matter of fact, most CubeSats feature COTS components that are rarely tested for reliability, so there is not enough data to conduct a rigorous quantitative analysis. Furthermore, even components that provide reliability information on their datasheet were not tested for a space application, so that data is not applicable to CubeSats' missions risk analyses.

The dependability tasks considered suitable for a CubeSat educational mission are the Failure Modes and effects analysis, the Fault Tree Analysis, and the Reliability Block Diagrams analysis.

3.5.1 Failure Modes, effects (and criticality) analysis (FMEA/FMECA)

The FMEA/FMECA analysis is primarily a reliability task, but it provides also information and support to safety, maintainability, logistics, test and maintenance planning, and failure detection, isolation and recovery (FDIR) design. They are performed to identify potential failures in both products and processes and to evaluate their effects. The purpose is to define mitigation strategies starting from those failures that have the highest impact on the project.

The FMEA/FMECA are bottom-up analysis that consider each single elementary failure mode and consider its effects propagating to the boundary of the analysed system. They are not well suited to evaluate the effects of a combination of different failures.

The FMEA evaluates the severity of every failure according to the severity levels described in Table 1 and applies a severity number for each failure mode following Table 2.

Table 1 Severity of failures' effects

Severity category	Severity level	Description of consequences (failure effects)	
		Dependability effects **(as specified in ECSS-Q-ST-30)**	**Safety effects** **(as specified in ECSS-Q-ST-40)**
Catastrophic	1	Failure propagation	Loss of life, life-threatening or permanently disabling injury or occupational illness.
			Loss of an interfacing manned flight system.
			Severe detrimental environmental effects.
			Loss of launch site facilities.

			Loss of system.
Critical	2	Loss of mission	Temporarily disabling but not life-threatening injury, or temporary occupational illness.
			Major detrimental environmental effects.
			Major damage to public or private properties.
			Major damage to interfacing flight systems.
			Major damage to ground facilities.
Major	3	Major mission degradation	
Minor or Negligible	4	Minor mission degradation or any other effect	

Table 2 Severity Number associated to Severity level

Severity level	Severity category	SN
1	Catastrophic	4
2	Critical	3
3	Major	2
4	Negligible	1

As prescribed by ECSS-Q-ST-30-02C, the FMEA shall be performed according to the following steps:

1) Describe the product (function or hardware) to be analysed, by providing:
   a) functional descriptions,
   b) interfaces,
   c) interrelationships and interdependencies of the items which constitute the product,
   d) operational modes,
   e) mission phases.
2) Identify all potential failure modes for each item and investigate their effect on the item under analysis and on the product and operation to be studied.
3) Assume that each single item failure is the only failure in the product. This implies that combination of failures is not considered.
4) Evaluate each failure mode in terms of the worst potential consequences and assign a severity category.
5) Identify failure detection methods.

6) Identify existing preventive or compensating provisions for each failure mode.
7) Provide for identified critical items corrective design or other actions (such as operator actions) necessary to eliminate the failure or to mitigate or to control the risk.
8) Document the analysis and summarize the results and the problems that cannot be solved by the corrective actions.
9) Record all critical items into a dedicated table as an input to the overall project critical item list (CIL).

The FMECA analysis is an extension of FMEA, as it classifies failures modes according to their criticality. Criticality keeps into account both the severity and the probability of failures modes.

The probability of failures modes and their associated probability number is evaluated as in Table 3. Then, the criticality number CN is computed as CN = SN x PN. A failure mode is considered critical if its CN is greater than 6.

Table 3 Probability of failures modes and Probability Number

Level	Limits	PN
Probable	P > 1E-1	4
Occasional	1E-3 < P ≤ 1E-1	3
Remote	1E-5 < P ≤ 1E-3	2
Extremely remote	P ≤ 1E-5	1

FMEA/FMECA should be initiated as soon as first information is available at high level of the system, and then it should be extended at lower levels once the system architecture is further defined. It is also possible to start a functional FMEA/FMECA since the beginning of the product lifecycle, and to convert it in a hardware analysis once the flight hardware is selected. It is important to perform this analysis early in the design process and to consider it an iterative activity. Late implementation of FMEA/FMECA greatly limits its use to improve the system design.

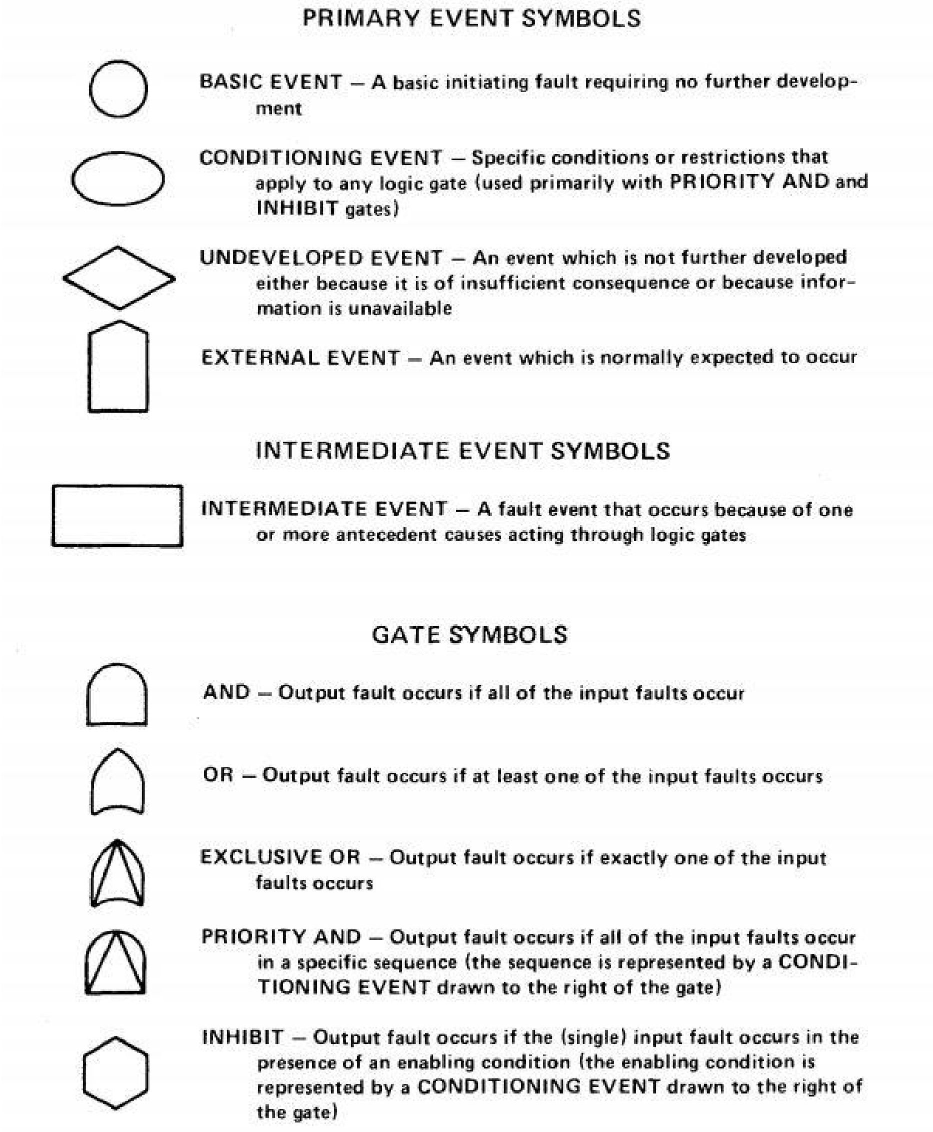
3.5.2 Fault Tree Analysis (FTA)

A Fault Tree Analysis is an analytical technique where the effects of a combination of failures are investigated. An undesired state of the system is specified, then the system is analysed in the context of its operations and environment to find credible ways in which the undesired event can occur. The analysis is carried out by assessing what failures in the next lower level can cause the undesired top event. Furthermore, it considers the logical relationships among the different failures related to the top event by correlating them through logical gates. The analysis is carried forward to lower levels until a satisfactory level of detail is reached.

Considered failures can include hardware failures, software failures, human errors, and everything that might be related to the realisation of the top event.

The FTA is a qualitative analysis, but it can be interpreted by Boolean algebra to obtain a set of equations that describe the logical relationship among the different elements of the fault tree. That allows to identify the minimum set of failures that must happen to realise the top event, and it is also possible to estimate the probability of system failure. If reliability information of the lower-level events is available, it is possible to perform a quantitative analysis.

It is necessary to draw multiple fault tree addressing different undesired events to have a complete description of the system.



PRIMARY EVENT SYMBOLS

BASIC EVENT – A basic initiating fault requiring no further development

CONDITIONING EVENT – Specific conditions or restrictions that apply to any logic gate (used primarily with PRIORITY AND and INHIBIT gates)

UNDEVELOPED EVENT – An event which is not further developed either because it is of insufficient consequence or because information is unavailable

EXTERNAL EVENT – An event which is normally expected to occur

INTERMEDIATE EVENT SYMBOLS

INTERMEDIATE EVENT – A fault event that occurs because of one or more antecedent causes acting through logic gates

GATE SYMBOLS

AND – Output fault occurs if all of the input faults occur

OR – Output fault occurs if at least one of the input faults occurs

EXCLUSIVE OR – Output fault occurs if exactly one of the input faults occurs

PRIORITY AND – Output fault occurs if all of the input faults occur in a specific sequence (the sequence is represented by a CONDITIONING EVENT drawn to the right of the gate)

INHIBIT – Output fault occurs if the (single) input fault occurs in the presence of an enabling condition (the enabling condition is represented by a CONDITIONING EVENT drawn to the right of the gate)

Figure 8 Fault Tree symbols

The FTA shall be performed according to the following steps:

1) Define the system and what it is considered a failure.
2) Define the top undesired events.

3) Identify causes for the top-level failure. Identify which faults can cause the failure alone (these are the input events for a gate "or") and which ones need to happen at the same time to make the top failure occur (these are linked by a gate "and").
4) For each event above, identify which faults cause them. Continue until the lowest level of interest is reached.
5) When possible, add probabilities of occurrence of each event.
6) Analyse the fault tree by identifying the events that can initiate multiple paths to failure.
7) Elaborate means to avoid or mitigate paths to failure.
8) Document the FTA and its results.

3.5.3 Reliability Block Diagrams (RBD)

Reliability Block Diagrams are another technique that shows the logical relationship among the different components of a system. The RBD is built by arranging the components in a network of series, parallel, or a combination of both, to describe how the system works.

A series network (Figure 9) corresponds to components that all need to work to allow the system to perform its function. All components cannot fail, and the system reliability is lower than the reliability of the worst component. If R is a measure of the reliability as the probability the system is working at a certain time, the reliability of the system can be computed as $R_{system} = \prod_{i=1}^{N} R_i$, while the failure rate is $\lambda_{system} = \sum_{i=1}^{N} \lambda_i$.

A parallel network (Figure 10) represents redundancies or a group of components where it is enough if only one of them works to allow the system to function. In this case, the reliability of the system is $R_{system} = 1 - \prod_{i=1}^{N}(1 - R_i)$ and it increases as the number of components increases.

A mixed network (Figure 11) can be solved by considering two different RBDs composed only by series and parallel networks, then by calculating the reliability of the system as the weighted mean value of the reliabilities of the two RBDs. Generally, these RBDs are obtained by considering the component that do not fall into the series or parallel always broken for the first RBD and always working for the second RBD. Then, the reliability of the component is used as a weight to calculate the mean value.

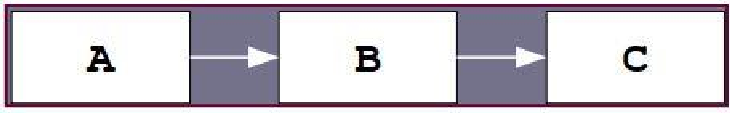


Figure 9 Series network

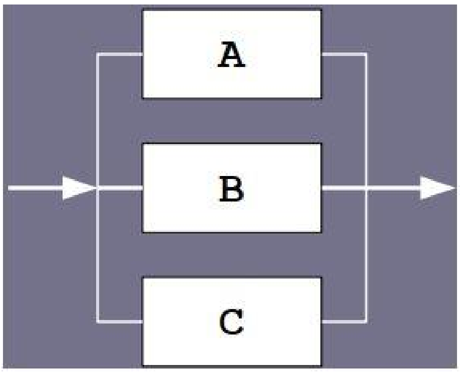


Figure 10 Parallel network

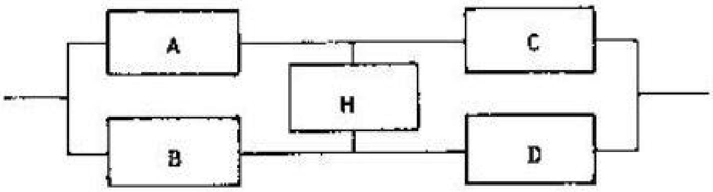


Figure 11 Mixed network

4 SILVA: mission and spacecraft

4.1 Mission objectives and payload

SILVA (Satellite based Innovative Land and Vegetation Analysis) is an educational Earth observation mission that aims at identifying and analyzing climate change effects on large green areas worldwide. The purpose is to collect data that can be used to prevent desertification and to evaluate the effectiveness of land restorations interventions or the consequences of deforestation. To fulfill this objective, the mission will perform vegetation mapping and assess vegetation status by computing the Green-Red Vegetation Index, defined as

$$GRVI = \frac{\rho_{green} - \rho_{red}}{\rho_{green} + \rho_{red}}$$

where ρ_{green} is the green reflectance and ρ_{red} is the red reflectance.

Given the nature of required data, the payload is a RGB camera. The quality of the mission data relies on the spatial resolution of the camera; unfortunately, the resolution of the selected camera is very likely to not be high enough to get useful information because of space and budget constraints. To overcome this issue, a software method is chosen to enhance the resolution of the data without having to select more expensive hardware. A Super Resolution Reconstruction algorithm (SRR) is implemented as onboard data processing: the same object is pictured from different perspectives in different images, and the non-redundant information from each image is combined to get an image characterized by higher resolution than the original ones. By using this technique, the collected data would have an accuracy high enough to get information with actual scientific value out of it. Another benefit of the onboard data processing is the reduction of the pictures number that is required to transmit to ground, resulting in a great simplification of the mission operations.

Therefore, the onboard data processing is considered a crucial feature to reach mission's success.

4.2 CubeSat's first design

SILVA's spacecraft is a 3U CubeSat, whose functions are represented by the functional tree in Figure 12. In a traditional design, those functions are allocated to CubeSat's subsystem as in the Function/Equipment Matrix (Table 4). The resulting system architecture is shown in Figure 13.

It is a straightforward system where each subsystem carries out the function it was designed to perform: communication from/to ground is guaranteed by the Communication System (COMMSYS), which operates in two frequency bands: UHF band to transmit housekeeping data and receive commands from ground, and S band to transmit mission data. The Electrical Power System (EPS) produces, stores, and distributes electrical power in the satellite. The Attitude Determination and Control System (ADCS) allows to determine and control the attitude of the spacecraft, after having performed the detumbling after the insertion into orbit. The On-Board Computer (OBC) manages the operations onboard and distributes commands among the different subsystems, while also collecting the telemetry produced by the spacecraft. The payload is constituted by the camera, that produces the mission data, and a processing unit, that process the data with SRR algorithm. The structure hosts all subsystems, and the mechanism deploys the deployable UHF antenna.

The interfaces among subsystems are represented in the N2 diagram in Figure 14.

The interfaces expected in the design are:

- One CAN bus as data interface to distribute commands and housekeeping;
- One MLVDS bus as data interface to manage mission data;
- One unregulated bus as power interface between batteries and solar panels;
- One 3.3V bus as power interface to ADCS, COMMSYS (UHF band equipment), OBC and payload;
- One 5V bus as power interface to OBC, ADCS, payload;
- One 12V bus as power interface to COMMSYS (S band equipment).

The physical block diagram of the system is shown in Figure 15. The main components are:

- OBC
  - Processing Unit, that includes CPU, clock, and memories;
  - Sensors and their logic unit, that includes ADCs, MUX and amplifiers;
  - Interface elements.
- ADCS:
  - Processing Unit, that includes CPU, clock, and memories;
  - Sensors for attitude determination: four sun sensors, one IMU, one triaxial magnetometer;
  - Actuators for attitude control: three reaction wheels and three magnetic torques rods, one for each axis;
  - Interface elements.
- COMMSYS:
  - UHF band board, that includes radio and modem;
  - UHF deployable antenna (connected to the deployment mechanism);
  - S band board, that includes radio and modem;
  - S patch antenna;
  - Interface elements.
- EPS:
  - Four solar panels;
  - Battery packs;
  - Two load switches;
  - Protection circuits;
  - Power converters;
  - Interface elements.
- Payload:
  - Processing Unit, that includes CPU, clock, and memories;

- ○ RGB camera;
- ○ Interface elements.

This system architecture is well known and easy to implement, and it can be a good solution for commercial CubeSats' developers that use highly reliable, well tested and space rated hardware.

However, it is not ideal for an educational mission, because it provides little protection against failures, as the malfunction of a single piece of hardware can easily cause the loss of the functionality of an entire subsystem. That would most likely result in the loss of the mission since every function is allocated to a single subsystem.

That means that a more reliable alternative architecture should be considered.

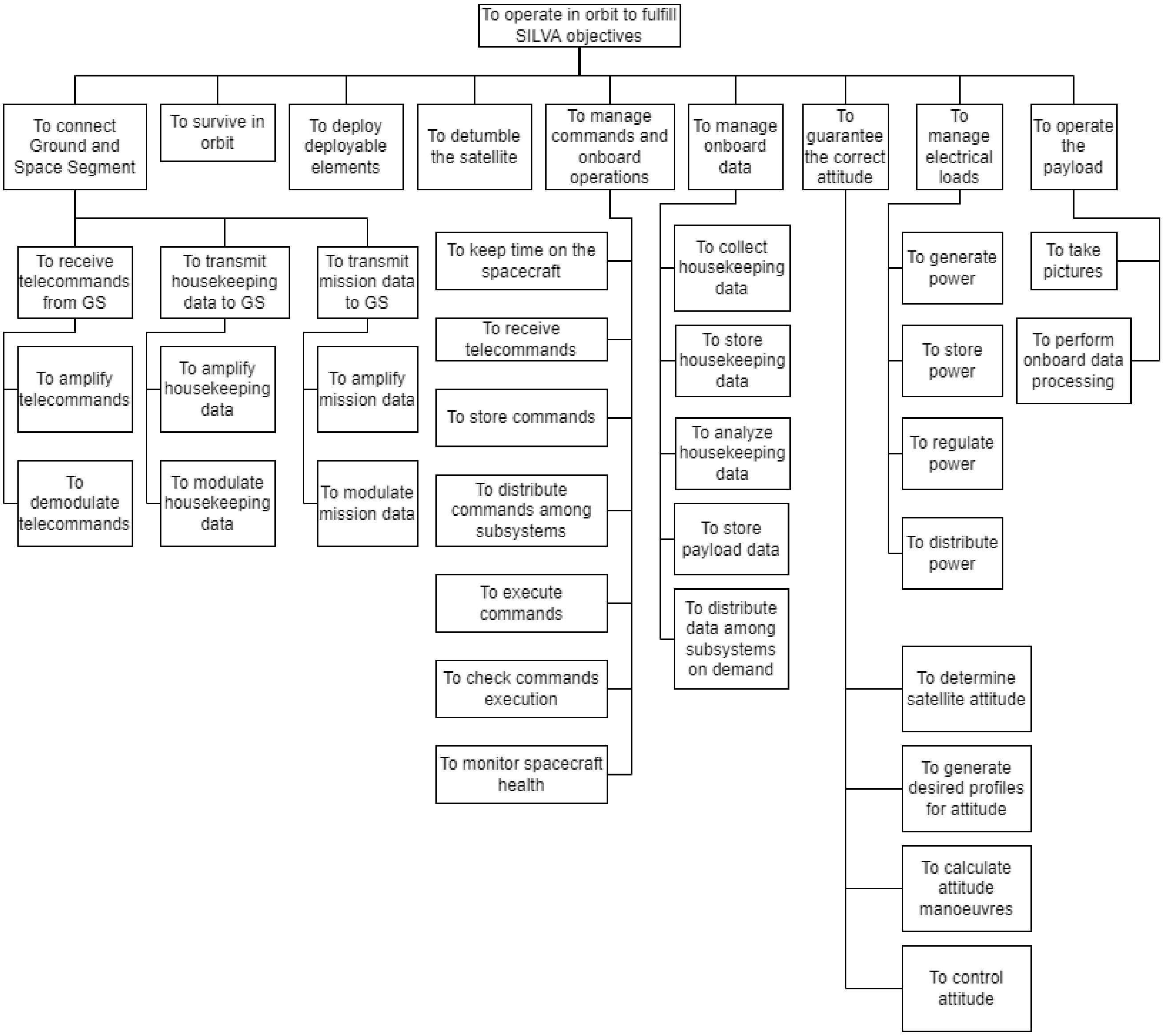

To operate in orbit to fulfill SILVA objectives
To connect Ground and Space Segment
To survive in orbit
To deploy deployable elements
To detumble the satellite
To manage commands and onboard operations
To manage onboard data
To guarantee the correct attitude
To manage electrical loads
To operate the payload
To receive telecommands from GS
To transmit housekeeping data to GS
To transmit mission data to GS
To amplify telecommands
To demodulate telecommands
To amplify housekeeping data
To modulate housekeeping data
To amplify mission data
To modulate mission data
To keep time on the spacecraft
To receive telecommands
To store commands
To distribute commands among subsystems
To execute commands
To check commands execution
To monitor spacecraft health
To collect housekeeping data
To store housekeeping data
To analyze housekeeping data
To store payload data
To distribute data among subsystems on demand
To generate power
To store power
To regulate power
To distribute power
To take pictures
To perform onboard data processing
To determine satellite attitude
To generate desired profiles for attitude
To calculate attitude manoeuvres
To control attitude

Figure 12 CubeSat's Functional Tree

Table 4 CubeSat's Function/Equipment Matrix

	COMMSYS	ADCS	OBC	EPS	Payload	Structure	TCS	Mechanisms
Connect Ground and Space Segment	x							
Survive in orbit						x	x	
Deploy deployable elements								x
Detumble satellite		x						
Manage commands and onboard operations			x					
Manage onboard data			x					
Guarantee correct attitude		x						
Manage electrical loads				x				
Operate the payload					x			

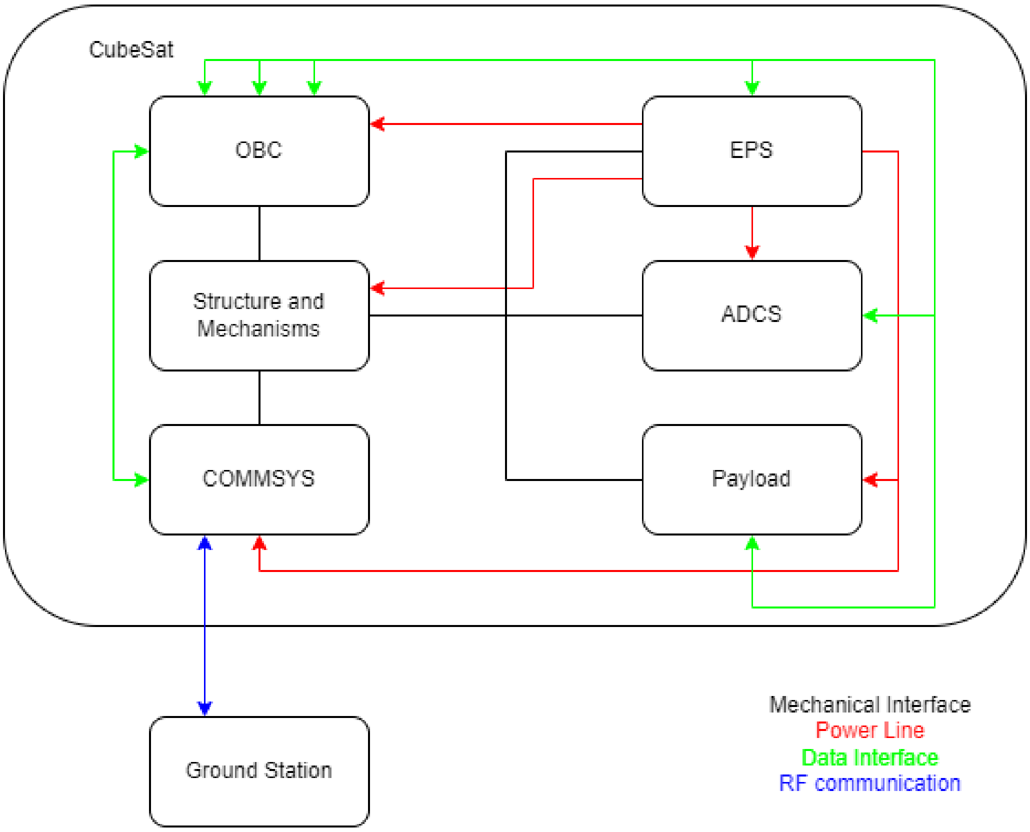
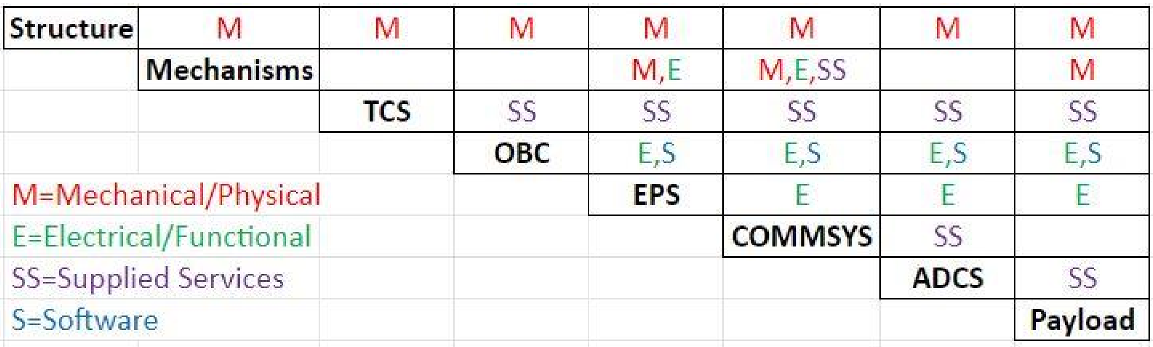


Figure 13 CubeSat's Functional Block Diagram



Structure	M	M	M	M	M	M	M
	Mechanisms			M,E	M,E,SS		M
		TCS	SS	SS	SS	SS	SS
			OBC	E,S	E,S	E,S	E,S
M=Mechanical/Physical				**EPS**	E	E	E
E=Electrical/Functional					**COMMSYS**	SS	
SS=Supplied Services						**ADCS**	SS
S=Software							**Payload**

Figure 14 SILVA N2 Diagram

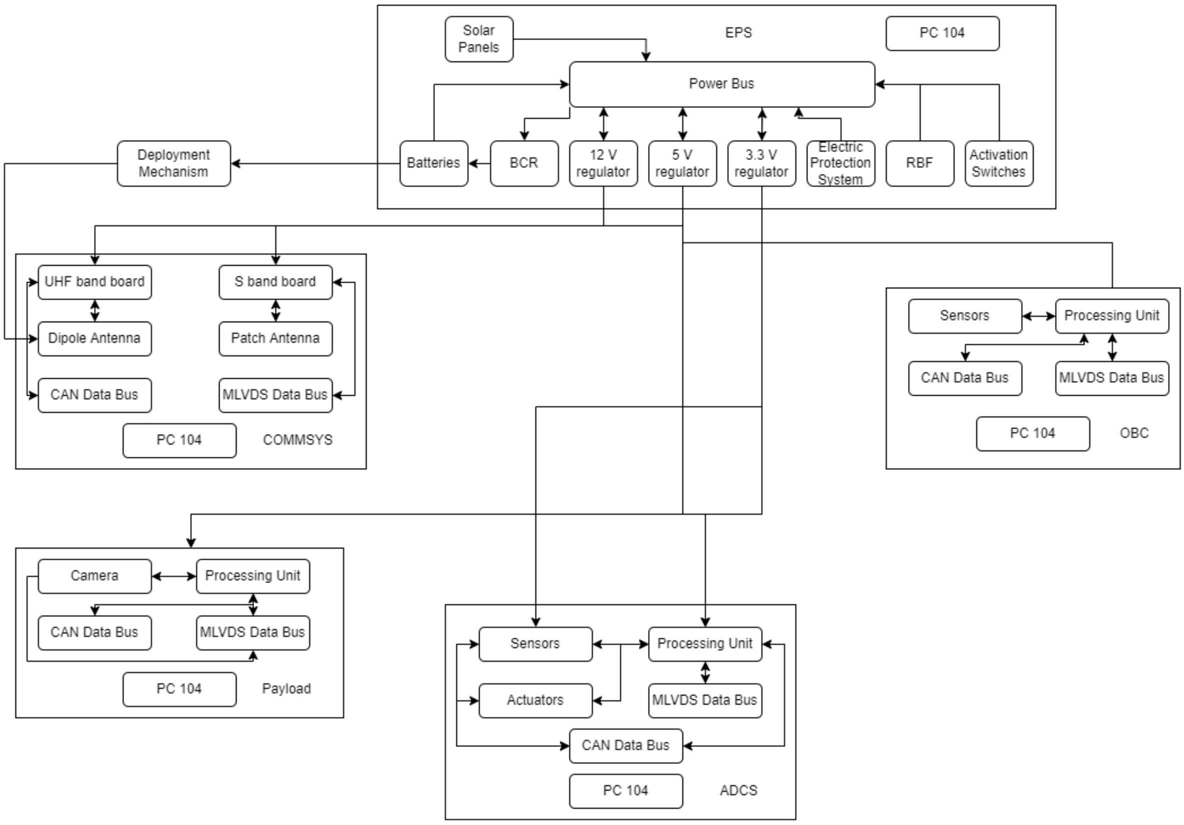


Figure 15 SILVA Physical Block Diagram

5 Dependable CubeSat’s Design

5.1 FMEA Analysis and Critical Functions

The first step to design a system by a dependable approach is to precisely define what criteria need to be met to consider the mission successful. That allows to establish which functionalities of the system have high priority and must be guaranteed.

The SILVA mission is considered successful if its mission objectives are fulfilled. The main SILVA mission objective is to study the vegetation status and changes over time; however, since it is also an educational project, it can be considered partially successful even if it does not provide the expected scientific results but still represents a meaningful learning experience for the students involved. If students can learn how to design and operate a CubeSat which can perform at least the basic functions of a working spacecraft, the educational goal of the mission is reached.

The success criteria for SILVA are summarized in Table 5.

- SILVA is considered a complete success if the CubeSat provides good enough mission data for its whole design life. Onboard operations are executed without major failures permanently damaging any of the subsystems. All basic functions are preserved. Both the educational and the scientific mission objectives are considered satisfied.
- SILVA is considered a good success if the CubeSat provides good enough mission data only for a part of its design life. However, the interruption of service involves only the payload, and the spacecraft keeps executing other onboard operations for its whole design life. Both the educational and the scientific mission objectives are considered satisfied.
- SILVA is considered somehow a success even if the CubeSat is never able to produce mission data. The CubeSat executes its basic operations without major failures for its design life, and the educational mission objective is still considered satisfied. As mission data are not collected, the scientific mission objective is not fulfilled.
- SILVA is considered somehow a failure if the CubeSat never produces mission data, and it performs its basic operations only for a part of its design life. The educational mission objective is considered partially satisfied, as the launch and the first period of operations are successfully experienced by students.
- SILVA is considered a complete failure if it is inoperative for its whole design life, and it is never established a contact with the spacecraft after launch. The educational mission objective is not fulfilled, as the students do not experience a successful launch and operation phase.

Table 5 Mission Success Criteria

Spacecraft Operativity Status	**Mission results**	**Mission Success**
Nominal Status	• Payload data are collected, processed	100%

	and transmitted to ground as expected for entire design life; • Spacecraft functions are all performed as expected for entire design life; • Failures happen, but they do not cause a significant lack of availability and they are effectively recovered.	
Reduced Nominal Status	• Payload data are collected, processed and transmitted to ground as expected for a fraction of design life; • Spacecraft functions are all performed as expected for entire design life; • Failures happen, but they do not cause a significant lack of availability and they are effectively recovered.	75%
Housekeeping Status	• Payload data are never collected, processed, and transmitted to ground; • Spacecraft functions are all performed as expected for entire design life; • Failures happen, but they do not cause a significant lack of availability and they are effectively recovered.	50%
Reduced Housekeeping Status	• Payload data are never collected, processed, and transmitted to ground;	25%

	• Spacecraft main functions are performed in a degraded way for a fraction of design life; • Failures happen, but they are effectively recovered.	
Dead on arrival	• First contact with spacecraft never happens; • Spacecraft does not perform its functions for a relevant amount of time; • Catastrophic failures are not recovered.	0%

After having defined the success criteria of the mission, a FMEA analysis can be initiated to evaluate the effects that different failures have on the overall mission. That helps identifying the critical functions that need to be guaranteed to increase the possibility of having a successful mission. The SILVA's FMEA is available in Chapter 8.

It is important to underline that the severity numbers are associated with the system failures following a different logic than that prescribed by Table 2. Since there are not safety issues involved in a CubeSat mission (especially if it is not foreseen that the CubeSat will be released into space from the International Space Station), to be rigorous the failures could be classified only as "major" and "minor". However, using only two severity levels does not allow to effectively describe the failure propagation dynamics. So, the severity levels were associated to failures as follows:

- A failure is considered catastrophic if it causes the loss of the mission, meaning it is no longer possible to operate the spacecraft.
- A failure is considered critical if it causes the degradation of the mission results, meaning the spacecraft performances are severely reduced or it is no longer possible to produce mission data.
- A failure is considered major if it reduces the performances of the spacecraft.
- A failure is considered minor if its effects are negligible or temporary.

In an educational context it is more convenient to execute a FMEA instead of a FMECA because the probability of failures of COTS components are generally not known. At system level, the probability of failure can be estimated based on experience. The analysis is carried out without considering the effects that mitigation strategies could have on the system.

The critical functions for SILVA identified through the FMEA are:

1. Detumble the CubeSat;
2. Communicate with Ground Segment;
3. Manage onboard operations;
4. Manage onboard data;
5. Generate power;
6. Distribute power;
7. Determine attitude;
8. Control attitude;
9. Take images;
10. Process images onboard.

The first six functions are essential to guarantee the spacecraft survival, while the loss of the attitude determination and control and payload functionalities would severely degrade the quality of collected mission data and thus the mission success.

The probability of losing a critical function was estimated by experience and by considering the procurement source of the hardware involved.

- A completely new ADCS is developed in house by students, and it needs a complete validation campaign. Therefore, it is considered probable failures might happen (PN = 4).
- COMMSYS is constituted by two radio equipment, the first one in the UHF frequency band, the other one in the S frequency band. The S equipment is bought by professional developers; thus, it is considered more reliable than hardware developed by students. The UHF radio has been developed in house, but it has been extensively validated in other missions and it is proved to be very reliable. Therefore, the probability that the COMMSYS fails is considered remote (PN = 2).
- OBC and its software is developed in house, thus it is considered prone to failures (PN = 4).
- EPS is designed by professionals, and it is considered quite reliable after an accurate validation campaign (PN = 2).
- While the RGB camera will be a commercial component (PN = 2), the payload processing unit is developed in house by students. Therefore, the probability of failure is considered quite high (PN =4).

Table 6 summarizes SILVA critical functions. The failures that need to be addressed with the highest priority are those that may affect the ADCS, OBC, and payload processing unit.

Table 6 SILVA Critical Functions Risk Evaluation – basic system

	Subsystem	**Severity level**	**SN**	**PN**	**CN**	**Risk Assessment**
Detumble the CubeSat	ADCS	Catastrophic	4	4	16	Severe - Avoid
Communication with Ground Segment	COMMSYS	Catastrophic	4	2	8	Major - Mitigate

Manage onboard operations	OBC	Catastrophic	4	4	16	Severe - Avoid
Manage onboard data	OBC	Catastrophic	4	4	16	Severe - Avoid
Generate power	EPS	Catastrophic	4	2	8	Major - Mitigate
Distribute power	EPS	Catastrophic	4	2	8	Major - Mitigate
Determine attitude	ADCS	Critical	3	4	12	Severe – Avoid
Control attitude	ADCS	Critical	3	4	12	Severe – Avoid
Take images	Payload - Sensor	Critical	3	2	6	Moderate - Allow
Process images onboard	Payload – Processing Unit	Critical	3	4	12	Severe - Avoid

5.2 Fault Tree Analysis

The Fault Tree analysis is carried out by drawing a Fault Tree for the undesired events that result in the impossibility of perform the system critical functions. The purpose is to identify the basic events that can cause a significant failure in the system.

- Figure 16 analyzes the undesired event "OBC does not distribute commands at the right time". If this failure happened, the system would not be able to manage the onboard operations, and it would be impossible to operate the spacecraft. The main causes that might lead to this failure are:
    - A faulty processing unit;
    - A faulty CAN data bus;
    - Loss of synchronization among the different onboard operations.

  While the synchronization issue can be easily managed by a careful software design and by an extensive verification campaign, the CAN bus and the processing units are both single points of failure. Data corruption by radiations' effects is a significant threat to onboard operations that needs to be addressed.
- Figure 17 shows the FT for the undesired event "Data are not collected", meaning that the OBC cannot manage the spacecraft telemetry and mission data. The main causes are:
    - A faulty signal formatting and processing unit;
    - A faulty CAN data bus;
    - A faulty MLVDS data bus.

  All of them are single points of failures.
- Figure 18 analyzes the "No communication with ground station" failure, which would make impossible to operate the spacecraft and know its status. There are two separate

communication lines, both can be used to transmit housekeeping telemetry to ground and to receive commands from ground. Mission data can be transmitted only through the S frequency band communication line, so the S radio equipment is a single point of failure for this function. Another weak point is the deployable UHF antenna, which would make unusable the UHF communication line if it were not correctly deployed.

- Figure 19 analyzes the "ADCS does not detumble the satellite" undesired event. If this failure verified, the CubeSat would be lost at the very beginning of the mission, and it would not even start to operate. The main causes of this event are:
    - A faulty magnetometer;
    - A faulty processing unit;
    - A faulty magnetic torque rod.

  Even though all of them are single point of failure, it is quite rare that a magnetometer or a magnetic rod fails; thus, the main threat to the fulfillment of this function is a failure in the processing unit.

- Figure 20 analyzes the "ADCS does not determine attitude" failure. This failure would make impossible to know the CubeSat attitude and then to obtain the desired one, greatly affecting the quality of the pictures taken by the payload and the effectiveness of the communications with ground. The main causes of this failure are:
    - A faulty processing unit;
    - A faulty IMU;
    - A faulty magnetometer;
    - The loss of three sun sensors.

  Once again, the most critical single point of failure is the processing unit. The quality of the data used in the calculations is a sensitive aspect, as the algorithms may not converge if corrupted data is used or if data is used at the wrong time. Thus, it is important to guarantee a proper synchronization in the data stream, that should also be as faulty free as possible.

- Figure 21 shows the FT for the "ADCS does not control attitude" undesired event. The main causes of this event are:
    - A faulty processing unit;
    - A faulty magnetic torque rod;
    - The loss of a reaction wheel.

  The significant single point of failure is a malfunction in the processing unit. The quality of the data used in the calculations is a sensitive aspect, as the algorithms may not converge if corrupted data is used or if data is used at the wrong time. Thus, it is important to guarantee a proper synchronization in the data stream, that should also be as faulty free as possible. While the failure of a magnetic torque rod is quite rare, the reaction wheels' pack is a significant single point of failure.

- Figure 22 analyzes the "Mission data are not collected" undesired event, that would lead to the complete failure of the scientific objective of the mission. Both the camera and the processing unit are single points of failure. Data corruption may degrade the quality of mission data.

- Figure 23 shows the “Battery does not recharge” failure, that would lead the spacecraft to not be able to store the newly generated power. The causes of such events are:
    - Battery malfunction or degradation;
    - Loss of all solar panels;
    - Faulty Battery Charge Regulator circuit;
    - Malfunction of protective and load switches.

  There are several points of failure, but the most critical ones are the single battery pack and recharging line.

- Figure 24 analyzes the “EPS does not distribute power” failure. In this case, each power bus is a single point of failures for the power distribution to the hardware connected to that bus. It is particularly important to preserve the functionality of the protective circuits.

Based on the FTA, it is possible to identify single points of failure that might cause more than one failure. ADCS, OBC and payload would all stop providing their service if their respective processing units experienced a failure. Many functions are sensitive to errors in the data stored on-board, and the synchronization among different operations is crucial to assure the correctness of the on-board calculations. Furthermore, reliable and robust data interface would benefit all the subsystems, as well as electrical protection circuits on a local level. Lastly, the entire generation of power is dependent to a single generation line.

Elaborating mitigation strategies that act upon these issues would decrease the system probability of failure.

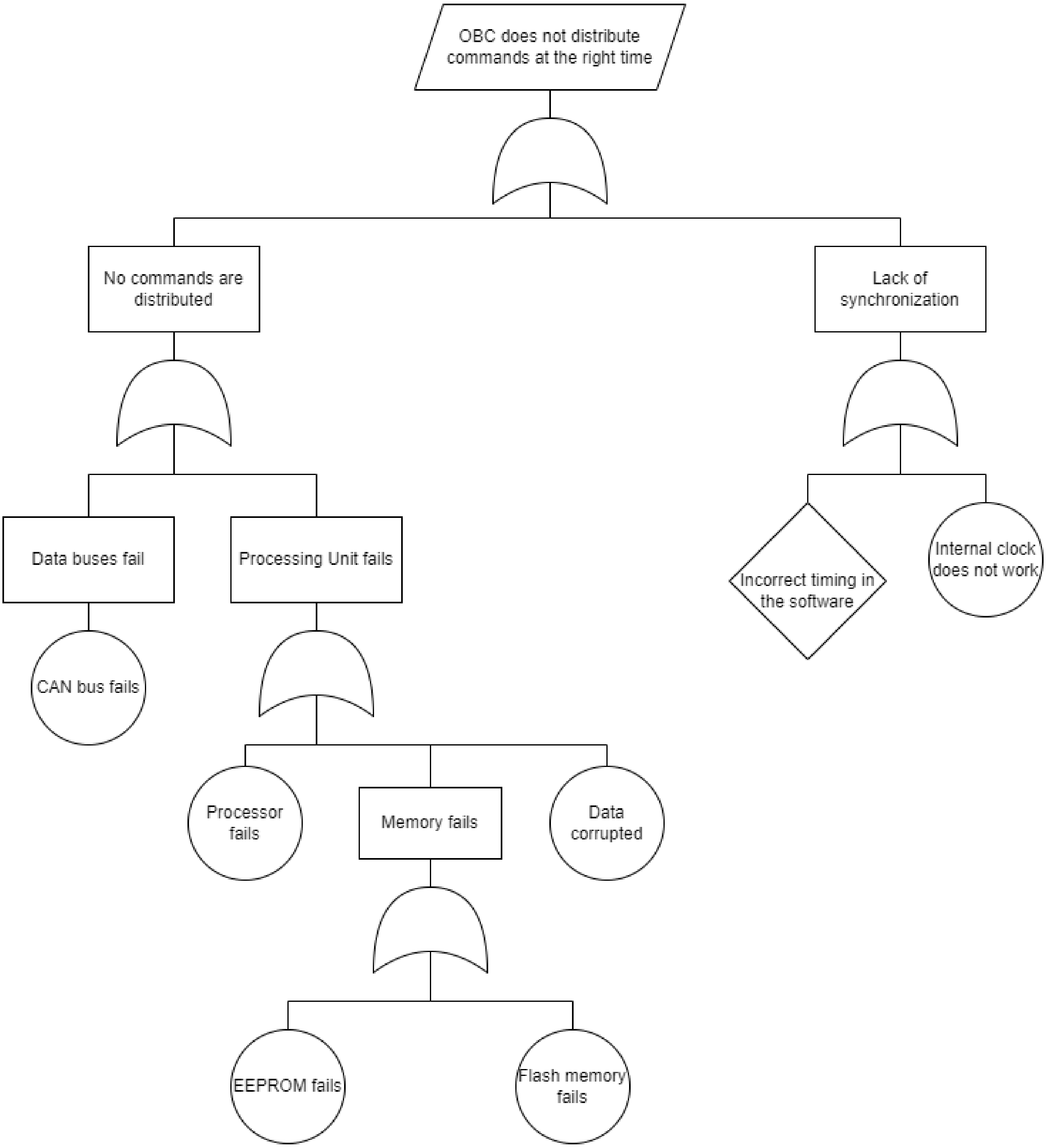


Figure 16 FTA - OBC – Commands and onboard operations management – basic system

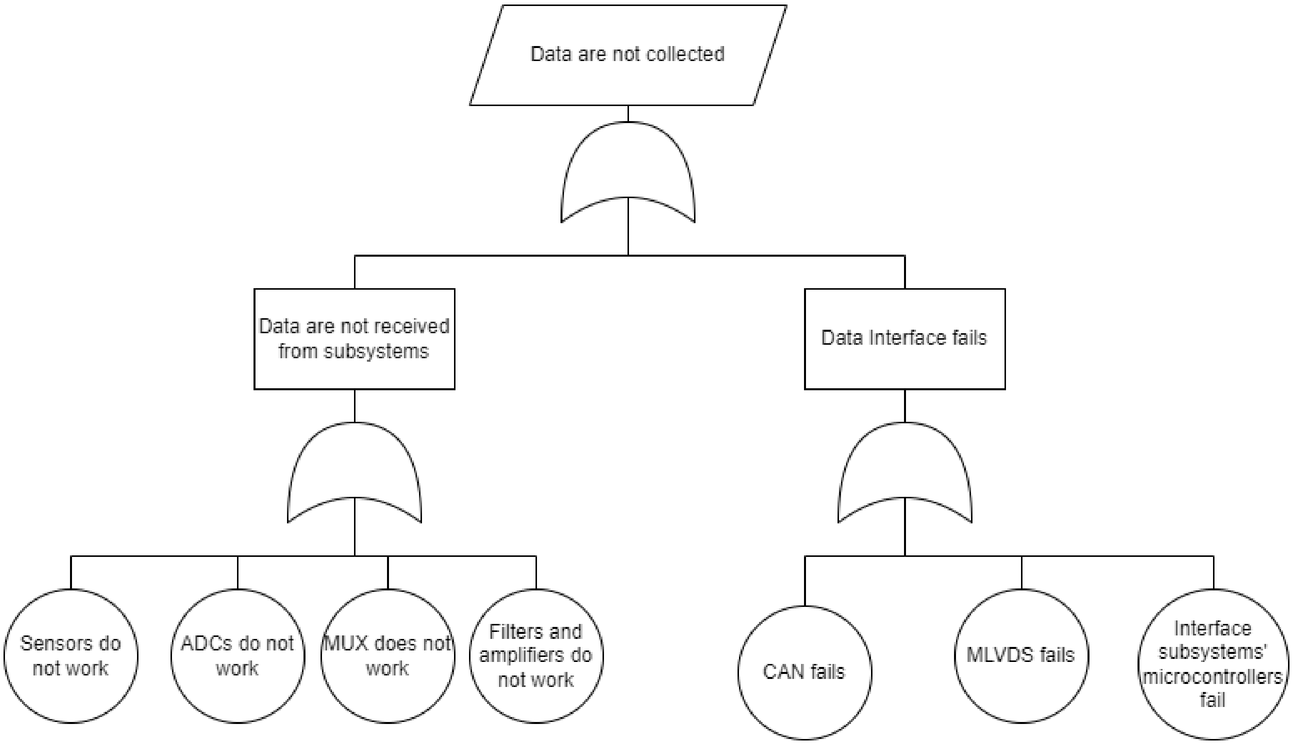

Data are not collected
Data are not received from subsystems
Data Interface fails
Sensors do not work
ADCs do not work
MUX does not work
Filters and amplifiers do not work
CAN fails
MLVDS fails
Interface subsystems' microcontrollers fail

Figure 17 FTA - OBC - Onboard data management – basic system

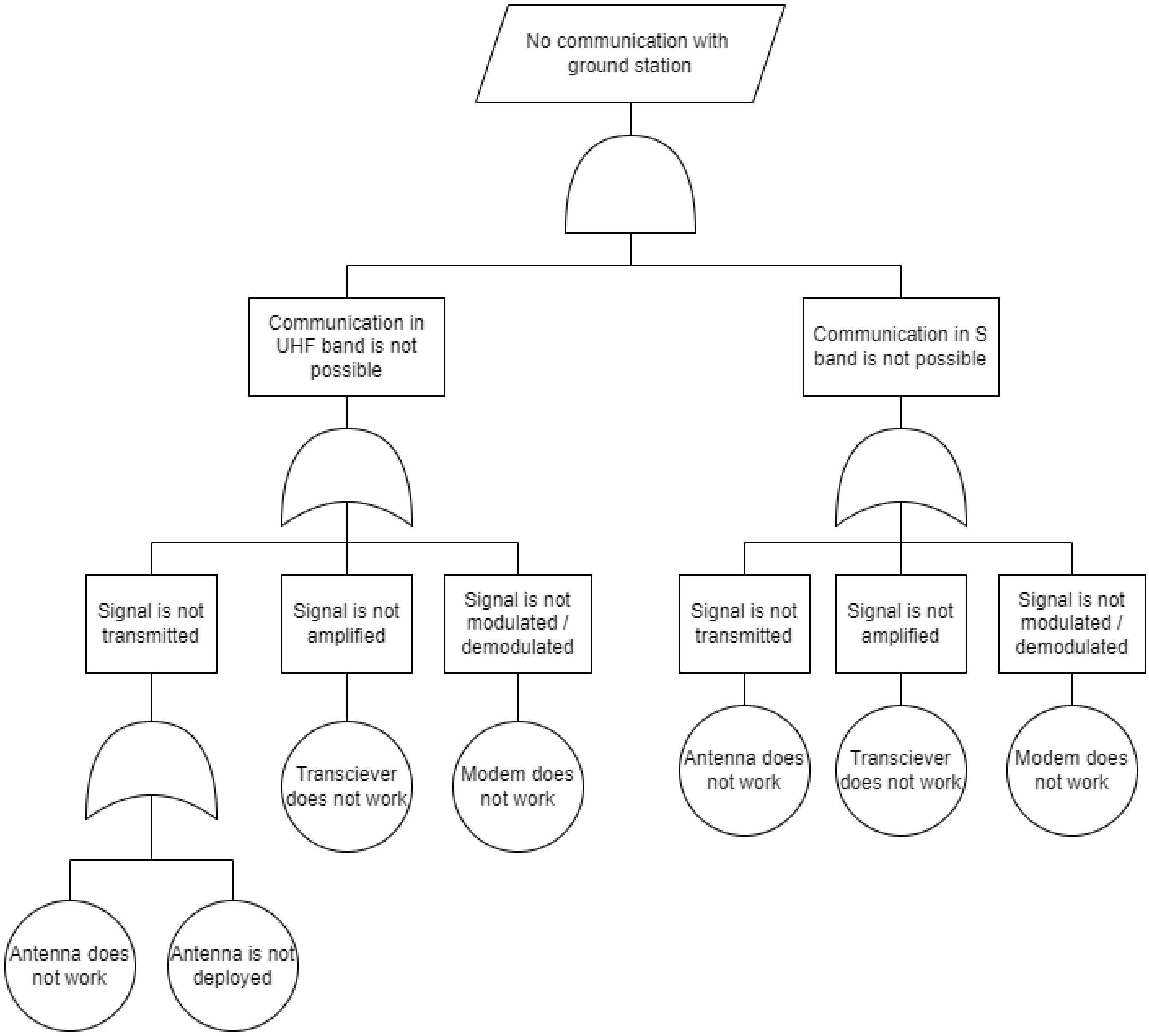

No communication with ground station
Communication in UHF band is not possible
Communication in S band is not possible
Signal is not transmitted
Signal is not amplified
Signal is not modulated / demodulated
Signal is not transmitted
Signal is not amplified
Signal is not modulated / demodulated
Transciever does not work
Modem does not work
Antenna does not work
Transciever does not work
Modem does not work
Antenna does not work
Antenna is not deployed

Figure 18 FTA - COMMSYS - Communication with ground – basic system

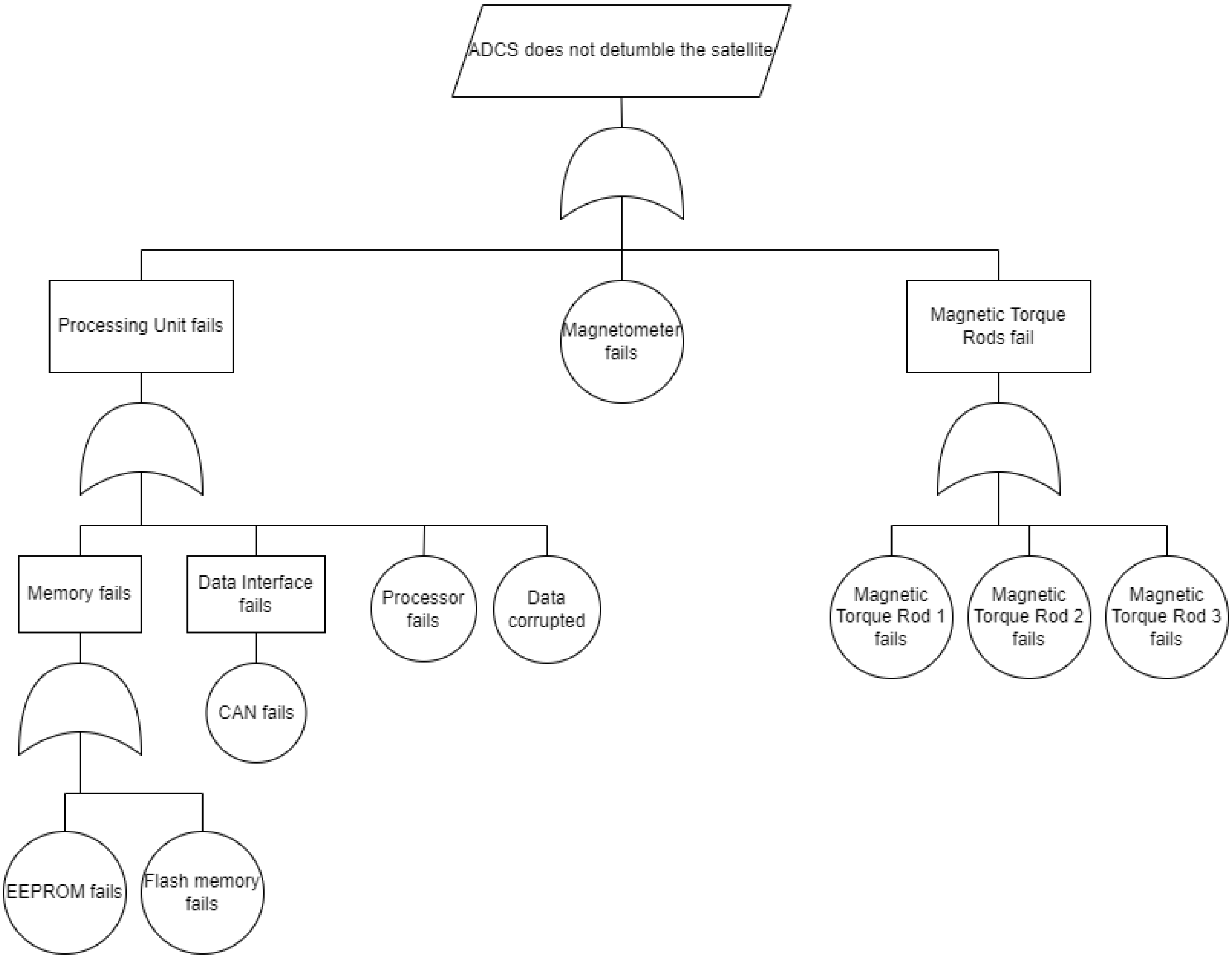

ADCS does not detumble the satellite
Processing Unit fails
Magnetometer fails
Magnetic Torque Rods fail
Memory fails
Data Interface fails
Processor fails
Data corrupted
CAN fails
EEPROM fails
Flash memory fails
Magnetic Torque Rod 1 fails
Magnetic Torque Rod 2 fails
Magnetic Torque Rod 3 fails

Figure 19 FTA - ADCS - Detumbling - basic system

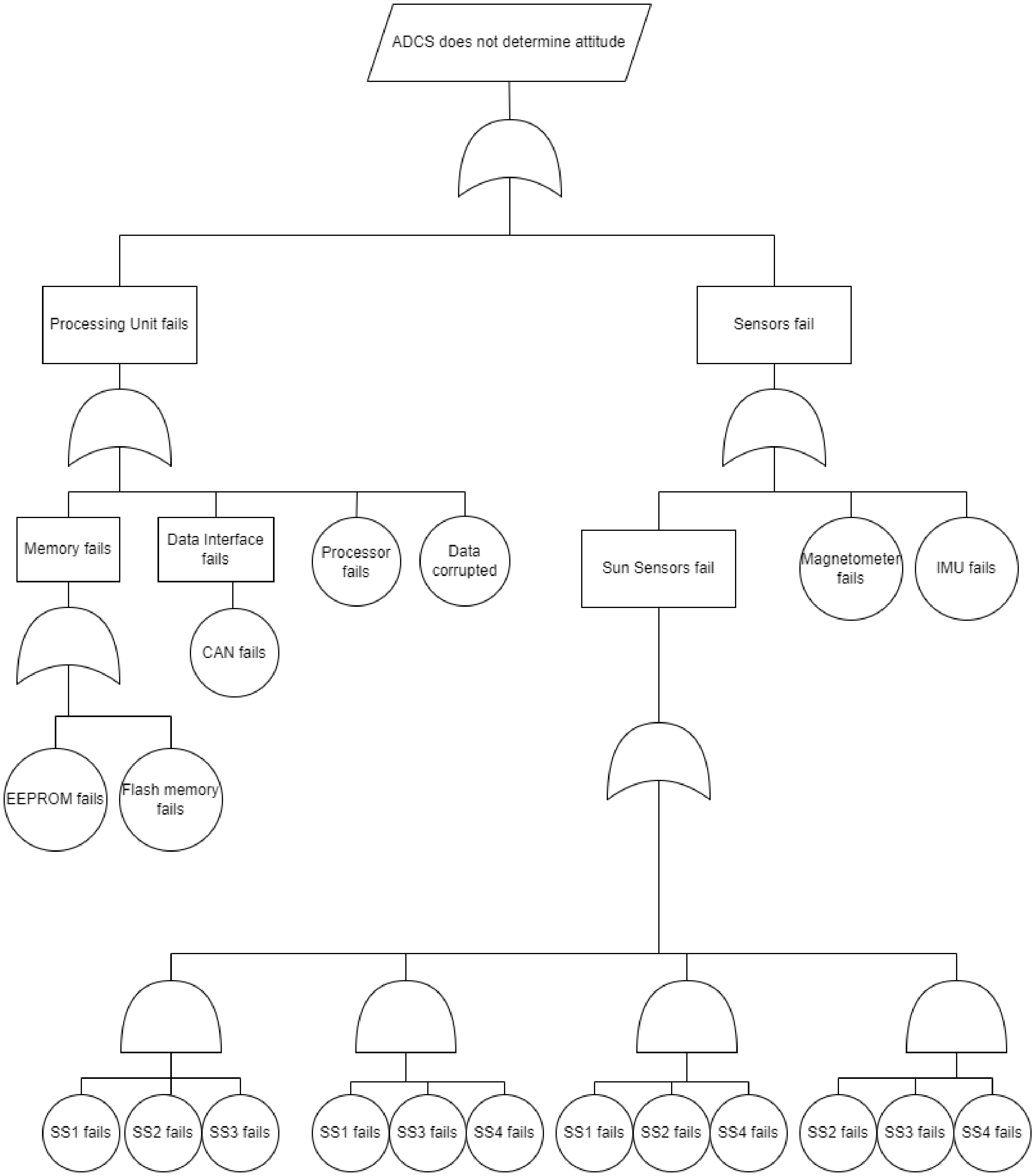


Figure 20 - FTA - ADCS - Determination - basic system

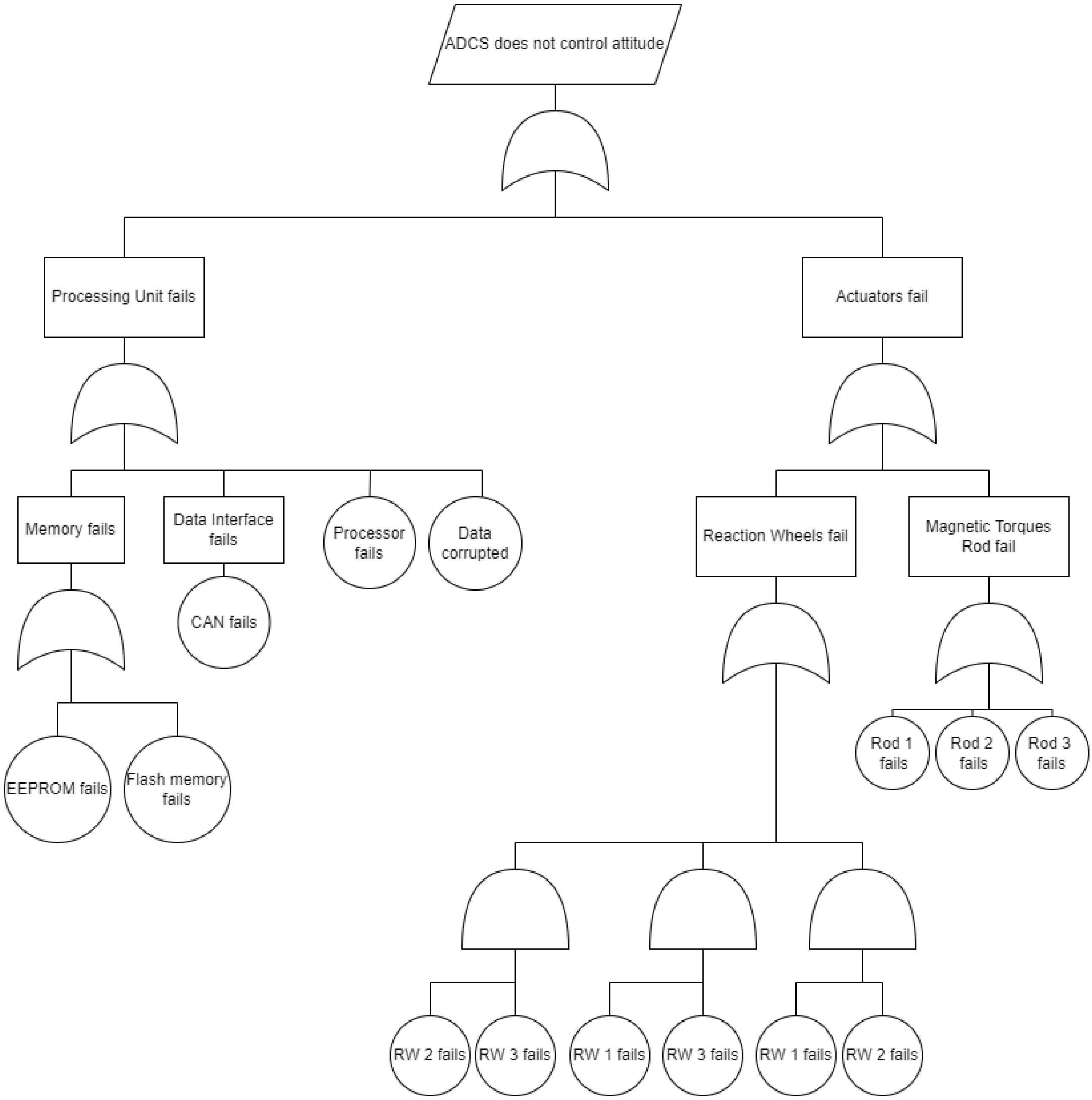


Figure 21 FTA - ADCS - Control - basic system

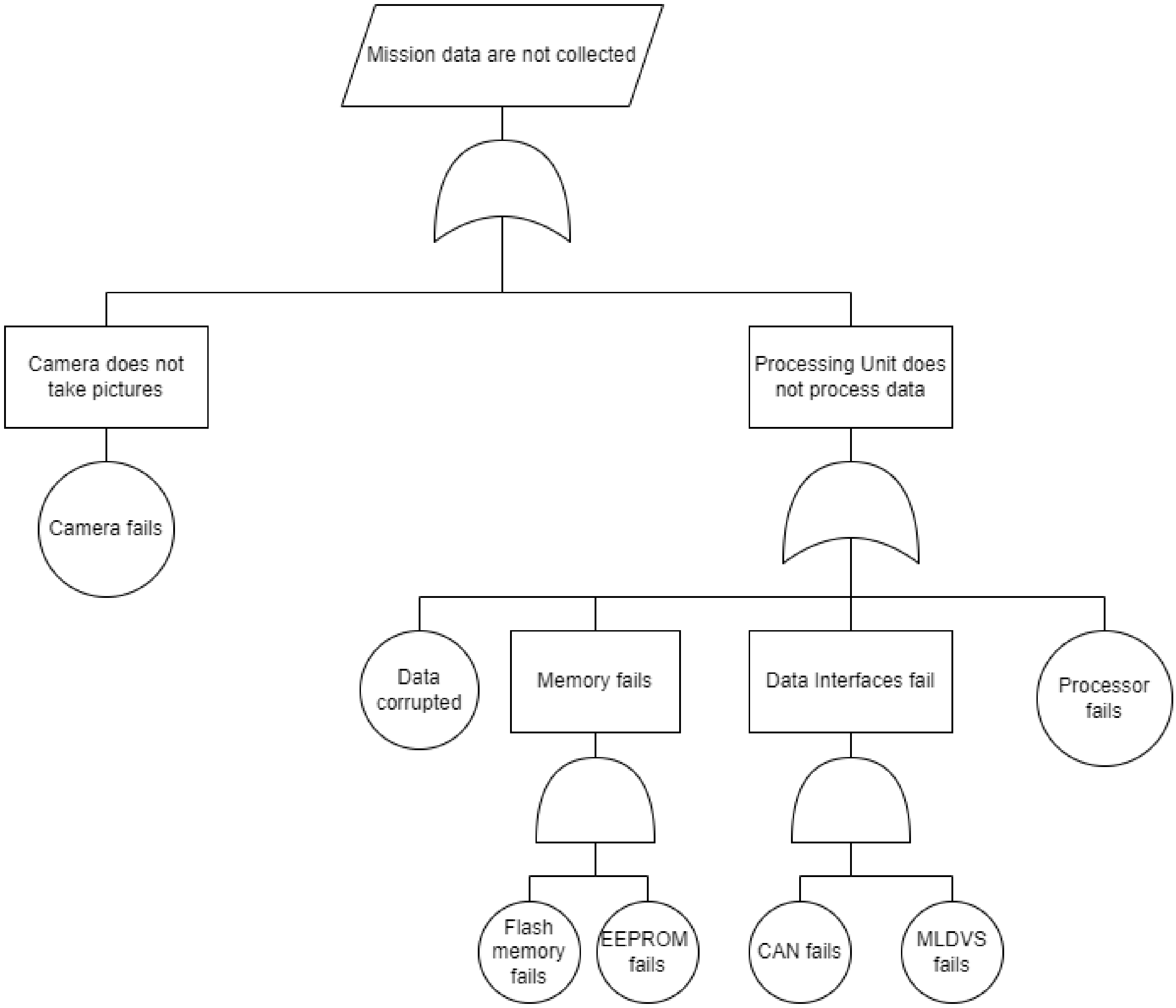


Figure 22 FTA - Payload - Collect and process mission data – basic system

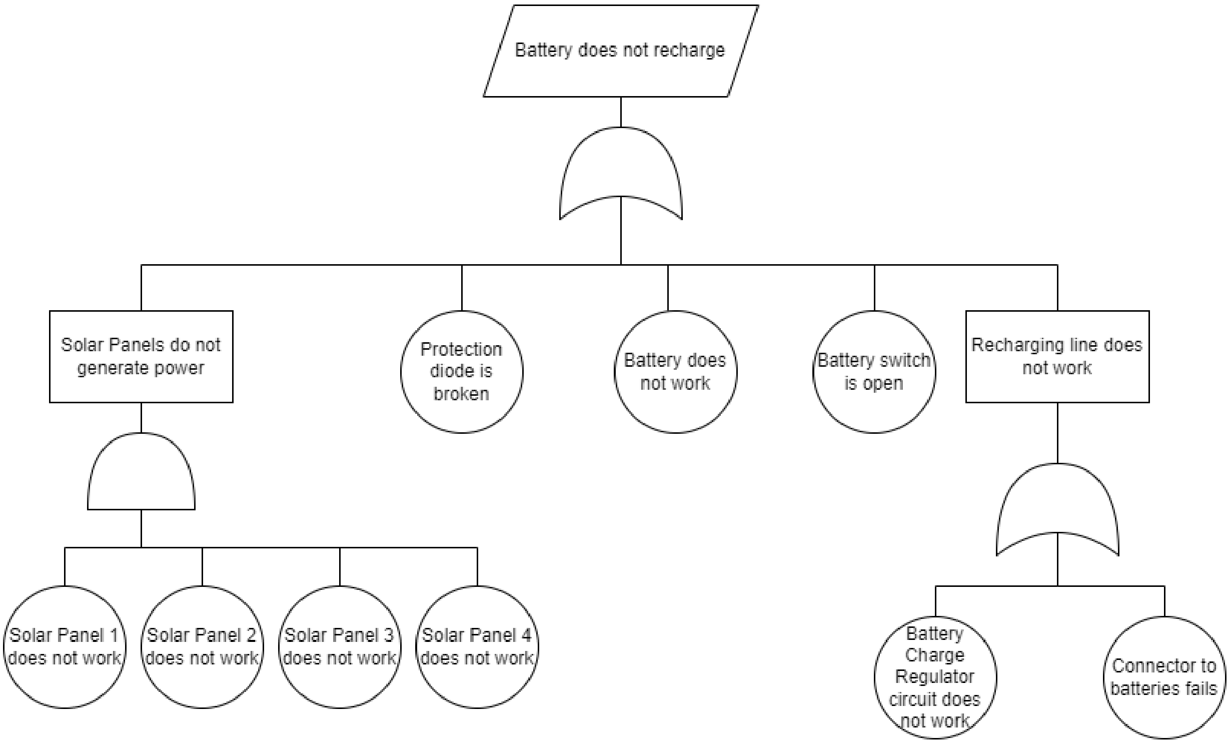

Battery does not recharge
Solar Panels do not generate power
Protection diode is broken
Battery does not work
Battery switch is open
Recharging line does not work
Solar Panel 1 does not work
Solar Panel 2 does not work
Solar Panel 3 does not work
Solar Panel 4 does not work
Battery Charge Regulator circuit does not work
Connector to batteries fails

Figure 23 FTA - EPS - Power Generation and Batteries recharge – basic system

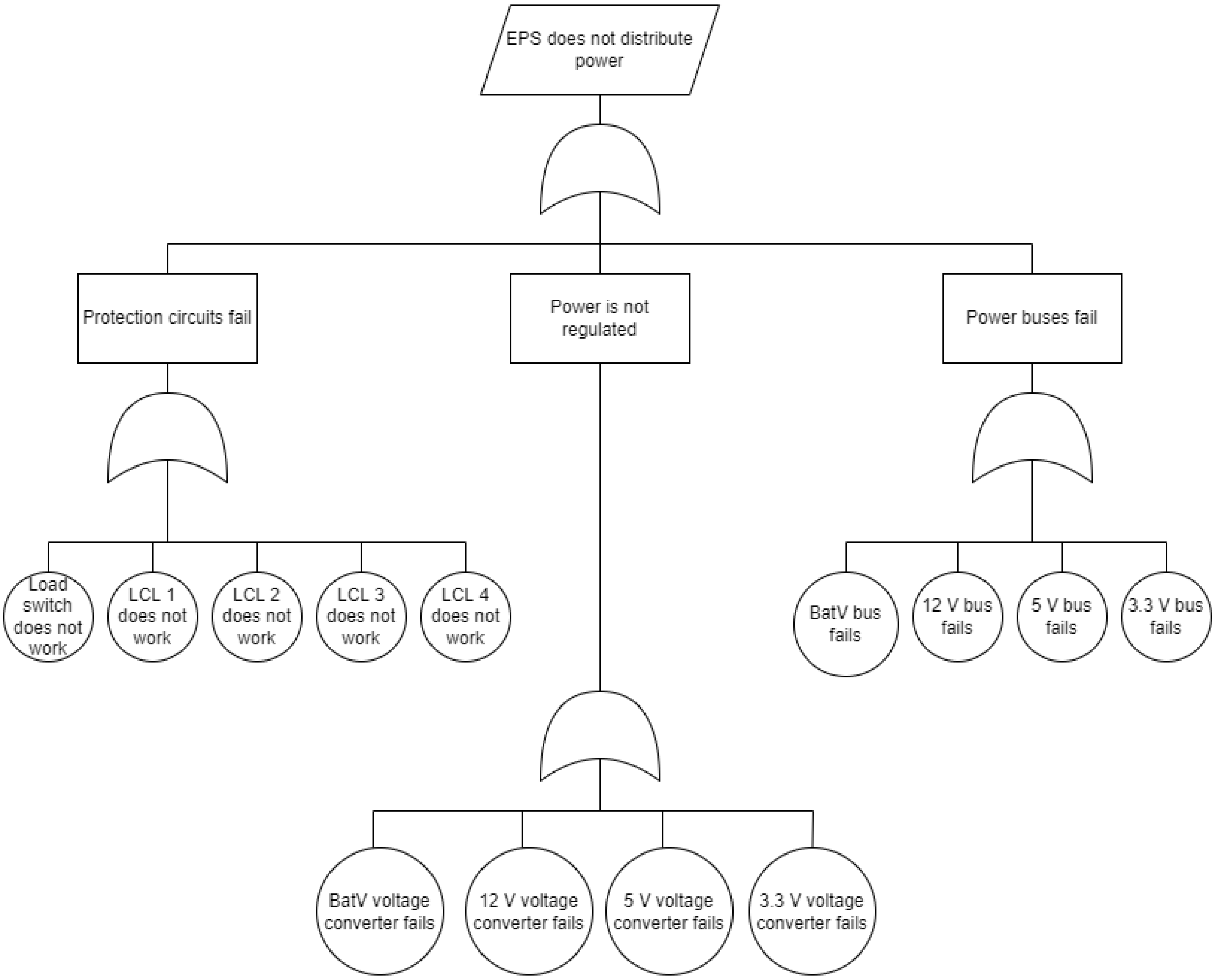


Figure 24 FTA - EPS - Power Distribution - basic system

5.3 Reliability Block Diagrams

Another method to model the system behaviour and identify critical components are the Reliability Block Diagrams.

- Figure 25 shows that the OBC functionality can be modelled as a series of components included in the processing unit and the data interfaces. If one of these components fail, OBC cannot complete its tasks.
- Figure 26 shows the ADCS functioning structure to perform detumbling. All the components involved in the function execution are single points of failure; therefore, the subsystem can be modelled as a series regarding the detumbling.
- Figure 27 shows the ADCS model to perform attitude determination. IMU, magnetometer, and processing unit are single points of failure, thus they are put in series. Out of the four sun sensors available, two are essential to allow the attitude determination. That can be expressed by a parallel network, where each branch represents a combination of sensors that would still allow the ADCS to complete this function.
- Figure 28 shows the ADCS model to attitude control. Since the processing units and the actuators are all required to perform this function, they can be modelled as a series network.
- Figure 29 shows the COMMSYS model. There are two separate lines that can be used to communicate with ground, thus they can be represented as a parallel network.
- Figure 30 shows the EPS model for the power generation function. Solar panels constitute a parallel network as theoretically the power generation function could be completed just by one panel. However, that would greatly decrease the amount of power generated and the operations that is possible to perform onboard; thus, it is considered that at least two solar panels should be functioning to consider this function fulfilled. Other components are single points of failure, so they are inserted as a series.
- Figure 31 shows the distribution unit of the EPS, that is modelled as a series of all the components required.
- Figure 32 shows the payload architecture, that is modelled as a series of the sensing instrument and the processing unit.

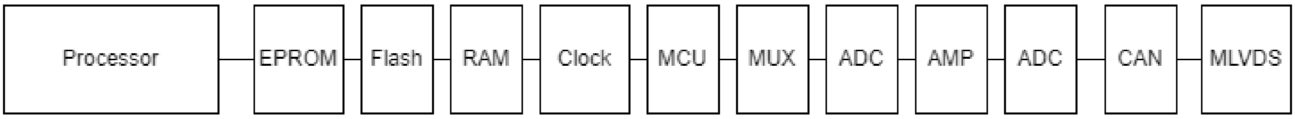


Figure 25 RBD - OBC - Commands distribution and data management - basic system

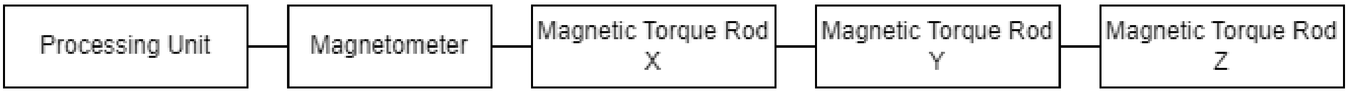


Figure 26 RBD - ADCS - Detumbling - basic system

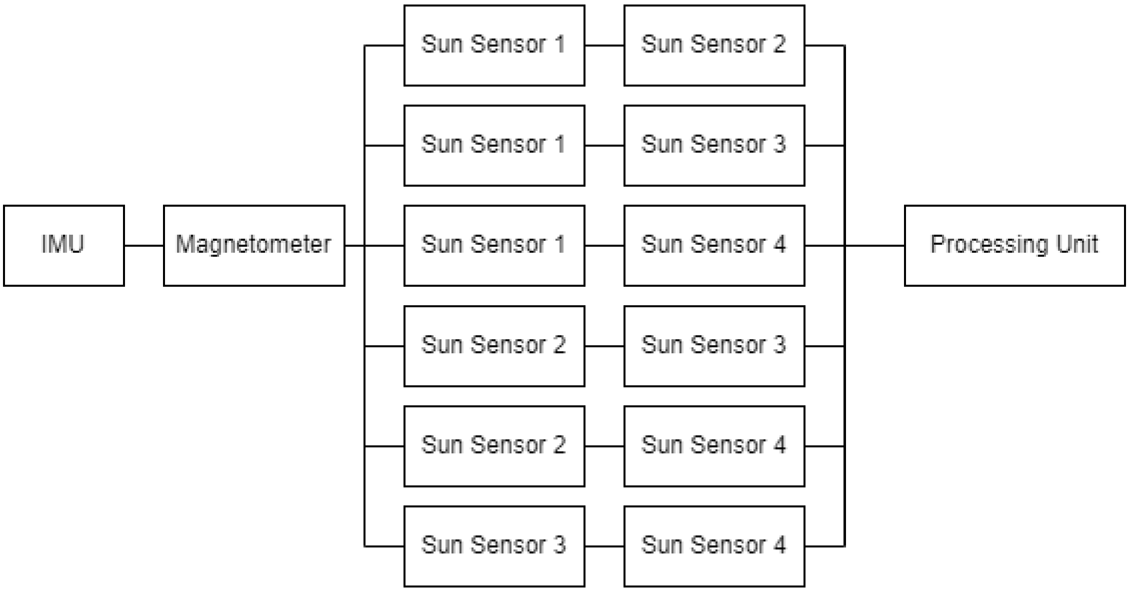


Figure 27 RBD - ADCS - Attitude Determination - basic system

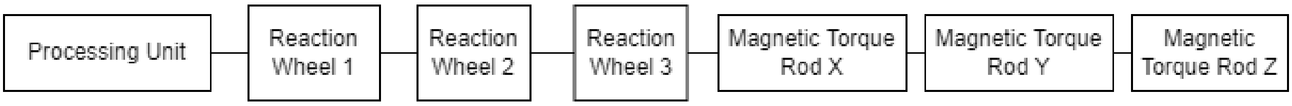


Figure 28 RDB - ADCS - Attitude Control - basic system

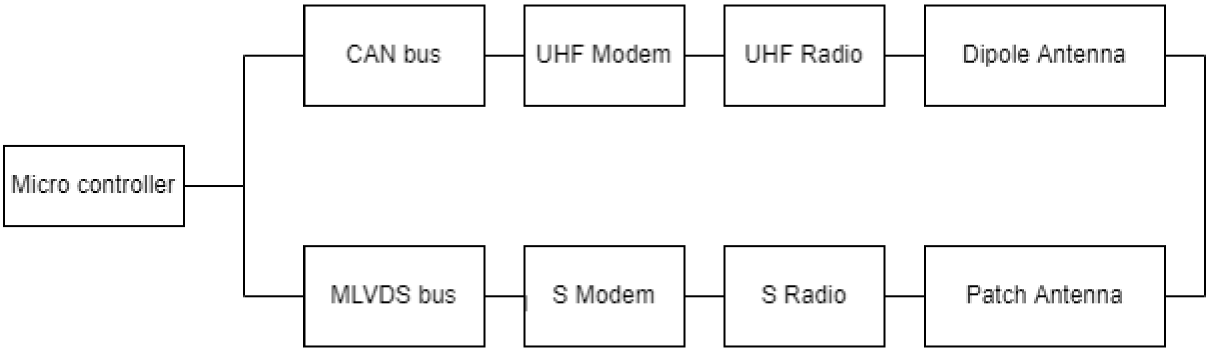


Figure 29 RBD - COMMSYS - Communication with ground - basic system

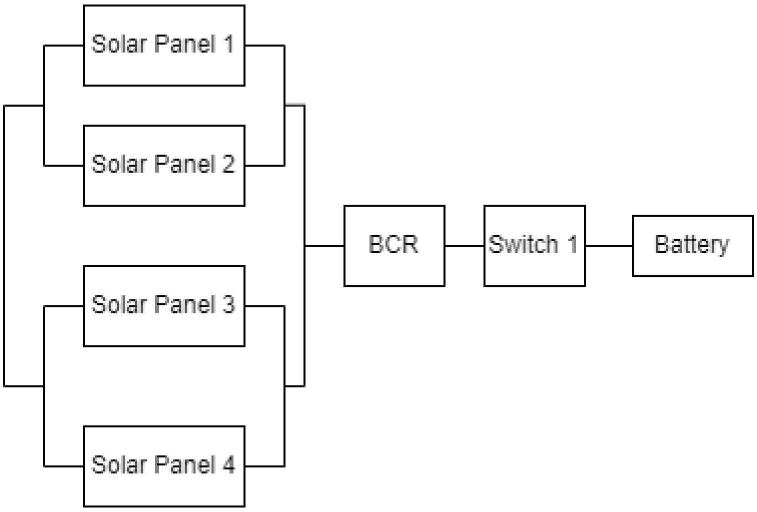


Figure 30 RBD - EPS - Power Generation and Battery Recharge - basic system

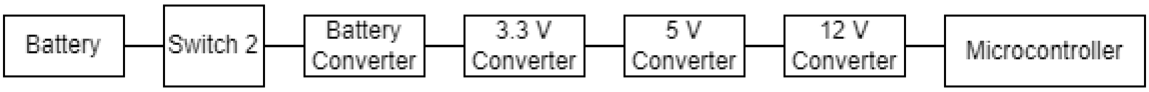


Figure 31 RBD - EPS - Power Distribution - basic system

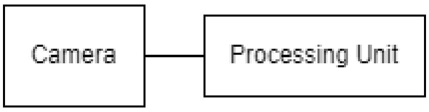


Figure 32 RBD - Payload - Mission data collection and processing – basic system

5.4 Mitigation Strategies

5.4.1 A dependable CubeSat's architecture

In the traditional architecture analysed through the FTA, each subsystem performs its specific function, and that means that critical functions are likely to be lost when a failure happens in one subsystem. In particular, the FMEA highlighted that the functions carried out by ADCS, OBC and payload can be considered critical to achieve a successful mission, and the FTA proved that all these subsystems have a single point of failure in their processing unit. To overcome this issue, it was developed a different system architecture based on the idea that these subsystems' functions can be reallocated in any of the processing units present in the CubeSat. In this way, even if one processor fails, the system can preserve its functionality because the affected subsystem is not lost.

In this new configuration, the core of the overall system are the three Processing Units (PU) that used to be the OBC, ADCS and payload processing units. The hardware characteristic of each subsystem (sensors, ADCS actuators, RGB camera) is divided into Resource Modules (RM) that are connected to all processing units. In this way, each processing unit can operate all the critical hardware in the spacecraft. Opposed to the traditional architecture where the subsystems' processors work under the OBC control, in this architecture the processing units run in an asymmetric multiprocessing configuration, where they can exchange executable functions one with each other. In the nominal operative mode, every PU runs a list of functions that implement the operations of a specific subsystem, while if a failure occurs, the functions of the compromised subsystem will be reallocated to another processing unit.

To make sure that a generic function can be moved successfully between PUs, there are two crucial elements that must be implemented. The first one is the Functions Manager (FM): a piece of software running on every PU that constantly checks their health status, evaluates their calculation by a voting system and manages the functions of the whole system performing the reallocation. The second crucial elements are common buses that allow any PU to access to any resource, such that a reallocated function will be able to be physically implemented regardless of where it is being executed. Figure 33 shows the new system architecture.

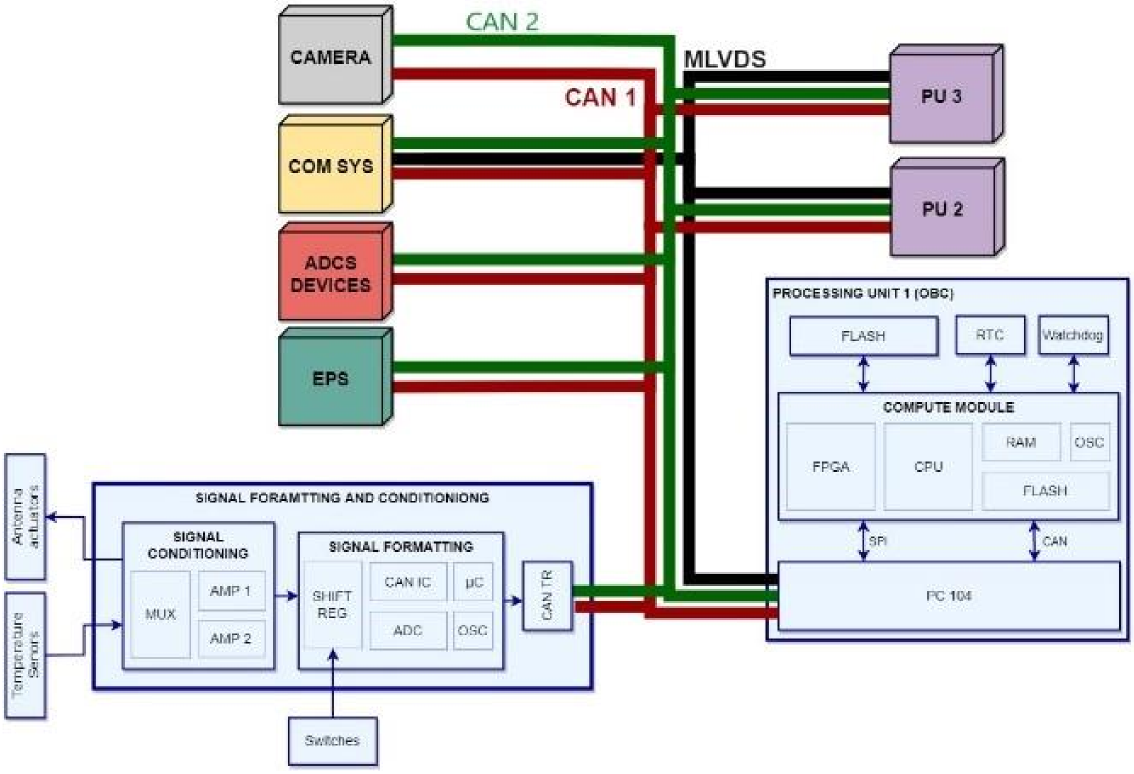


Figure 33 CubeSat's dependable architecture

The satellite's three main processing units provide computational and storage capacity to the overall system. With respect to the centralized architecture, these major components must have better technical specifications, since each one of them should be able to store and execute files inherent to some other subsystem's function. The three processing units are connected to all the resource modules with two different kinds of bus, in order to manage scientific and housekeeping data separately. For the command and data handling two CAN bus are used, and one of them has the specific purpose to have a communication channel that is always free for FM to reach any PU at any moment. Furthermore, in off nominal scenarios it can also work as a backup data bus. The CAN bus allows the communication in a multi-master configuration with a bit rate that goes up to 1Mbps, providing the system with a reliable and efficient data interface. For scientific data, a higher bit rate is required, so that a MLVDS bus resulted to be the optimal candidate, in comparison to other options that would not provide a multi-master configuration at the same bit rate (≤ 200Mbps).

For what concerns the resources, they are all communicating through either the CAN or the MLVDS, depending on the kind of data that they are sending or receiving. Each resource module has one microcontroller which function is to simply gather the data from their connected devices, to make them available on the bus and share them with the processing unit that requires that data.

Such configuration enhances the ability of the system to autonomously mitigate failures while decreasing the necessary hardware harness needed for the redundancy implementation. In this configuration, the redundancies are implied in the architecture itself (leaving out the case where the fault is on the resource module), since all the processing units are designed to carry out the critical tasks that usually would be running on the other PUs.

However, despite it carries several benefits in terms of reliability, the main downside of this design is the more complex implementation and the synchronization between all the devices for a correct communication on the bus. This issue can be mitigated by designing a careful validation campaign during the development of the software.

5.4.2 Function Manager: a simple Fault Detection System

The Function Manager is a software included in all the processing units' software, whose purpose is to determine whether a processing unit has failed. While simple fault detection features might be already present in the operative system, it is appropriate to design a custom software for the specific system.

The CAN bus already provides two alternatives for the fault detection of the connected hardware (node): cyclic querying of the node state by a higher order instance ("node guarding" principle), and automatic transmission of a "heartbeat message" by the network nodes ("heartbeat" principle).

With the node guarding approach, a certain network node of higher level (in a CubeSat it could be the OBC) requests the other nodes in the network at defined intervals to transmit a communication about their operational state (stopped, operational, pre-operational). If a note does not respond to this request within a certain period of time, it is interpreted as a failure of the node. At the same time, if the master node does not send this request for longer than the expected period, the other nodes in the network detect a failure in the master node.

With the heartbeat principle, each node automatically transmits its state at regular intervals.

In the SILVA spacecraft, the idea is to combine both principles to detect the processing units' failures. In nominal conditions, each PU uses the heartbeat principle, and transmits its health state at predefined intervals. If one PU does not transmit its message, the other two can then apply the node guarding principles and solicit the dormant processing unit to respond to their status request. Since in the SILVA dependable architecture there is not a hierarchically superior processing unit, all of them can take the role of master node in the network and request other elements in the network to state their operative status. If the dormant processing unit does not respond a certain amount of time, it is considered a failed unit.

The Function Manager is also able to perform diagnostic and consistency checks within the single processing unit, by comparing the results obtained by onboard processes and the results expected to be seen. That can be implemented by checking the value of some identified critical parameters against the defined nominal ranges, or by using a model of spacecraft's functions as a reference. Another control the Function Manager can perform is verifying that onboard operations are executed within the expected time and duration. If irregularities are detected, like a command that has not been executed, health and diagnostic routines are submitted to the affected processing unit.

In specific instances where the operative state of a processing unit is in doubt, the Function Manager can apply a voting system. All the processing units can execute all the software functions at any time; thus, it is possible to run the same routine in all the PUs at the same time to compare the results. Since there is not a voter external to the processing units, a set of criteria and scenarios should be elaborated to allow the processing units themselves to perform the voting (this technique is called super voting).

5.4.3 Hardware redundancy

Several hardware redundancies are included in the dependable design of SILVA CubeSat.

- The functions' redistribution that the system can perform if non nominal conditions are met makes the three processing units a redundancy one for another. It is important to consider that this is the case even though additional computers are not included in the design, and the processing units are redundant by a different onboard software architecture. This measure does not cause an increase in the weight or power consumption of the CubeSat.
- Since several processing units can perform the same functions, it is helpful to include a safety switch on a local level of each processing unit, so that the faulty ones can be rebooted or isolated. That would allow the disconnection of faulty processing units without generating other malfunctions to the bus.
- Critical data and telemetry essential to perform onboard operations shall be saved in the memories of all processing units. This data include:
    - Operative system;
    - OBC software executable;
    - ADCS software executable;
    - Payload data processing software executable;
    - Information about mission time and spacecraft operative modes;
    - Telemetry from ADCS sensors: IMU, magnetometer, sun sensors;
    - Telemetry from EPS: voltage of power buses, currents of power buses, voltage of batteries, charging currents of batteries, voltage of solar panels, currents out of solar panels, temperature of batteries, temperature of solar panels, temperature of EPS board;
    - Telemetry from OBC: temperature of OBC board, temperature of EPS board, temperature of ADCS board, temperature of payload board, temperature of COMMSYS boards.
- Two CAN buses are included. In nominal conditions, one of them is used only to assess the health status of the processing units, but it can be used as a redundancy if the main CAN bus fails.
- Two batteries are included in the design.
- An additional recharging line is included in the design. That can be a completely separate line from the original one (in that case, if one of them fails the power generated onboard is halved) or can be a crossed line (in that case, one recharging line can serve both batteries).

- One reaction wheel is added to ADCS actuators. If the system has four reaction wheels in a pyramidal configuration, it is still possible to control attitude on three axes if one of them fails. That might cause a complication in the determination and control algorithms, but it does not greatly reduce the system performance. The spacecraft weight is slightly increased by the additional reaction wheel.
- Solar panels can be used as a substitution for sun sensors if they fail. That would decrease the accuracy of attitude determination.
- The S band equipment can be used as a backup communication line to transmit housekeeping data and receive commands from the ground station.

5.4.4 Information redundancy

An easy way to enhance the reliability of the system is to protect data stored onboard or received from ground through encoding. These information redundancy techniques are based on adding specific information to the data packets so that it is possible to detect errors. Some coding schemes can even perform error correction.

Usually, these techniques are used to avoid data corruption during its transmission, storing or processing. Different functions benefit more from different coding schemes.

There are different techniques that can be implemented according to necessity.

- Parity codes: in their simplest form they consist in adding a further bit to the data, such that the total number of 1 bit is even or odd. This scheme allows to detect one fault in the data, while more refined versions of it may detect more faults in particular cases. These codes are vastly used in memories.
- m-out-of-n code: the codewords are composed of n bits, and m of them have the value 1. This code allows the detection of one fault.
- Checksum codes: the data is divided into groups and to each of them are added the bits corresponding to the sum of the data in the group. They allow error detection (even multiple errors can be detected in particular combinations), and they are mostly used to protect transmissions.
- Cyclic Redundancy Codes: these codes are based on the properties of Boolean polynomials. They are particularly suited to protect data packets in transmission channels and in mass storage devices.
- Hamming codes: these codes are based on adding a given number of code bits that are calculated each as the XOR of a given group of data bits. They are the most popular solution to protect data in memory devices. They allow a single error correction and double error detection.

A combination of these techniques should be implemented to reduce the errors propagation that may arise when faulty data is used in further onboard calculations.

5.4.5 Failures Recovery Scenarios

In this paragraph, examples of how the system would recover from some failures are covered.

5.4.5.1 One processing unit fails

The failure of a processing unit can be detected in several ways by the Function Manager.

In this scenario, it is assumed that the PU1 does not transmit its periodic heartbeat message. The system response would be articulated in the following steps:

1. The system recognizes the missing heartbeat message from the processing unit;
2. If PU1 does not transmit another heartbeat message in a defined amount of time, the other two processing units request it;
3. If PU1 still does not respond with a heartbeat message, PU2 and PU3 ask confirmation to each other that they both do not receive response from PU1;
4. If the answer is negative, meaning that one between PU2 and PU3 receives the heartbeat message from PU1, diagnostic routines are performed to identify where the failure is. If the answer is positive, meaning that none processing unit receives response from PU1, PU2 or PU3 commands the reboot of PU1;
5. After the reboot and some reconfiguration time, it is requested another heartbeat message from PU1;
6. If there is still no response, the whole reboot routine is repeated other two times;
7. If PU1 is still inactive, it is then isolated by the rest of the system by disconnecting it from the bus;
8. PU1 functions are reallocated to the other processing units according to the computational resources available in each processing unit and considering the criticality of the software running on them. That means:
    - If the processing unit running the ADCS software fails, its functions are reallocated to the processing unit running the OBC software, which is the least computational demanding one;
    - If the processing unit running the onboard images processing software (payload) fails, its functions are reallocated to the processing unit running the OBC software, which is the least computational demanding one;
    - If the processing unit running the OBC software fails, its functions are reallocated to the processing unit running the payload software, because it is less critical than the ADCS one and it can be slowed down without greatly affecting the system performance.

5.4.5.2 Two processing units fail

If a second processing unit fails, the CubeSat operational state becomes critical. At this point, it is not guaranteed that the system succeeds to recover the failure. However, the system response would be articulated in the following steps:

1. If one PU does not transmit its heartbeat message, the other one solicits it;
2. If the request is not satisfied, if it is possible, both processing units perform an interface check to verify whether the failure is located on the bus or in the other processing unit;
3. If one processing unit does not find failures in the interface elements, it commands the reboot of the other processing unit. It is important to assure that the processing units are instructed to command the reboot of the other ones in different time stamps, so that

it is avoided the situation where both processing units try to reboot the other one at the same time;

4. After the reboot and some reconfiguration time, new attempts of communication are established;
5. If the processing unit still does not respond, it is disconnected from the bus;
6. All onboard software functions are then allocated to the surviving processing unit.

Ideally, all the processing units should be able to run all the onboard software at the same time. However, it is reasonable to expect that the onboard processors might not be that oversized. In that case, it is accepted that the system would operate at a lower level of performance, and that the different software would be executed at different times, according to their priority and computational power available. In particular,

- The OBC software is the most critical one and it is always active;
- The ADCS software is fully active when the CubeSat is flying over a mission target (thus, it is required a higher pointing accuracy and stabilization to take clear images) or it is necessary to transmit mission data to ground (the S band antenna is quite directive). In other points of the orbit, the ADCS requirements are relaxed, so that the needed computational effort to satisfy them is lowered;
- The payload software is active only when particular operations are not being executed onboard, particularly by the ADCS software. Its resources allocation is reduced, thus longer data processing time is to be expected.

5.4.5.3 One reaction wheel fails

The failure of a reaction wheel can be detected by observing an anomaly difference between the attitude commanded and that realized by the system. Furthermore, there are subsystem parameters that can be checked to identify a failure in the reaction wheels pack.

If one reaction wheel fails, the torques required to guarantee the attitude control on three axes can be redistributed on the other three reaction wheels. That can somehow reduce the attitude control ability, but the obtained result is still compatible with the system requirements. The control laws are complicated by this modification, then it is possible to observe an increase in the computational and power consumption of the ADCS subsystem.

5.4.5.4 Sun Sensors fail

If the measurements from the Sun Sensors are no longer received or are corrupted/unsuitable to be used to attitude determination calculations, solar panels can be used as alternative sensors. However, the measurement is coarser, and it might not be accurate enough to satisfy the system requirements.

5.4.5.5 One communication line fails

If one communication line with ground fails, it is possible to use the other one as a backup line.

The UHF band line is used to transmit housekeeping data and to receive commands from ground; if it fails, its communications can be entirely managed by the S band line without significantly altering the system operational life.

The S band line is used to transmit mission data; if it fails, it is not that easy to use the UHF band line to perform this kind of communication. The UHF equipment allows to reach a data rate that is a lot lower than that obtainable with a S communication system. This issue could be overcome by fragmentating the mission data to be sent in several packets, but that would seriously slow down the onboard operations and reduce the scientific output of the mission.

5.4.5.6 One recharging line fails

If one EPS recharging line fails, there are two possible scenarios.

If the two lines are completely independent from one another, the power generated onboard is halved because one line cannot charge both batteries.

If the two lines are crossed, one line can power the whole circuit, thus eliminating the failure effect on the system. This solution is more complex to implement, but it is more reliable and robust.

5.5 Fault Tree Analysis – Dependable system

To evaluate the effectiveness of the mitigation strategies it can be helpful to repeat some of the analysis, such as the FTA.

- Figure 34 analyzes the undesired event “OBC does not distribute commands at the right time”. The leading causes of this event are:
    - The failure of three processing units;
    - The failure of the two CAN buses;
    - Loss of synchronization among onboard operations.

  The two single points of failure have been eliminated, and the probability of data corruption greatly affecting the onboard operations has been reduced by the implementation of information redundancy techniques.

- Figure 35 shows the FT for the undesired event “Data are not collected”, meaning that the OBC cannot manage the spacecraft telemetry and mission data. The event happens when:
    - Signal formatting and conditioning unit of all three processing units fails;
    - Two CAN buses fail;
    - MLVDS fails.

  Two single points of failure have been eliminated.

- Figure 36 analyzes the “No communication with ground station” failure, which has not been really affected by the mitigation strategies.
- Figure 37 analyzes the “ADCS does not detumble the satellite” undesired event. The leading causes are:
    - The failure of three processing units;
    - A faulty magnetometer;
    - A faulty magnetic torque rod.

The main and most critical single point of failure has been eliminated.

- Figure 38 analyzes the "ADCS does not determine attitude" failure. The leading causes of this event are:
    - The failure of three processing units;
    - A faulty magnetometer;
    - A faulty IMU;
    - The loss of three sun sensors.

  The main single point of failure has been eliminated. The probability of data corruption greatly affecting the determination algorithms has been reduced by the implementation of information redundancy techniques. Besides, if reduced performances in attitude determination are tolerated, the system can use the measurements from the solar panels instead of those from the sun sensors. That makes losing that information extremely improbable.

- Figure 39 shows the FT for the "ADCS does not control attitude" undesired event. The leading causes of this event are:
    - The failure of three processing units;
    - The loss of two reaction wheels;
    - A faulty magnetic torque rod.

  The two main single points of failure have been eliminated, and the probability of data corruption greatly affecting the control algorithms has been reduced by the implementation of information redundancy techniques.

- Figure 40 analyzes the "Mission data are not collected" undesired event. The leading causes of this event are:
    - Failure of the RGB camera;
    - Failure of three processing units.

  The main single point of failure has been eliminated, and the probability of losing mission data due to data corruption has been decreased by information redundancy.

- Figure 41 shows the "Batteries do not recharge" failure, that would lead the spacecraft to not be able to store the newly generated power. The leading causes of this event are:
    - Failure of four solar panels;
    - Failure of two battery packs;
    - Failure of two recharging lines;
    - Faulty protection and load switches.

  The two main single points of failure have been eliminated.

- Figure 42 analyzes the "EPS does not distribute power" failure, which has not been affected by the implemented mitigation strategies.

The FTA on the dependable system highlighted a significant improvement in the number of single points of failure for critical functions. That directly translates in a higher system reliability.

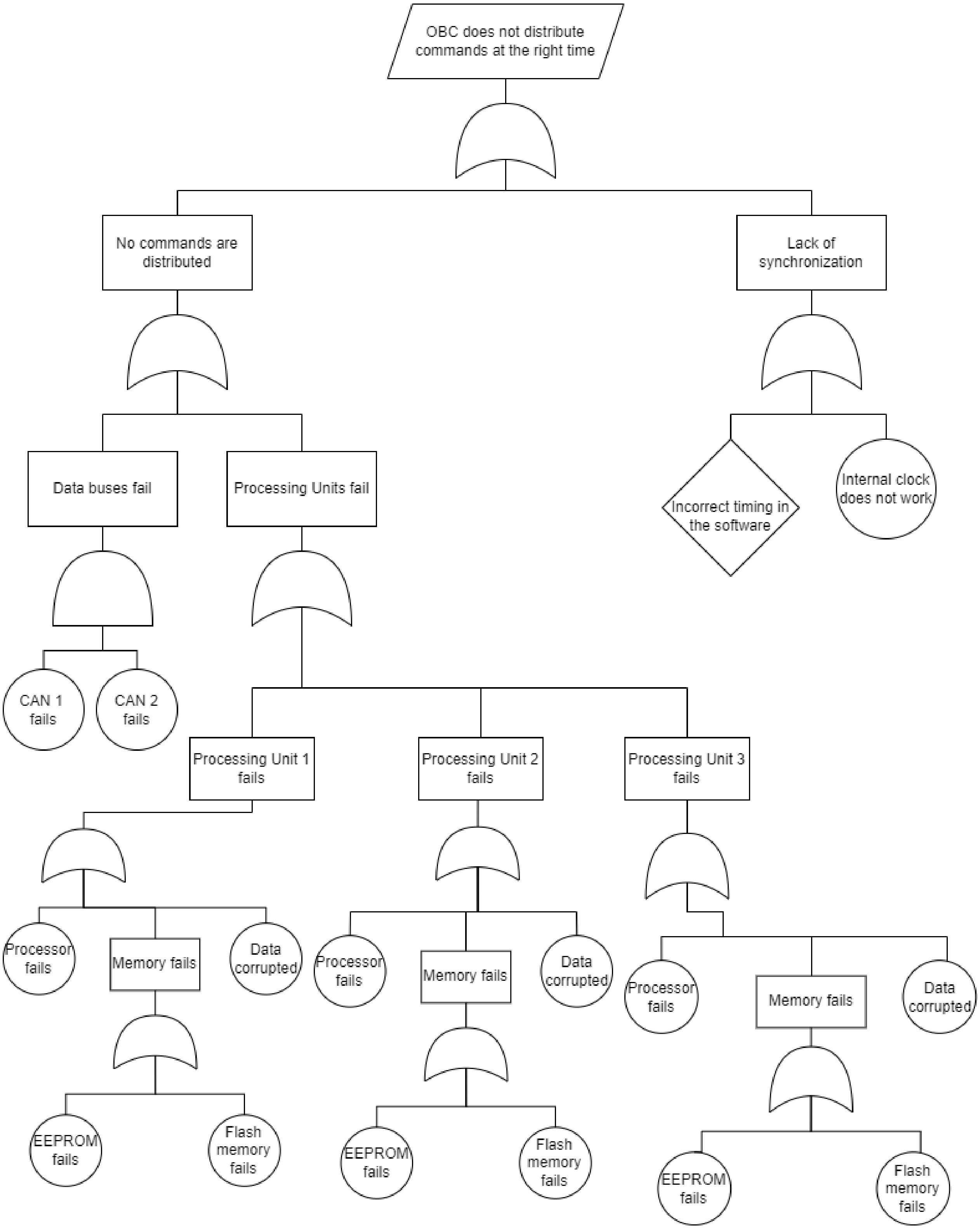


Figure 34 FTA - OBC – Commands and onboard operations management – dependable system

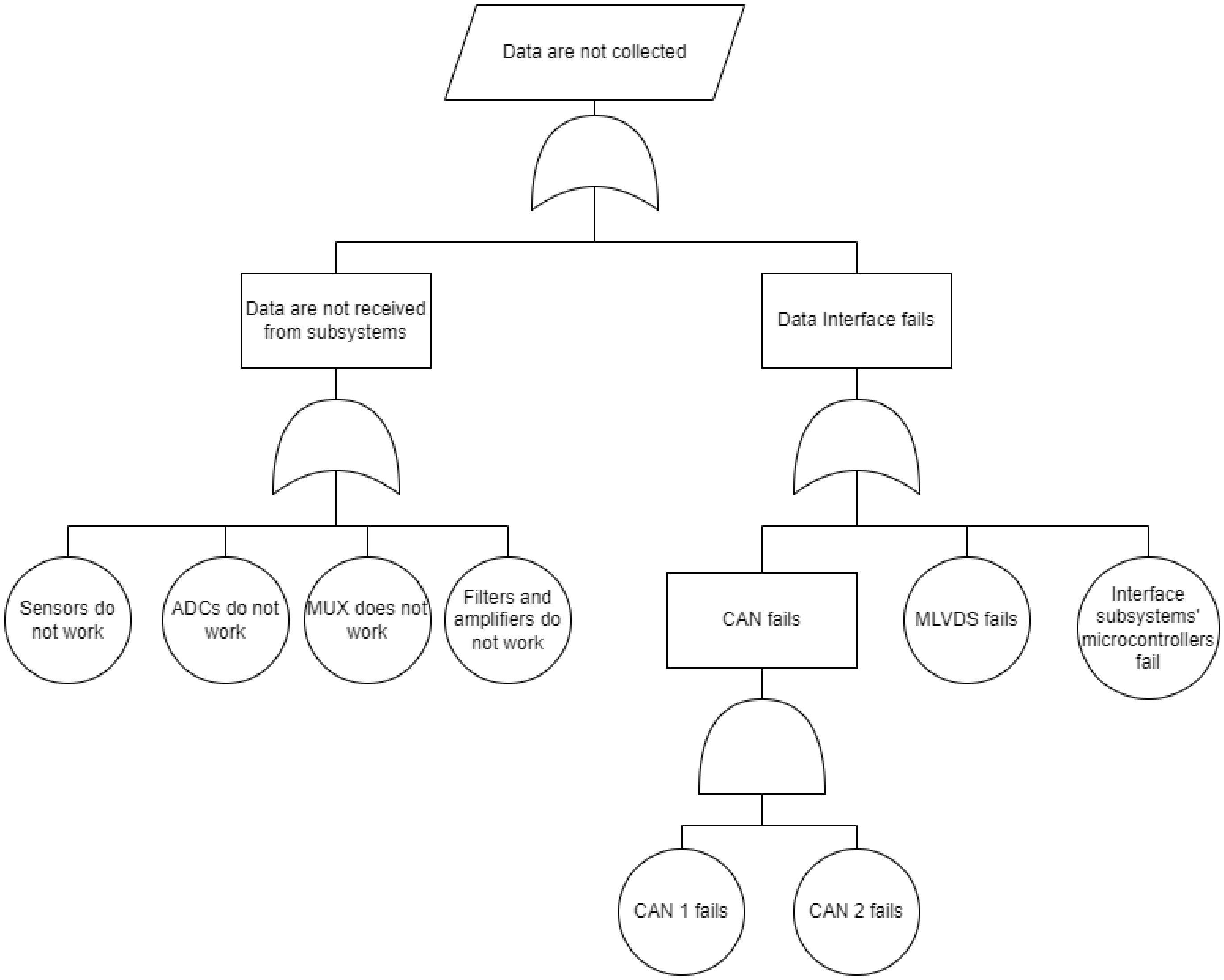


Figure 35 FTA - OBC - Onboard data management – dependable system

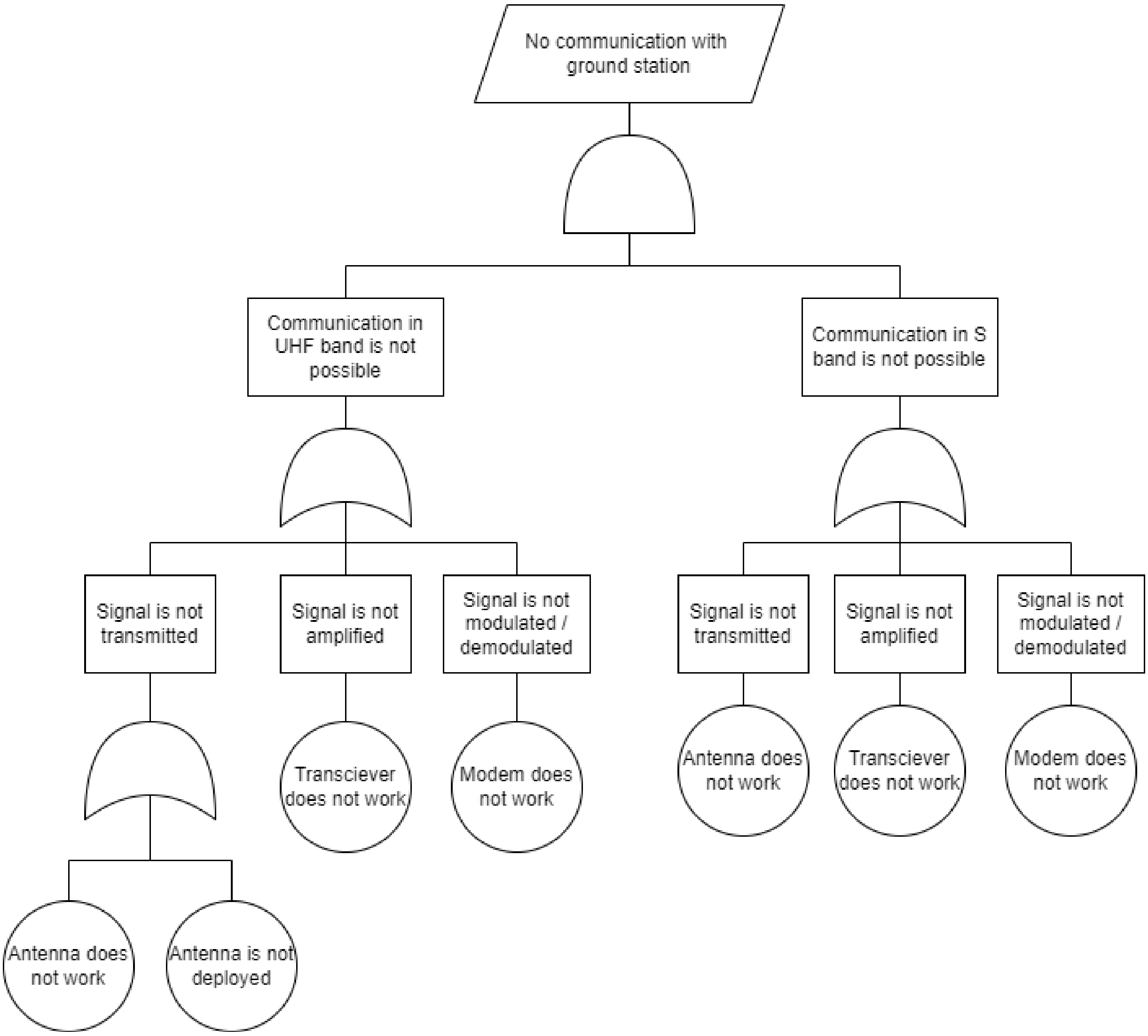

No communication with ground station
Communication in UHF band is not possible
Communication in S band is not possible
Signal is not transmitted
Signal is not amplified
Signal is not modulated / demodulated
Signal is not transmitted
Signal is not amplified
Signal is not modulated / demodulated
Transciever does not work
Modem does not work
Antenna does not work
Transciever does not work
Modem does not work
Antenna does not work
Antenna is not deployed

Figure 36 FTA - COMMSYS - Communication with ground – dependable system

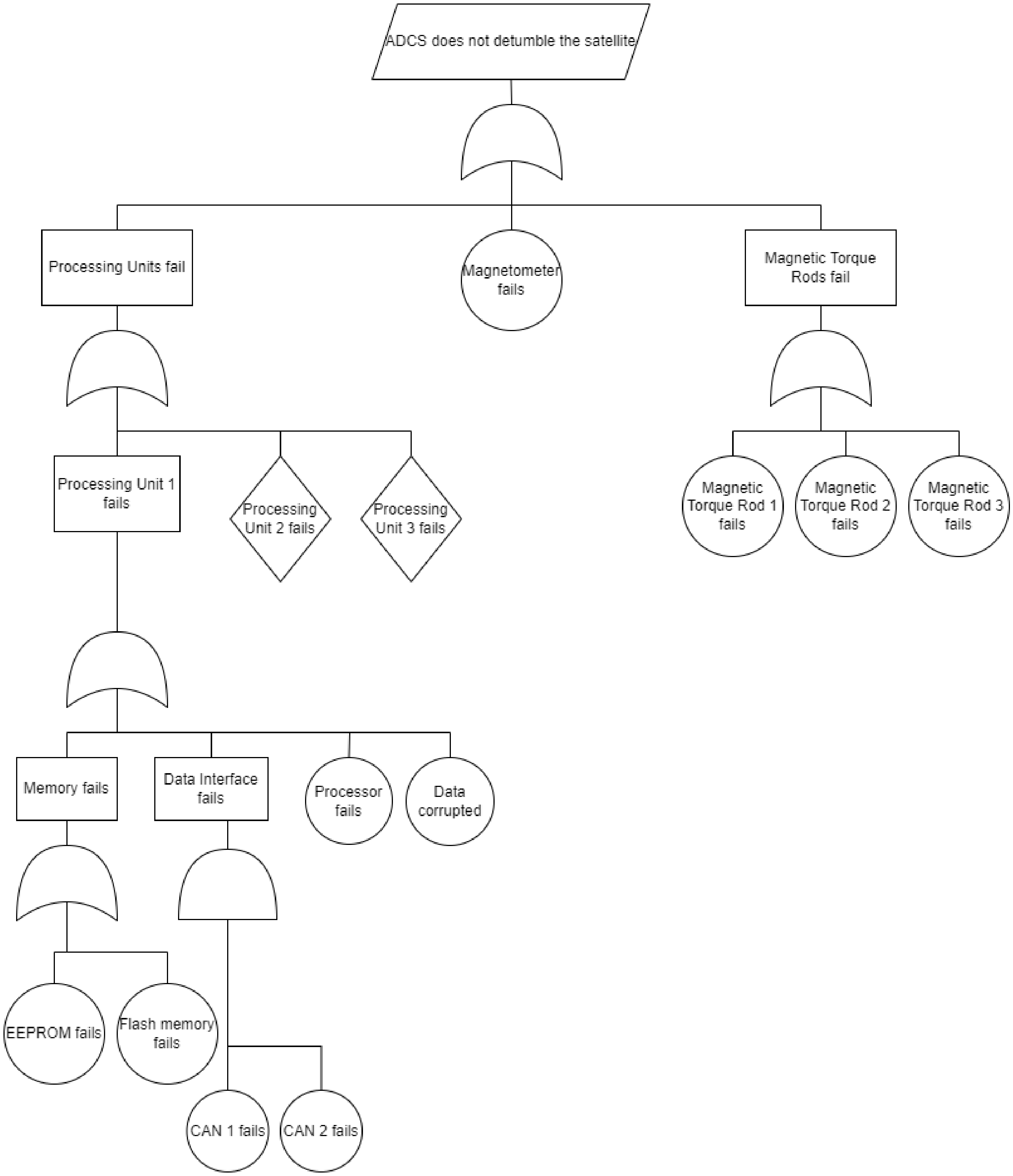


Figure 37 FTA - ADCS – Detumbling – dependable system

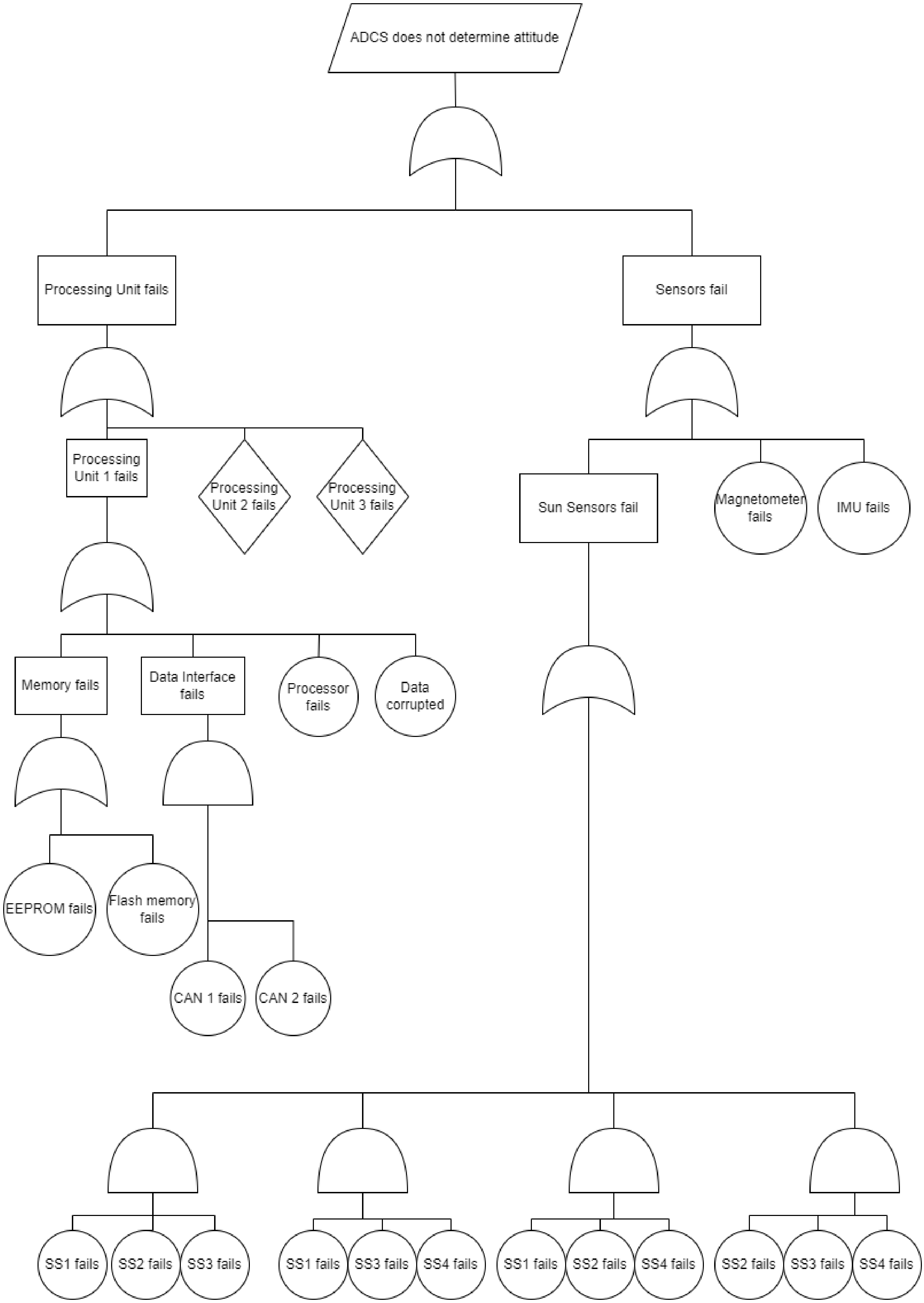


Figure 38 FTA - ADCS – Attitude Determination – dependable system

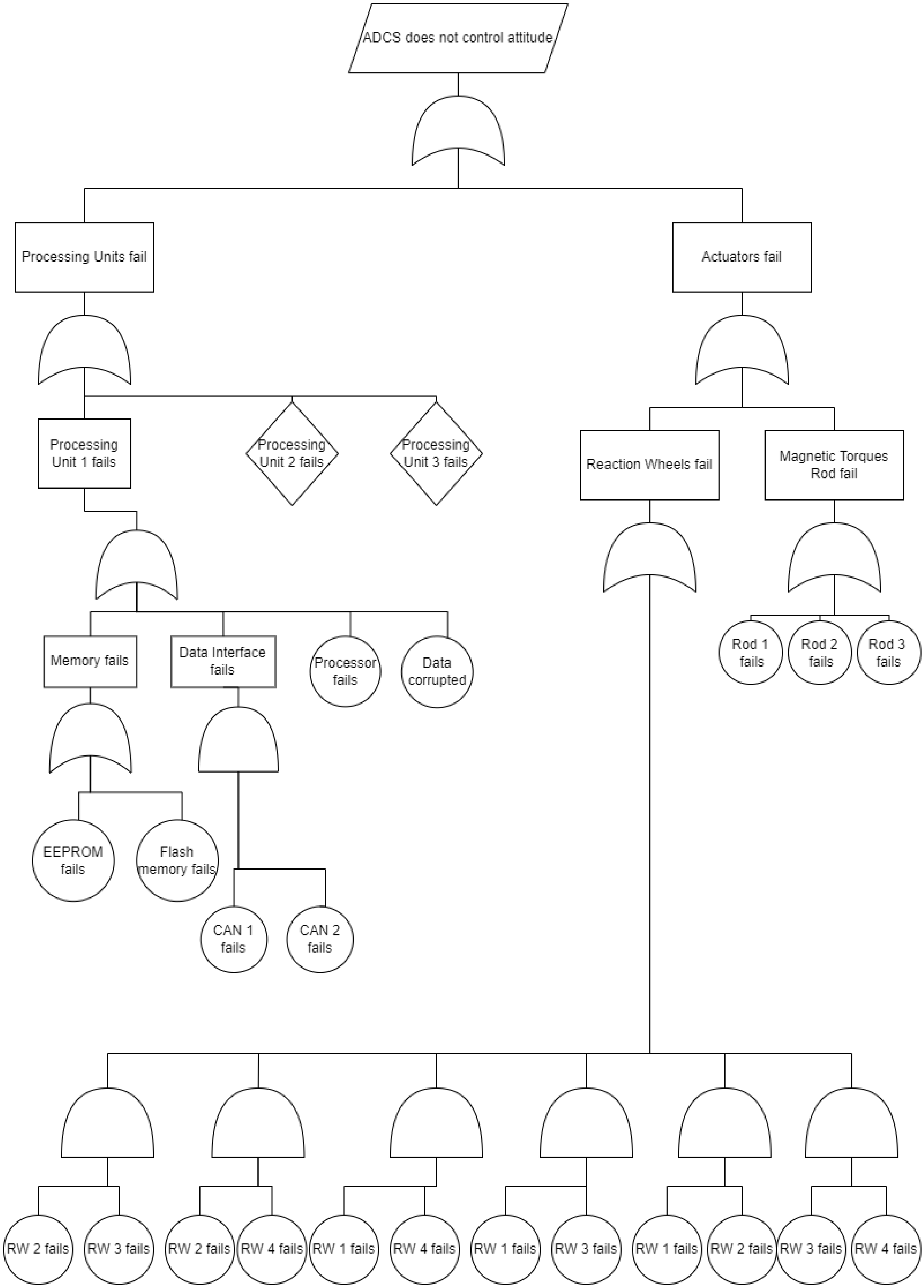


Figure 39 FTA - ADCS - Attitude Control – dependable system

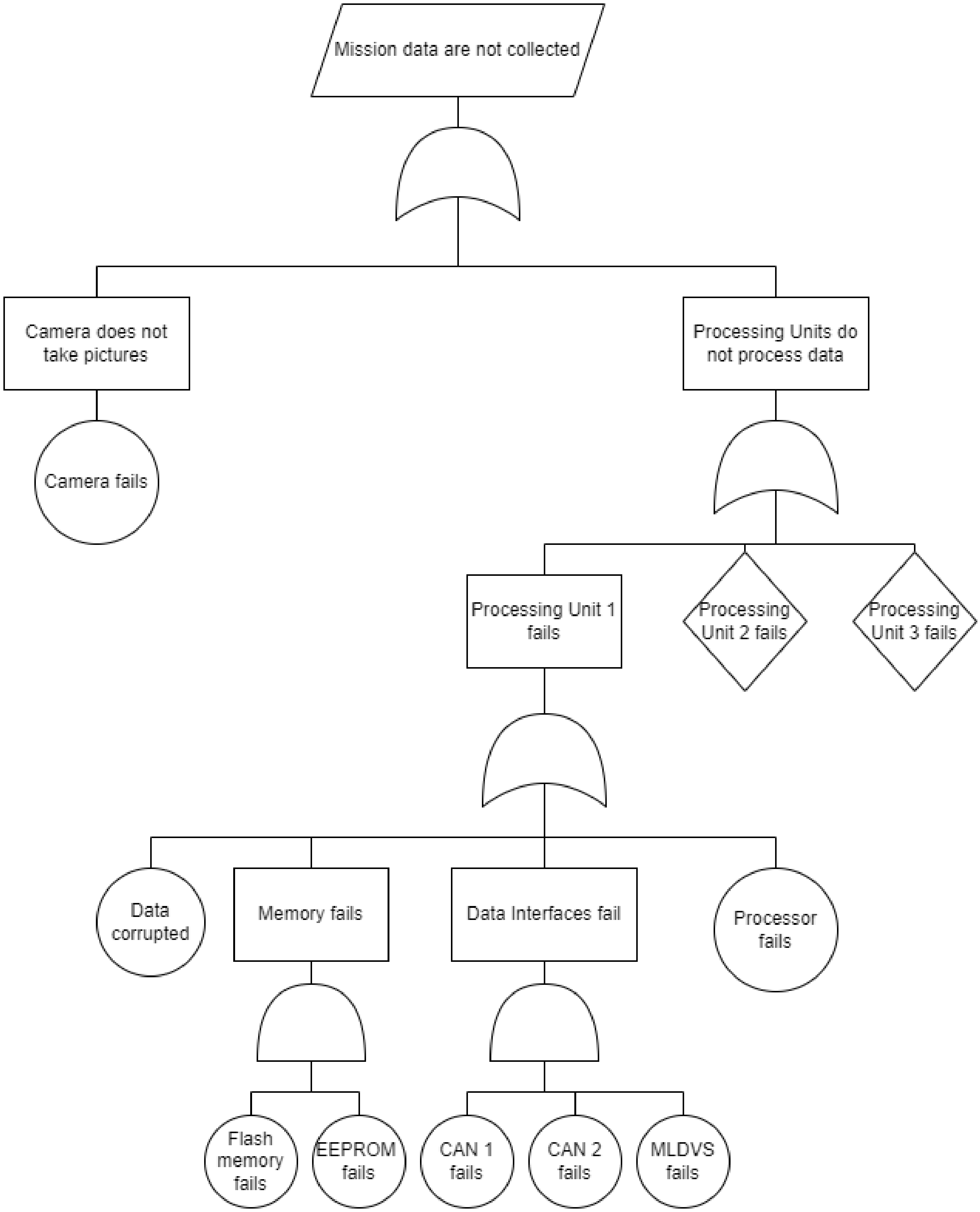


Figure 40 FTA - Payload - Collect and process mission data – dependable system

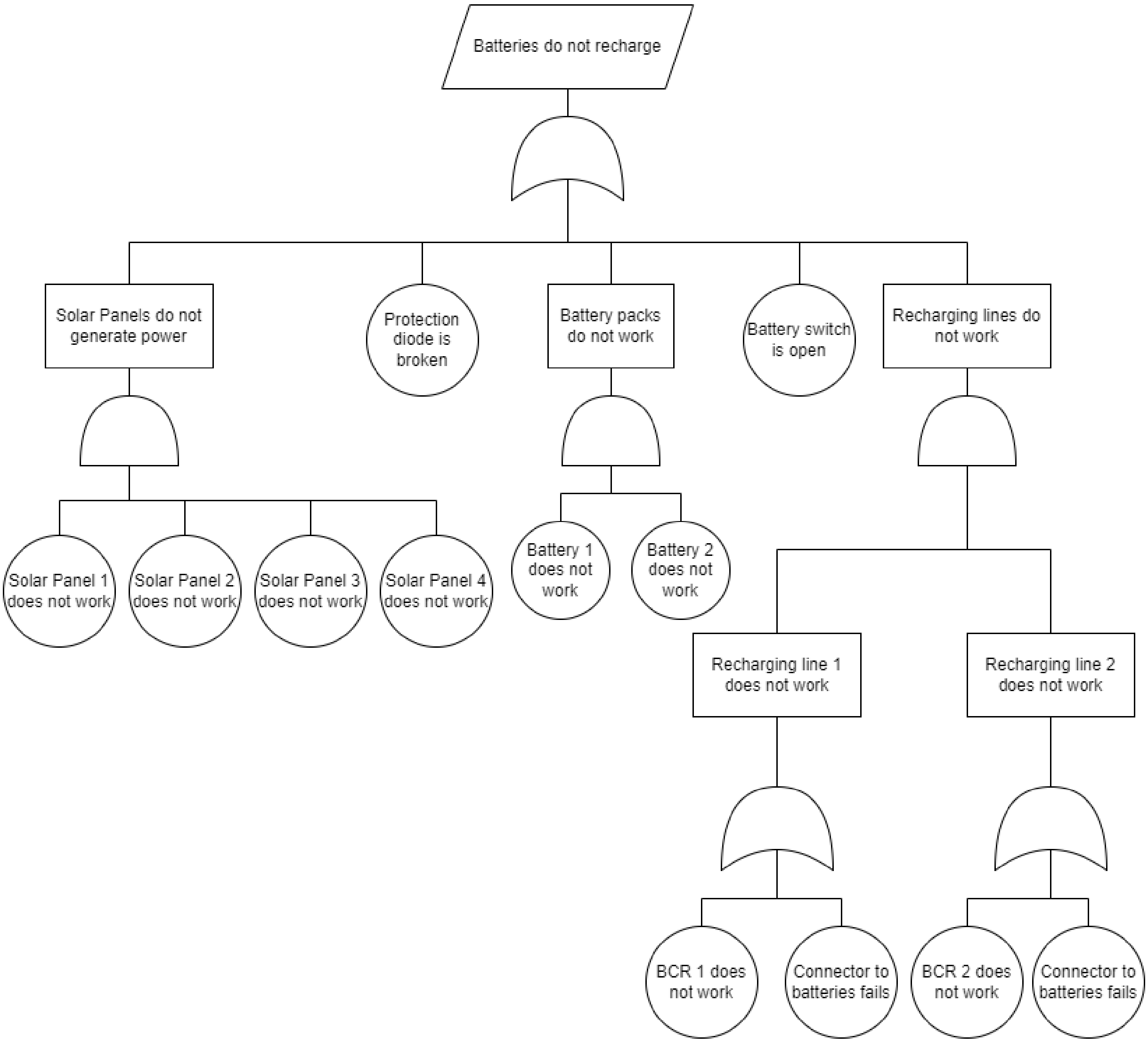

Batteries do not recharge
Solar Panels do not generate power
Protection diode is broken
Battery packs do not work
Battery switch is open
Recharging lines do not work
Solar Panel 1 does not work
Solar Panel 2 does not work
Solar Panel 3 does not work
Solar Panel 4 does not work
Battery 1 does not work
Battery 2 does not work
Recharging line 1 does not work
Recharging line 2 does not work
BCR 1 does not work
Connector to batteries fails
BCR 2 does not work
Connector to batteries fails

Figure 41 FTA - EPS - Power Generation and Batteries recharge – dependable system

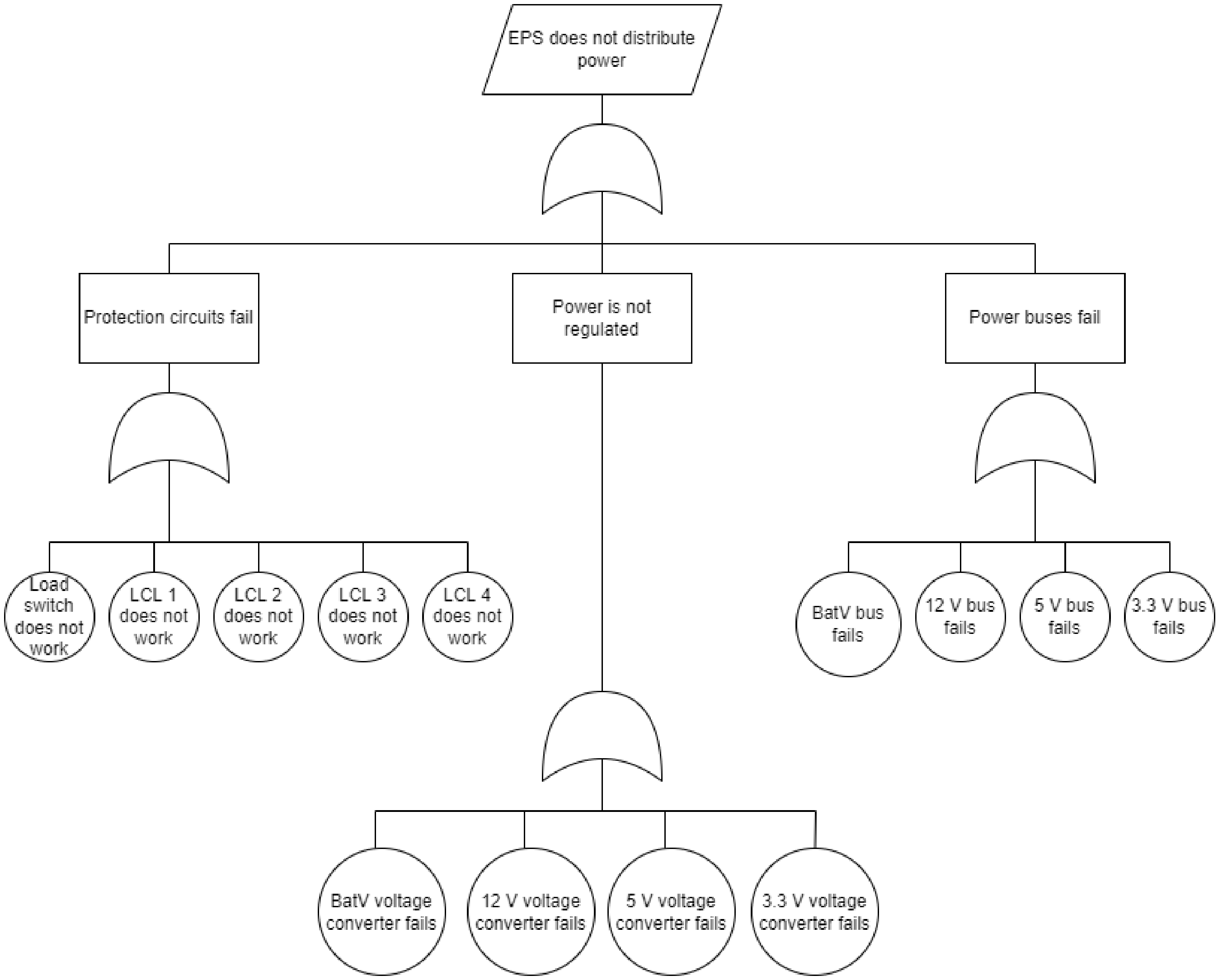


Figure 42 FTA - EPS - Power Distribution – dependable system

5.6 Reliability Block Diagrams – Dependable System

To complete the analysis of the dependable system, the reliability block diagrams of the main system functions are reconsidered.

- Figure 43 shows the OBC model considering the implemented redundancies. The three processing units behave like a parallel network, and that includes the signal conditioning units too. The two CAN buses also constitute a parallel network. The only element that is still in a series relationship with other components is the MLVDS bus.
- Figure 44 shows the ADCS model for detumbling. The three processing units constitute a parallel network, while the magnetometer and magnetic torque rods are still in series.
- Figure 45 shows the ADCS model for attitude determination. IMU and the magnetometer are still in series, while sun sensors and processing units constitute two different parallel networks. Even though the solar panels could be used as a redundancy for the sun sensors, they are not included in the RBD because that would greatly reduce the accuracy

of the attitude determination capabilities of the system; therefore, this possibility is considered as an undesired emergency solution rather than a subsystem design feature.

- Figure 46 shows the ADCS model for attitude control. The three processing units constitute a parallel network. The addition of the fourth reaction wheel allows to consider the reaction wheels pack as a parallel, because the attitude control can be guaranteed even if one reaction wheel fails. The magnetic torque rods are still in series.
- Figure 47 shows the COMMSYS model. The only modification is that the two CAN bus are a parallel network in the new configuration.
- Figure 48 shows the EPS model for power generation and battery recharge function. Solar panels are still in a parallel as before, and they are also included in another parallel representing the two different recharging lines. The two batteries are in a parallel too, thus the only single point of failure that still is in a series respect to other components is the load switch.
- Figure 49 shows the EPS model for the power distribution function. All the components in the distribution unit are still in a series, but the batteries are a parallel network.
- Figure 50 shows the payload model. The three processing units constitute a parallel, thus the only single point of failure left is the RGB camera.

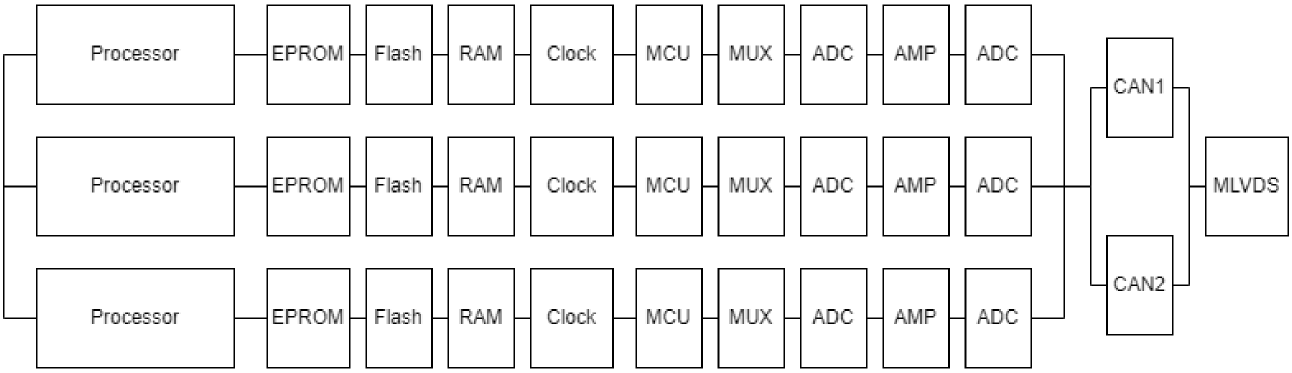


Figure 43 RBD - OBC - Commands distribution and data management - dependable system

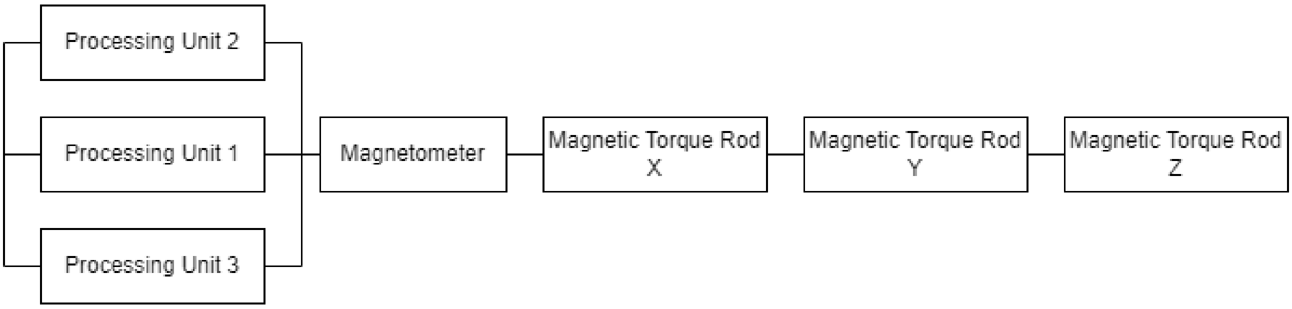


Figure 44 RBD - ADCS - Detumbling - dependable system

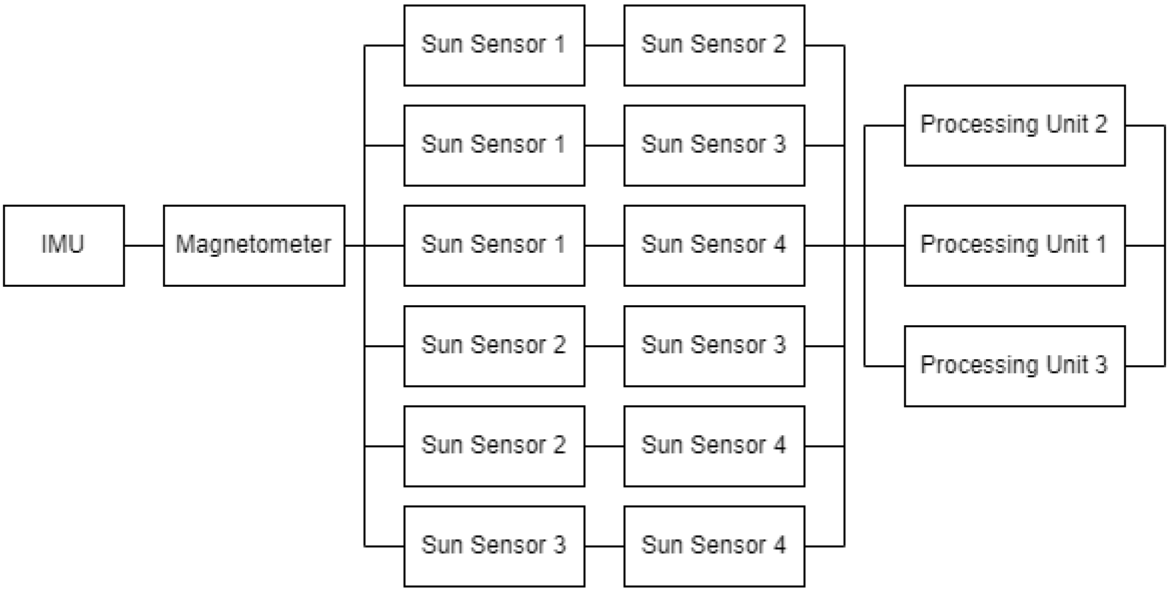


Figure 45 RBD - ADCS - Attitude Determination - dependable system

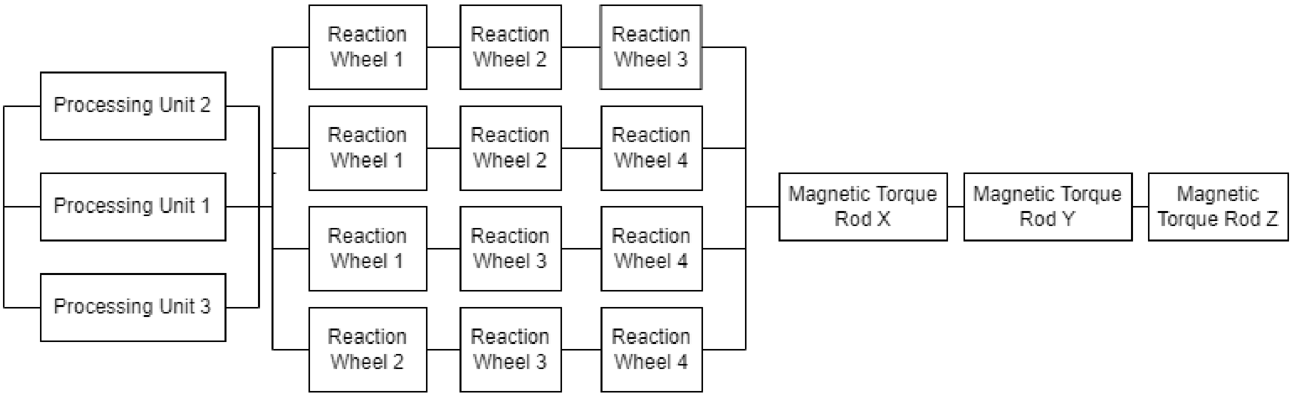


Figure 46 RBD - ADCS - Attitude Control - dependable system

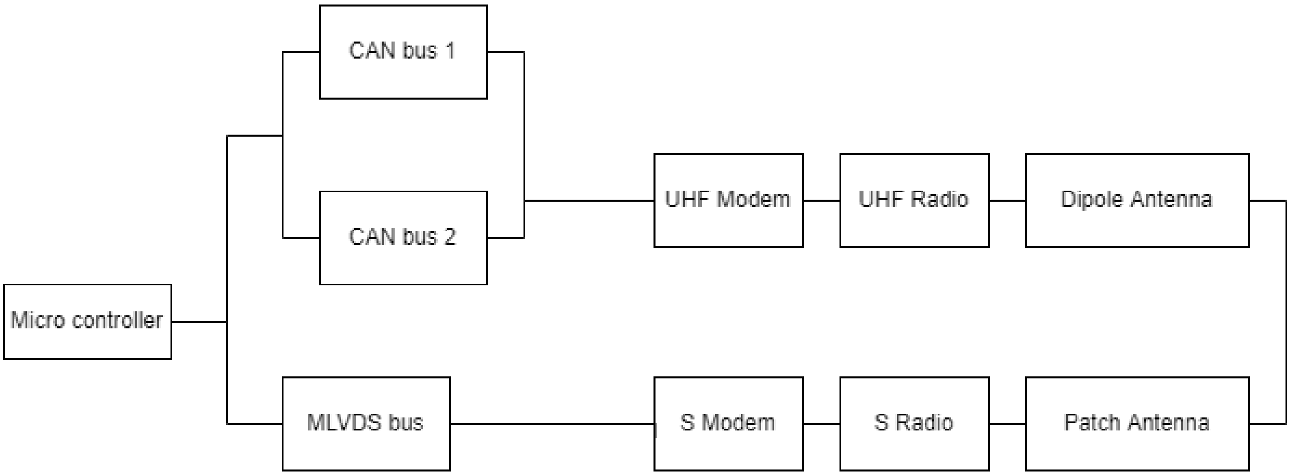


Figure 47 RBD - COMMSYS - Communication with ground - dependable system

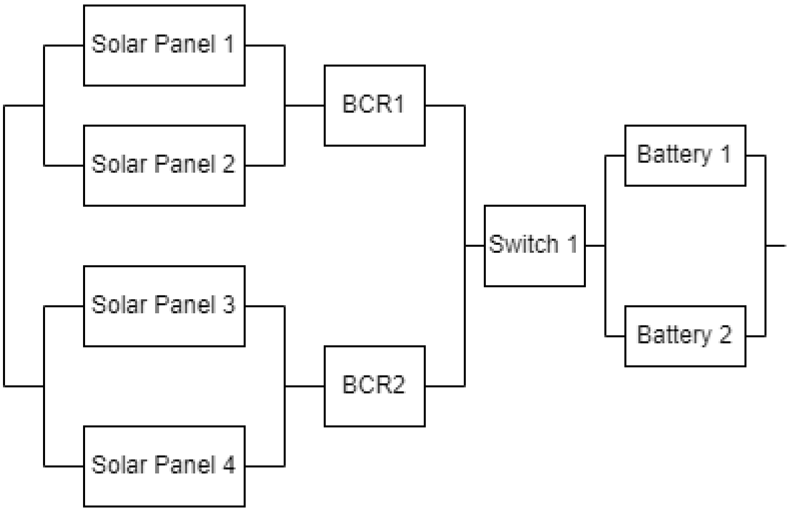


Figure 48 RBD - EPS - Power Generation and Batteries Recharge - dependable system

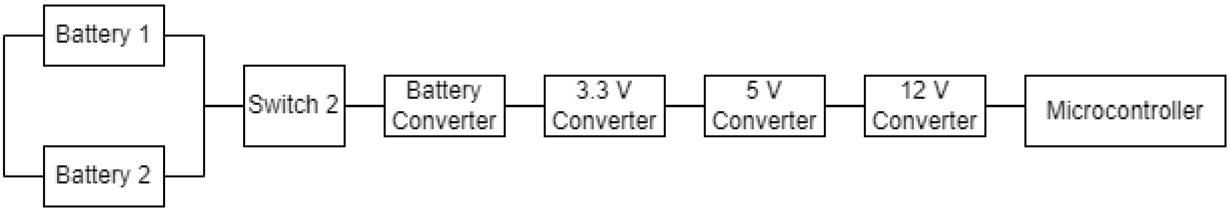


Figure 49 RBD - EPS - Power Distribution - dependable system

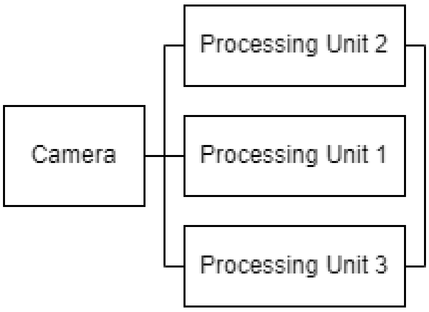


Figure 50 RBD - Payload - Mission data collection and processing - dependable system

Given the results of the previous analysis, it is reasonable to lower the probability number associated with some of the failures affecting the SILVA critical functions. In particular,

- The ADCS has been made more reliable both on the computational side (in the dependable design three processing units instead of one can perform the required calculations) and on the hardware one (one additional reaction wheel is included). Therefore, PN = 3.
- The COMMSYS is the subsystem less involved in the discussed mitigation strategies. Therefore, it is not considered appropriate to lower its probability number.
- The OBC has been made more reliable by distributed architecture. Therefore, PN = 3.

- The EPS has been made more reliable by the redundancies included, especially the double recharging line. However, it seems unrealistic to consider a PN lower than 2, so it is left unchanged.
- The payload has been made more reliable on the computational side, so PN = 3 for the onboard data processing function.

Table 7 shows the updated criticality evaluations for the SILVA functions. All of them remain critical (CN more than 6), but a fair amount have a CN lower than the original design.

Table 7 SILVA Critical Functions Risk Evaluation - dependable system

	Subsystem	**Severity level**	**SN**	**PN**	**CN**	**Risk Assessment**
Detumble the CubeSat	ADCS	Catastrophic	4	3	12	Severe - Avoid
Communication with Ground Segment	COMMSYS	Catastrophic	4	2	8	Major - Mitigate
Manage onboard operations	OBC	Catastrophic	4	3	12	Severe - Avoid
Manage onboard data	OBC	Catastrophic	4	3	12	Severe - Avoid
Generate power	EPS	Catastrophic	4	2	8	Major - Mitigate
Distribute power	EPS	Catastrophic	4	2	8	Major - Mitigate
Determine attitude	ADCS	Critical	3	3	9	Major - Mitigate
Control attitude	ADCS	Critical	3	3	9	Major - Mitigate
Take images	Payload - Sensor	Critical	3	2	6	Moderate - Allow
Process images onboard	Payload – Processing Unit	Critical	3	3	9	Major - Mitigate

6 Conclusions

The number of CubeSats' missions is destined to keep increasing over the next decade, and always higher quality standards are required as the mission objectives become more ambitious. In this context, it is important to guarantee that the CubeSats will be able to provide the service they were designed for; therefore, the dependability of CubeSats needs to increase.

A statistical analysis highlighted that the main reason why CubeSats missions have high rate of failure is the lack of implementation of risk analysis and management techniques. The main purpose of this thesis is to propose an agile method that is manageable even by students, but it is still effective in strengthening the system against failures.

The first step of this method consists in defining the mission's success criteria and main goals.

Then, alongside the first design activities, the first reliability task to be completed is a FMEA. The analysis allows to identify the modes of failure of the system and evaluate their severity and impact on the overall mission. Considering the FMEA results, the system engineer should be able to identify the critical functions of the system and the correlated failures that need to be mitigated with the highest priority.

Focusing on the individuated critical functions and failures, the method continues with the evaluation of combinations of failures. Therefore, the next tasks to be completed are the FTA e RBD analysis. These analyses allow the system engineer to identify the single points of failure in the system and the minimum set of components that need to fail to cause the loss of the system.

The mitigation strategies are defined to address these criticalities.

All the analyses are meant to be considered iterative tasks, so that it is possible to evaluate the effects of the mitigation strategies and further improve the system design.

The method was applied on a real educational mission under development in the CubeSat team Polito, SILVA. SILVA is an Earth observation mission whose mission objective is to study the vegetation status and evolution over time. To reach this goal, the 3U CubeSat hosts a RGB camera and an onboard data processing software based on SRR algorithms.

The analyses carried on the mission showed that the most critical and prone to failures subsystems were the OBC, the ADCS, and the payload. The individuated mitigation strategies involved adding little to none additional hardware in the system design (only one additional reaction wheel and battery), and the redundancies were automatically included in a non-standard, dependable system architecture. The idea is to use the on board computers as hardware redundancy one for another, such that, if one of them fails, its functions can be redistributed to the other computer available.

While this solution does not increase the weight, the cost, or the power consumption of the CubeSat, it highly increases the reliability of the system. The cost to pay is a more complex implementation, but it is an interesting alternative to the design approach based on procuring high quality and space rated EEE components.

7 References

[1] ECSS – Q – ST — 30C - Dependability.

[2] ECSS – M – ST - 80C - Risk Management.

[3] ECSS – Q – ST – 30 – 02C – Failure modes, effects (and criticality) analysis (FMEA/FMECA).

[4] ECSS – Q – ST – 40 – 12C – Fault tree analysis.

[5] ECSS – E – ST – 50 – 15C – CANbus extension protocol.

[6] W. E. Vesely, F. F. Goldberg, N. H. Roberts, D. F. Haasl, Fault Tree Handbook, U.S. Nuclear Regulatory Commission.

[7] Sergio Chiesa, Affidabilità sicurezza e manutenzione nel progetto dei sistemi, CLUT.

[8] Martin Langer, Jasper Bouwmeester, Reliability of CubeSats – Statistical Data, Developers' Beliefs and the Way Forward, conference paper on 30th Annual AIAA/USU Conference on Small Satellites.

[9] Jasper Bouwmeester, Martin Langer, Eberhard Gill, Survey on the implementation and reliability of CubeSat electrical bus interfaces, CEAS Space Journal - Springer.

[10] J. Bouwmeester, A. Menicucci, E. K. A. Gill, Improving CubeSat reliability: subsystem redundancy or improved testing?, Reliability Engineering and System Safety 220 – Elsevier.

[11] Martin Langer, Michael Weisgerber, Jasper Bouwmeester, Alexander Hoehn, A Reliability Estimation Tool for Reducing Infant Mortality in CubeSat Missions, conference paper.

[12] Michael Swartwout, Secondary Spacecraft in 2016: Why Some Succeed (And Too Many Do Not).

[13] Gerard Obiols Rabasa, Methods for dependability analysis of small satellite missions, Politecnico di Torino.

[14] Daniel P. Siewiorek, Priya Narasimhan, Fault-tolerant architectures for space and avionics applications

[15] Amarendra Edpuganti, Vinod Khadkikar, Mohamed S Elmoursi, Hatem Zeineldin, Mohamed Al Hosani, A Novel EPS Architecture for 1U/2U Cubesats with Enhanced Fault-Tolerant Capability, IEEE

[16] Bungo Shiotani, Reliability analysis of Swampsat, University of Florida.

[17] ECSS – S – ST – 00 - 01 – Glossary.

[18] Simone Calamia, Marianna Centrella, Tommaso Giovara, Luca de Pasquale, Alessandro Allegrini, Lorenzo Galante, Luisa Iossa, etc., 3U CubeSat mission to assess vegetation hydration status and hydrological instability risk, 73rd International Astronautical Congress (IAC 2022), International Astronautical Federation.

8 Appendix A – FMEA Analysis

Failure Modes Effects Analysis (FMEA)

Product:	System: 3U CubeSat	Subsystem:	Equipment:

Ident. number	Item/ block	Function	Failure mode	Failure cause	Mission phase/ Op. mode	Failure effects a. Local effects b. Next higher level c. End effects	Severity classification	Failure detection method/ observable symptoms	Compensating provisions	Severity Number SN
1	Spacecraft	Fulfil Mission Objectives	It is not possible to establish communication with the ground segment	COMMSYS does not properly work; ADCS does not provide adequate pointing performances; Ground station is not available; Ground station is not able to process signal from spacecraft	Commissioning Mode Basic Mode Mission Mode Transmission Mode Safe Mode	a. It is not possible to communicate with the spacecraft; b. It is not possible to operate the spacecraft; c. Mission lost.	Catastrophic	Telemetry does not arrive to ground station		4

2			Spacecraft is not ejected by POD	Mechanical Interferences;
				CubeSat Release System fails;
				Electrical faults happen
					Launch	a. Spacecraft is not released into orbit;
						b. N/A;
						c. Mission lost
							Catastrophic	Spacecraft remains in the launcher		4

3			Spacecraft does not operate properly	Subsystems do not execute their functions; Missing or incorrect functions synchronization; Camera does not collect images in orbit; Payload processing unit does not process mission data	Detumbling Mode Commissioning Mode Basic Mode Mission Mode Transmission Mode Safe Mode	a. Spacecraft does not work as designed; b. Spacecraft does not fulfil mission objectives; c. Mission lost or severely degraded.	Catastrophic	Spacecraft does not survive or generate mission data		4
4			EPS does not correctly work	Voltage regulators do not work; MPPTs do not work; ADCs do not work; Filters and protection circuits are lost; Batteries do not work; Solar panels do not work; BCDR circuits do not work; Connectors fail; Activation switches fail Electrical buses do not distribute power correctly	Detumbling Mode Commissioning Mode Basic Mode Mission Mode Transmission Mode Safe Mode	a. No power to satellite subsystems; b. Loss of all subsystem; c. Mission lost.	Catastrophic	CubeSat is not powered		4

5			ADCS does not correctly work	Processor fails;
				IMU fails;
				Magnetometers fail;
				Reaction Wheel 1 fails;
				Reaction Wheel 2 fails;
				Reaction Wheel 3 fails;
				Reaction Wheel 4 fails;
				Magnetic Torque 1 fails;
				Magnetic Torque 2 fails;
				Magnetic Torque 3 fails;
				Sun Sensors 1 fails;
				Sun Sensors 2 fails;
				Sun Sensors 3 fails;
				Sun Sensors 4 fails;
				Connectors fail
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Not possible to determine and control attitude;
						b. Loss of payload and difficulty in communication;
						c. Mission degraded
							Critical	CubeSat cannot point to target accurately enough		3

6			UHF - COMMSYS does not correctly work	Antenna is not correctly deployed; Antenna does not work; Coaxial cable between antenna and board fails; Modem does not work; Radio module does not work; Filtering stages fail; Switches fail	Commissioning Mode Basic Mode Mission Mode Transmission Mode Safe Mode	a. COMMSYS does not receive commands and does not send telemetry; b. Not possible to operate the spacecraft; c. Mission lost	Catastrophic	Communication does not happen in the UHF band		4

7			S - COMMSYS does not correctly work	Antenna does not work; Coaxial cable between antenna and board fails; Modem does not work; Radio module does not work; Filtering stages fail; Switches fail	Transmission Mode	a. COMMSYS does not send mission data; b. Not possible to use mission data; c. Mission degraded	Critical	Communication does not happen in the S band		3
8			OBC does not correctly work	Processor does not work; RAM fails; Mass Memory fails; Timer does not work; Watchdog circuit fails; Data formatter and logic unit does not work; ADCs do not work; Switches fail; Thermocouples and Thermistors fail.	Detumbling Mode Commissioning Mode Basic Mode Mission Mode Transmission Mode Safe Mode	a. Not possible to manage data and to execute onboard operations; b. Not possible to control the spacecraft; c. Mission lost	Catastrophic	CubeSat does not respond to commands		4
9			Payload does not work	Camera does not work; Payload processing unit does not work	Commissioning Mode Basic Mode Mission Mode Transmission Mode	a. Not possible to acquire mission data; b. Not possible to process mission data; c. Mission degraded	Critical	Mission data is missing		3

10	OBC Processor	Manage command and data handling	Hardware break	Mechanical loads;
				Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Launch
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. OBC cannot execute onboard operations;
						b. Not possible to control the spacecraft;
						c. Mission lost
							Catastrophic	Processor does not respond to watchdog circuit	Failure propagation to other subsystems should be avoided	4

			Information corruption	Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Instructions and/or data are corrupted;
						b. Operative System crashes or is in undefined status;
						c. System temporarily out of service
							Minor	Detection algorithms recognize faulty data packets	Error detection and correction algorithms shall be implemented;
									Corrupted commands and data should not be distributed to other subsystems
										1

11	RAM	Store onboard data	Hardware break	Mechanical loads;
				Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Launch
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Working memory is not longer available;
						b. OBC cannot execute onboard operations;
						c. Mission lost.
							Catastrophic	OBC crashes		4

			Information corruption	Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Instructions and/or data are corrupted;
						b. Operative System crashes or is in undefined status;
						c. System temporarily out of service
							Minor	Detection algorithms recognize faulty data packets	Error detection and correction algorithms shall be implemented;
									Corrupted commands and data should not be distributed to other subsystems
										1

12	Mass Memory	Store onboard data and software	Hardware break	Mechanical loads;
				Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Launch
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Not possible to save data and access system code;
						b. OBC cannot execute onboard operations;
						c. Mission lost
							Catastrophic	Data is not available
								OBC crashes
									Multiple separated memories shall be included in the design	4

			Operative System Corruption	Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Operative System is not longer available;
						b. OBC cannot execute onboard operations;
						c. Mission lost
							Catastrophic	OBC crashes	Copies of the Operative Systems shall be saved in different memories;
									Ways to reinstall operative system should be considered and implemented
										4

			Information corruption	Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Instructions and/or data are corrupted;
						b. Operative System crashes or is in undefined status;
						c. System temporarily out of service
							Minor	Detection algorithms recognize faulty data packets	Error detection and correction algorithms shall be implemented;
									Corrupted commands and data should not be distributed to other subsystems
										1

13	Timer	Count time	Hardware break	Mechanical loads;
				Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Launch
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Not possible to keep spacecraft time;
						b. Synchronized operations cannot be executed;
						c. Possible mission degradation
							Major	Time on board is not longer available		2

			Information corruption	Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Spacecraft time not accurate;
						b. Synchronized operations are executed incorrectly;
						c. Possible mission degradation
							Major	Time on board is different from time know at the ground station		2

14	Watchdog circuit	Control and reset processor	Hardware break	Mechanical loads;
				Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Launch
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Watchdog circuit cannot reset OBC processor;
						b. Temporarily out of service processor status cannot be resolved;
						c. Possible mission loss.
							Critical			3

			Information corruption	Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Watchdog counting value is altered;
						b. OBC processor is reset even if not due;
						c. System temporarily out of service
							Minor	Detection algorithms recognize faulty data packets		1

15	Data formatter and logic unit	Format input/output data	Hardware break	Mechanical loads;
				Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Launch
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Telemetry data from connected hardware is not longer available;
						b. N/A
						c. Possible mission degradation.
							Critical	Loss of telemetry data		3

			Wearout	Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Noise on telemetry measurements is generated;
						b. Telemetry data measurements are discharged;
						c. N/A
							Minor			1

16	ADCs	Convert analog to digital data	Hardware break	Mechanical loads;
				Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Launch
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Telemetry data from connected hardware is not longer available;
						b. N/A
						c. Possible mission degradation.
							Critical	Loss of telemetry data		3

			Wearout	Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Noise on telemetry measurements is generated;
						b. Telemetry data measurements are discharged;
						c. N/A
							Minor			1

17	Switches	Monitor operative status of considered equipment	Hardware break	Mechanical loads;
				Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Launch
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Not possible to detect equipments operative status;
						b. N/A;
						c. Decision making ability may be reduced
							Minor			1

18	Thermocouples and Thermistors	Measure onboard temperatures	Hardware break	Mechanical loads;
				Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Launch
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Not possible to measure onboard temperatures;
						b. Decision making ability may be reduced;
						c. Some subsystems may overheat
							Minor	Missing temperatures measurements		1

19	CAN bus 1	Distribute data and commands among subsystems	Incorrect data transfer	Information corruption;
				Lack of synchronization;
				incorrect synchronization
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Data are missing, incorrect or they arrive with wrong timing;
						b. Onboard operations are incorrectly executed;
						c. Temporary lack of availability
							Minor			1

20			Hardware break	Mechanical loads;
				Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Data interface damaged;
						b. Data transfer is reduced;
						c. Spacecraft performances are degraded
							Critical	Data and commands are not distributed among different subsystem		3

21	CAN bus 2	Allow the monitoring of processors' health status;
		Distribute data and commands among subsystems
			Incorrect data transfer	Information corruption;
				Lack of synchronization;
				incorrect synchronization
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Data are missing, incorrect or they arrive with wrong timing;
						b. Onboard operations are incorrectly executed;
						c. Temporary lack of availability
							Minor			1

22			Hardware break	Mechanical loads;
				Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Launch
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Data interface damaged;
						b. Data transfer is reduced;
						c. Spacecraft reconfiguration ability is not guaranteed
							Major	Function Manager cannot access to this bus		2

23	MLVDS bus	Transfer mission data	Incorrect data transfer	Information corruption	Detumbling Mode Commissioning Mode Basic Mode Mission Mode Transmission Mode Safe Mode	a. Data are missing or corrupted; b. Loss of a mission data packet; c. N/A	Minor			1

24			Hardware break	Mechanical loads;
				Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Launch
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Data interface damaged;
						b. Reduced transmission rate of mission data;
						c. Spacecraft performance degraded
							Major	Mission data is not transfered from payload to commsys		2

25	Voltage regulators	Regulate voltage levels	Hardware break	Mechanical loads;
				Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Launch
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. EPS can regulate voltage towards connected subsystems;
						b. Affected subsystems cannot use power;
						c. Spacecraft and Mission lost
							Catastrophic	Off nominal voltages are measured along the buses		4

26	MPPTs	Change solar panels' voltage to produce the maximum power	Hardware break	Mechanical loads;
				Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Launch
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Voltage regulators cannot receive power;
						b. Energy cannot be acquired by Solar Panels and Batteries cannot be charged;
						c. Spacecraft and Mission lost
							Catastrophic	Power produced by solar panels is reduced		4

27	ADCs	Convert analogue to digital data	Hardware break	Mechanical loads;
				Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Launch
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Telemetry lost from connected hardware;
						b. EPS Thermal environment cannot be assessed;
						c. Decision making ability reduced.
							Major	Telemetry data loss		2

28	Filters and protection circuits	Protect the system from overcurrents and failures propagation	Hardware break	Mechanical loads;
				Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Launch
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Circuits cannot be protected by electrical hazards;
						b. Power may not be delivered to other subsystem and failure propagation cannot be prevented;
						c. Spacecraft and Mission lost.
							Catastrophic	Affected subsystems do not work or respond		4

29	Batteries	Store power	Hardware break	Mechanical loads;
				Radiations effects;
				Off nominal temperatures;
				Overcurrents;
				End of life
					Launch
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Power cannot be stored;
						b. Spacecraft cannot be powered during eclipses and cannot be rebooted at down;
						c. Spacecraft and Mission lost.
							Catastrophic	After a while, spacecraft is not powered		4

30	BCDR circuits	Regulate batteries charging and discharging	Hardware break	Mechanical loads;
				Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Launch
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Batteries cannot be charged and discharged;
						b. Power cannot be distributed;
						c. Spacecraft and Mission lost
							Catastrophic	Batteries charge and discharge do not happen nominally		4

31	Solar Panels	Produce power by solar radiations	Hardware break	Mechanical loads;
				Radiations effects;
				Off nominal temperatures;
				Overcurrents;
				Panels degradation
					Launch
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Power cannot be produced;
						b. Spacecraft cannot be powered;
						c. Mission lost
							Catastrophic	Power produced by solar panels is reduced or missing		4

32	Connectors	Connect EPS components to one another	Mechanical Connection failure	Mechanical loads	Launch	a. Connectors do not work; b. No data transmission among components; c. Loss of data	Critical			3

			Intermittant contact	Mechanical loads; Vibrations during launch	Launch	a. Connectors do not work; b. No data transmission among components; c. Intermittant loss of data	Critical			3
33	Activation switches	Prevent spacecraft activation during lauch	Mechanical Connection failure	Mechanical loads	Launch	a. Switches do not work; b. Spacecraft is powered in the launcher; c. Safety requirements are not met	Critical	Spacecraft is powered		3
			Intermittant contact	Mechanical loads; Vibrations during launch	Launch	a. Switches do not work; b. Spacecraft is intermittantly powered in the launcher; c. Safety requirements are not met	Critical			3

34	Electrical buses (3.3V, 5V, 12V, unregulated)	Distribute power	Loss of electrical protection	Radiations effects;
				Overcurrents;
				Off nominal temperatures
					Launch
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Protection circuits fail;
						b. Off nominal tension levels happen;
						c. Connected subsystems damaged
							Catastrophic	Power is not distributed across the spacecraft	All subsystems should have protection circuits at a local level	4

35	ADCS Processor	Manage ADCS operations and data	Hardware break	Mechanical loads;
				Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Launch
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. ADCS cannot execute onboard operations;
						b. Not possible to control the spacecraft;
						c. Mission lost
							Catastrophic	ADCS processor doesn not respond		4

			Information corruption	Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Instructions and/or data are corrupted;
						b. Attitude Determination algorithm does not converge and attuators do not work as expected;
						c. Not possible to control attitude
							Critical	Error detection algorithms identify faulty data packets	Error detection and correction algorithms shall be implemented	3

36	IMU	Measure angular velocities and attitude parameters	Hardware break	Mechanical loads;
				Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Launch
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Not possible to measure attitude telemetry;
						b. Attitude control accuracy reduced;
						c. Mission may be degradated
							Critical	IMU measurements are missing		3

37	Magnetometers	Measure magnetic field	Hardware break	Mechanical loads;
				Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Launch
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Not possible to asses magnetic environment;
						b. Not possible to reset IMU's gyroscopes and to use precisily magnetic torques;
						c. Not possible to detumble the spacecraft and attitude control performances are degradated
							Catastrophic	Magnetic measurements are no longer available		4

			Information corruption	Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Data are not accurate;
						b. Not possible to estimate spacecraft attitude;
						c. Attitude control performaces are degradated
							Catastrophic			4

			ElectroMagnetic Interferences	Radiotions effects; Magnetic Torques activity	Detumbling Mode Commissioning Mode Basic Mode Mission Mode Transmission Mode Safe Mode	a. Measumentes not accurate; b. Not possible to estimate spacecraft attitude; c. Attitude control performances are degradated	Major			2

38	Reaction Wheel 1	Generate and apply control torques	Hardware break	Mechanical loads;
				Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Launch
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Not possible to generate and apply control torques;
						b. Not possible to effectively control attitude;
						c. Mission degradated
							Catastrophic	Reaction Wheel does not regulate or generate the required control torque		4

39	Reaction Wheel 2	Generate and apply control torques	Hardware break	Mechanical loads;
				Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Launch
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Not possible to generate and apply control torques;
						b. Not possible to effectively control attitude;
						c. Mission degradated
							Catastrophic	Reaction Wheel does not regulate or generate the required control torque		4

40	Reaction Wheel 3	Generate and apply control torques	Hardware break	Mechanical loads;
				Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Launch
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Not possible to generate and apply control torques;
						b. Not possible to effectively control attitude;
						c. Mission degradated
							Critical	Reaction Wheel does not regulate or generate the required control torque		3

41	Reaction Wheel 4	Generate and apply control torques	Hardware break	Mechanical loads;
				Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Launch
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Not possible to generate and apply control torques;
						b. Not possible to effectively control attitude;
						c. Mission degradated
							Critical	Reaction Wheel does not regulate or generate the required control torque		3

42	Magnetic Torque Coil 1	Generate and apply control torques	Hardware break	Mechanical loads;
				Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Launch
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Not possible to generate and apply control torques and to desaturate the reaction wheels;
						b. Not possible to detumble the spacecraft and/or control attitude;
						c. Mission lost
							Catastrophic	Magnetic Torque Coil’s magnetic field is no longer measured;
								Magnetic Torque Coil cannot be used to desaturate the Reaction Wheels
										4

43	Magnetic Torque Coil 2	Generate and apply control torques	Hardware break	Mechanical loads;
				Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Launch
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Not possible to generate and apply control torques and to desaturate the reaction wheels;
						b. Not possible to detumble the spacecraft and/or control attitude;
						c. Mission lost
							Catastrophic	Magnetic Torque Coil’s magnetic field is no longer measured;
								Magnetic Torque Coil cannot be used to desaturate the Reaction Wheels
										4

44	Magnetic Torque Coil 3	Generate and apply control torques	Hardware break	Mechanical loads;
				Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Launch
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Not possible to generate and apply control torques and to desaturate the reaction wheels;
						b. Not possible to detumble the spacecraft;
						c. Mission lost
							Catastrophic	Magnetic Torque Coil’s magnetic field is no longer measured;
								Magnetic Torque Coil cannot be used to desaturate the Reaction Wheels
										4

45	Sun Sensors 1	Measure Sun vector	Hardware break	Mechanical loads;
				Radiations effects;
				Off nominal temperatures;
				Overcurrents;
				Sensor external degradation
					Launch
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Not possible to measure sun vector;
						b. Not possible to calculate attitude;
						c. Attitude Control performances degradated
							Catastrophic	Measurements lost		4

46	Sun Sensors 2	Measure Sun vector	Hardware break	Mechanical loads;
				Radiations effects;
				Off nominal temperatures;
				Overcurrents
				Sensor external degradation
					Launch
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Not possible to measure sun vector;
						b. Not possible to calculate attitude;
						c. Attitude Control performances degradated
							Catastrophic	Measurements lost		4

47	Sun Sensors 3	Measure Sun vector	Hardware break	Mechanical loads;
				Radiations effects;
				Off nominal temperatures;
				Overcurrents
				Sensor external degradation
					Launch
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Not possible to measure sun vector;
						b. Not possible to calculate attitude;
						c. Attitude Control performances degradated
							Catastrophic	Measurements lost		4

48	Sun Sensors 4	Measure Sun vector	Hardware break	Mechanical loads;
				Radiations effects;
				Off nominal temperatures;
				Overcurrents
				Sensor external degradation
					Launch
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Not possible to measure sun vector;
						b. Not possible to calculate attitude;
						c. Attitude Control performances degradated
							Catastrophic	Measurements lost		4

49	Connectors between Magnetic Torques and ADCS board	Connect Magnetic Torques to ADCS board	Mechanical Connection Failure	Mechanical loads; Vibrations	Launch	a. Affected attuator does not work; b. Affected attuator cannot control attitude; c. Attitude control performances degradated	Critical			3

			Intermittant contact	Mechanical loads; Vibrations	Launch	a. Affected attuator does not work continously; b. Affected attuator controls attitude intermittatly; c. Attitude control performances degradated	Major			2
50	Connectors between Reaction Wheels and ADCS board	Connect Reaction Wheels to ADCS board	Mechanical Connection Failure	Mechanical loads; Vibrations	Launch	a. Affected attuator does not work; b. Affected attuator cannot control attitude; c. Attitude control performances degradated	Critical			3

			Intermittant contact	Mechanical loads; Vibrations	Launch	a. Affected attuator does not work continously; b. Affected attuator controls attitude intermittatly; c. Attitude control performances degradated	Major			2

	UHF - Antenna	Generate electromagnetic signal	Hardware break	Mechanical loads;
				Radiations effects;
				Debris collision;
				Overcurrents
					Launch
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Antenna cannot generate signal;
						b. Not possible to communicate with ground;
						c. Mission lost
							Catastrophic	Communication in UHF band does not happen		4

			Hardware degradation	Radiations effects;
				Cleanliness degradation
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Antenna performances degradated;
						b. Noisy signal;
						c. Communication performances degradated
							Major	Noisy or weak signal is received at the ground station		2

			Interferances	Presence of other signals	Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Signal is disturbed;
						b. Telemetry/telecommands packet degradated;
						c. N/A
							Minor	Noisy or weak signal is received at the ground station		1

51	Coaxial cable	Connect UHF-antenna to UHF-board	Hardware break	Mechanical loads	Launch Detumbling Mode	a. Connection between antenna and radio lost; b. Not possible to communicate; c. Mission lost	Catastrophic	Data packet are not transmitted to ground through UHF antenna		4

52	UHF - Modem	Modulate and demodulate signal	Hardware break	Mechanical loads;
				Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Launch
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Not possible to modulate and demodulate signal;
						b. Not possible to communicate;
						c. Mission lost
							Catastrophic	UHF signal cannot be generated		4

			Information Corruption	Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Instructions/ data are corrupted;
						b. Inconsistent signal;
						c. Telemetry/telecommands packet lost
							Minor	Error detection algorithms identify faulty data packets	Error detection and correction algorithms shall be implemented	1

53	UHF – Radio module	Establish communication	Hardware break	Mechanical loads;
				Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Launch
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Not possible to establish communication;
						b. Not possible to communicate;
						c. Mission lost
							Catastrophic	Telemetry does not arrive to ground station through UHF band		4

			Information corruption	Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Instructions/ data are corrupted;
						b. Inconsistent signal;
						c. Telemetry/telecommands packet lost
							Minor	Error detection algorithms identify faulty data packets	Error detection and correction algorithms shall be implemented	1

			High Power Amplifier Switches fail	Mechanical loads;
				Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Launch
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Not possible to turn off and on the HPA;
						b. Increased power consumption/not possible to transmit;
						c. Mission lost
							Catastrophic			4

54	UHF - Filtering stages	Filter signal frequencies	Hardware break	Mechanical loads;
				Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Launch
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Not possible to correctly filter the signal;
						b. Very noisy signal;
						c. Communication performances degradated
							Major	Signal is noisy		2

55	S-Antenna	Generate electromagnetic signal	Hardware break	Mechanical loads;
				Radiations effects;
				Debris collision;
				Overcurrents
					Launch
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Antenna cannot generate signal;
						b. Not possible to transmit mission data;
						c. Mission degradated
							Critical	Communication in UHF band does not happen		3

			Hardware degradation	Radiations effects;
				Cleanliness degradation
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Antenna performances degradated;
						b. Noisy signal;
						c. Communication performances degradated
							Major	Noisy or weak signal is received at the ground station		2

			Interferences	Presence of other signals	Transmission Mode	d. Signal is disturbed; e. Mission data packet degradated; f. N/A	Minor	Noisy or weak signal is received at the ground station		1
56	Coaxial cable	Connect S-antenna to S-board	Hardware break	Mechanical loads	Launch Detumbling Mode	a. Connection between antenna and radio lost; b. Not possible to transmit mission data; c. Mission degradated	Critical	Data packet are not transmitted to ground through S antenna		3

57	S - Modem	Modulate and demodulate signal	Hardware break	Mechanical loads;
				Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Launch
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Not possible to modulate and demodulate signal;
						b. Not possible to transmit mission data;
						c. Mission degradated
							Critical	S signal cannot be generated		3

			Information Corruption	Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Instructions/ data are corrupted;
						b. Inconsistent signal;
						c. Mission data packet lost
							Minor	Error detection algorithms identify faulty data packets	Error detection and correction algorithms shall be implemented	1

58	S – Radio module	Establish communication	Hardware break	Mechanical loads;
				Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Launch
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Not possible to establish communication;
						b. Not possible to transmit mission data;
						c. Mission degradated
							Critical	Telemetry does not arrive to ground station through S band		3

			Information corruption	Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Instructions/ data are corrupted;
						b. Inconsistent signal;
						c. Mission data packet lost
							Minor	Error detection algorithms identify faulty data packets	Error detection and correction algorithms shall be implemented	1

			High Power Amplifier Switches fail	Mechanical loads;
				Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Launch
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Not possible to turn off and on the HPA;
						b. Increased power consumption/not possible to transmit;
						c. Mission lost
							Catastrophic			4

59	S - Filtering stages	Filter signal frequencies	Hardware break	Mechanical loads;
				Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Launch
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Not possible to correctly filter the signal;
						b. Very noisy signal;
						c. Communication performances degradated
							Major	Signal is noisy		2

60	Rails + main panel (as one component) (configuration 1 TBC)	Contain and protect subsystem	Hardware deformation	Inertial mechanical loads	Launch	a. Mechanical interfaces damaged; b. Susceptibility to thermal loads increased; c. Subsystems or equipments may be damaged	Critical			3

			Vibrations	Inertial mechanical loads; Vibrations	Launch	a. Vibrations are transmitted to other subsystems in the spacecraft; b. Subsystems can be damaged (solar panels may be detached, locking cable may initiate deployment prematurarly); c. Spacecraft may be damaged	Catastrophic			4
61	Main panels (laterals)	Substain shear loads and protect subsystem	Hardware deformation	Inertial mechanical loads	Launch	a. Mechanical interfaces damaged; b. Connected internal hardware may be displaced; c. N/A	Minor			1

			Vibrations	Inertial mechanical loads; Vibrations	Launch	a. Vibrations may be propagated; b. Solar panels may be detached; c. Spacecraft performances are degraded	Major			2
62	Top panel	Protect subsystem	Hardware deformation	Inertial mechanical loads	Launch	a. Mechanical interfaces damages; b. Sun sensor/solar panels may be detached; c. Spacecraft performances bay be degraded	Minor			1
			Vibration	Inertial mechanical loads; Vibrations	Launch	a. Mechanical interfaces damaged; b. Sun sensor/solar panels may be detached; c. Spacecraft performances bay be degraded	Minor			1

63	Bottom panel	Protect subsystem	Hardware deformation	Inertial mechanical loads	Launch	a. Bottom panel deformed;
						b. Payload and/or antenna misallineament;
						c. Spacecraft performances degraded
							Critical			3

			Vibrations	Inertial mechanical loads; Vibrations	Launch	a. Vibrations are propagated to connected hardware; b. Antenna deployment locking cable may be damaged; c. Antenna deploys incorrectly	Catastrophic			4

64	Crossmembers	Substain internally subsystem	Hardware deformation	Inertial mechanical loads	Launch	a. Crossmembers deformes; b. Connected hardware (payload, thermal interfaces material and boards) may get misalligned or detached; c. Subsystem performances degraded	Major			2
			Vibrations	Inertial mechanical loads; Vibrations	Launch	a. Vibrations are propagated; b. Connectors may be detached; c. Connected hardware may bishave	Critical			3
65	Frame (configuration 2 TBC)		Hardware deformation	Inertial mechanical loads	Launch	a. Mechanical Interfaces with other structural elements damaged; b. Joints and screws may be detached; c. Structural integraty damaged	Critical			3

			Vibrations	Inertial mechanical loads; Vibrations	Launch	a. Vibrations are propagated; b. Connected hardware (solar panels, deployment mechanism) may be damaged; c. SPacecraft performances degraded	Critical			3

66	Kapton	Thermal insulation	Degradation	Outgassing;
				Radiations affects;
				Contaminants
					Launch;
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Thermal Control performances degraded;
						b. Off nominal temperatures may be experienced/payload optics may be contaminated;
						c. Spacecraft performances degraded
							Minor			1

			Detachment	Outgassing;
				Radiations affects;
				Contaminants;
				Mechanical loads
					Launch;
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Thermal Control performances degraded;
						b. Off nominal temperatures may be experienced /detached katpon may interfere with external hardware;
						c. Spacecraft performances degraded
							Minor			1

67	Thermal straps	Absorb and transfer heat	Detachment	Mechanical loads; Vibrations	Launch; Detumbling Mode Commissioning Mode Basic Mode Mission Mode Transmission Mode Safe Mode	a. Thermal strap cannot transfer heat/thermal strap can be detached; b. Thermal Control performances degraded; c. Subsystem performances may be degraded	Minor			1

			Hardware break	Off nominal temperatures;
				Mechanical loads;
				Vibrations
					Launch;
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Thermal strap cannot transfer heat/thermal strap can be detached;
						b. Thermal Control performances degraded;
						c. Subsystem performances may be degraded
							Minor			1

68	Thermal Interface Material	Thermal insulation/conduction	Hardware degradation	Off nominal temperatures;
				Radiations effects;
				Material wearout;
				Vibrations;
				Thermal cycles
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Thermal conductivity may be degraded;
						b. Thermal Control performances are degraded;
						c. Subsystem performances may be degraded
							Minor			1

69	Paintings/Coatings	Reflect/absorb radiative heat	Degradation	Material degradation;
				Contaminants;
				Radiations effects;
				Material wearout;
				Vibrations;
				Thermal cycles
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Thermal Control performances degraded;
						b. Pieces of paintings may detach and contaminate payload optics;
						c. Spacecraft performances degraded
							Minor			1

70	Locking cable	Block antenna in undeployed configuration	Hardware damage	Mechanical loads;
				Vibrations;
				Off nominal temperatures
					Launch
					Detumbling mode
						a. Deployment mechanism is damages and/or activated at the wrong time;
						b. Antenna may be damaged or incorrectly deployed/spacecraft may interfere with launcher;
						c. Communication performances degraded
							Critical			3

71	Burning resistance	Activate deployment mechanism	Hardware detachment	Mechanical loads;
				Vibrations;
				Overcurrents;
				Off nominal temperatures
					Launch
					Detumbling mode
						a. Component is detached and may interfere with other elements in the spacecraft;
						b. Not possible to deploy antenna;
						c. Communication performances degraded
							Critical			3

			Off nominal operation	Mechanical loads;
				Vibrations;
				Overcurrents;
				Off nominal temperatures
					Launch
					Detumbling mode
						a. Burning resistance does not burn the locking cable;
						b. Antenna in not correcly deployed;
						c. Deployment may last much longer than supposed
							Minor			1

72	Transistor NMOS/CMOS	Regulate activation and deactivation of the burning resistance	Off nominal operation	Mechanical loads;
				Vibrations;
				Overcurrents;
				Off nominal temperatures;
				Radiations effects
					Launch
					Detumbling mode
						a. Transistor does not open or close the circuit as expected;
						b. If circuit stays open, antenna cannot be deployed/if circuit stays closed, it endlessly dissipates heat;
						c. Communication performances are degraded/components near the circuit may be thermally damaged and EPS behaviour is affected by the continuous power absorption
							Critical			3

73	Subchassis (configuration 2)	Keep the antenna folded	Hardware detachment	Mechanical loads; Vibrations	Launch	a. Component is detached by spacecraft; b. Antenna is lost and cannot be deployed; c. Communication performances degraded	Critical			3
74	Mounting screws	Hold deployment elements and structure together	Hardware failing	Mechanical loads; Vibrations	Launch	a. Deployment mechanism is detached by spacecraft; b. Locking cable is prematurely activated; c. Antenna may be damaged	Minor			1
75	Secure parts	Keep the mechanism in place	Hardware failing	Mechanical loads; Vibrations	Launch	a. Component is detached by spacecraft; b. Antenna is lost and cannot be deployed; c. Communication performances degraded	Minor			1

76	Camera	Collect mission data	Hardware degradation	External contaminants	Launch Detumbling Mode Commissioning Mode Basic Mode Mission Mode Transmission Mode Safe Mode	a. Unclear images taken; b. Quality of mission data compromised; c. Mission degraded	Major	Pictures are unclear		2

			Hardware break	Vibrations;
				Mechanical loads;
				Off nominal temperatures;
				Overcurrents
					Launch
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Impossible to take images;
						b. Missing mission data;
						c. Mission severely compromised
							Critical	Pictures cannot be taken		3

77	Payload Processing Unit	Process mission data onboard	Information corruption	Radiations effects;
				Off nominal temperatures;
				Overcurrents
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Some mission data are corrupted;
						b. It is not possible to process that data;
						c. Data packet lost
							Minor	Detection algorithms recognize faulty data packets	Error detection and correction algorithms shall be implemented	1

78			Hardware break	Vibrations;
				Mechanical loads;
				Off nominal temperatures;
				Overcurrents
					Launch
					Detumbling Mode
					Commissioning Mode
					Basic Mode
					Mission Mode
					Transmission Mode
					Safe Mode
						a. Processing algorithms are no longer available;
						b. It is not possible to process mission data on board;
						c. Mission degraded
							Major	Payload Processor crashes		2