Methods for dependability analysis of small satellite missions

POLITECNICO DI TORINO

Dottorato di Ricerca in Ingegneria Aerospaziale

XXVII Ciclo

Methods for dependability analysis of small-satellite missions

Tutors
Dr. Sabrina Corpino
Prof. Sergio Chiesa

Candidate
Gerard Obiols Rabasa

SUMMARY

The use of small-satellites as platforms for fast-access to space with relatively low cost has increased in the last years. In particular, many universities in the world have now permanent hands-on education programs based on CubeSats. These small and cheap platforms are becoming more and more attractive also for other-than-educational missions, such as for example technology demonstration, science application, and Earth observation. This new objectives require the development of adequate technology to increase CubeSat performances. Furthermore, it is necessary to improve mission reliability.

The research aims at studying methods for dependability analysis conducted by small satellites. The attention is focused on the reliability, as main attribute of the dependability, of CubeSats and CubeSats missions.

The work has been structured in three main blocks. The first part of the work has been dedicated to the general study of dependability from the theoretical point of view. It has been studied the dependability attributes, the threads that can affect the dependability of a system, the techniques that are used to mitigate the threads, parameters to measure dependability, and models and techniques for dependability modelling.

The second part contains a study of failures occurred during CubeSats missions in the last ten years and their observed reliability evaluation have been conducted. In order to perform this analysis a database has been created. This database contents information of all CubeSats launched until December 2013. The information has been gathered from public sources (i.e. CubeSat projects webs, publications on international journals, etc.) and contains general information (e.g. launch date, objectives) and data regarding possible failures. All this information is then used to conduct a quantitative reliability analysis of these missions by means of non-parametric and parametric methods, demonstrating that these failures follow a Weibull distribution.

SUMMARY

In the third section different methods, based on the concept of fault prevention, removal and tolerance, have been proposed in order to evaluate and increase dependability, and concretely reliability, of CubeSats and their missions. Concretely, three different methods have been developed: 1) after an analysis of the activities conducted by CubeSat's developers during whole CubeSat life-cycle, it has been proposed a wide range of activities to be conducted during all phases of satellite's life-cycle to increase mission rate of success, 2) increase reliability through CubeSats verification, mainly tailoring international ECSS standards to be applied to a CubeSat project, 3) reliability rising at mission level by means of implementing distributed mission architectures instead of classical monolithic architectures.

All these methods developed in the present PhD research have been applied to a real space projects under development at Politecnico di Torino within e-st@r program. The e-st@r program is being conducted by the CubeSat Team of the Mechanical and AeroSpace Engineering Department. Concretely, e-st@r-I, e-st@r-II, and 3STAR CubeSats have been used as test cases for the proposed methods.

Moreover, part of the present research has been conducted within an internship at the European Space research and Technology Centre (ESTEC) of the European Space Agency (ESA) at Noordwijk (The Netherlands). In particular, the partially realisation of the CubeSats database, the analysis of activities conducted by CubeSat developers and statement of activities for mission rate of success increase have been conducted during the internship.

SOMMARIO

L'utilizzo di piccoli satelliti come piattaforme che acconsentono a un rapido accesso allo spazio a costo contenuto è cresciuto negli ultimi anni. In particolare, molte università hanno stabilito, negli ultimi anni, programmi educativi basati su CubeSats. Tuttavia, queste piccole ed economiche piattaforme stanno diventando attraente per missioni diverse da quelle con obiettivi puramente educativi, come ad esempio dimostrazione tecnologica, applicazioni scientifiche e di osservazione della Terra. Questi nuovi obiettivi richiedono lo sviluppo di un'adeguata tecnologia per incrementare le prestazioni dei CubeSats. Inoltre, è necessario migliorare l'affidabilità di questi satelliti e delle loro missioni.

L'obiettivo principale di questa tesi è identificare i possibili metodi per valutare e migliorare gli attributi di *dependability* (affidabilità, disponibilità, manutenibilità e sicurezza) dei piccoli satelliti e le loro missioni, e in particolare da CubeSats.

Il lavoro è strutturato in tre blocchi principali. La prima parte del lavoro è stata dedicata allo studio generale della *dependability* da un punto di vista teorica, analizzando gli attributi che la compongono, le minacce che possono violare la *dependability* di un sistema, le tecniche utilizzate per tentare di ovviare a tali minacce, i suoi parametri di misura e i modelli e tecniche di modellizzazione della *dependability*.

La seconda parte si focalizza nello studio dei guasti avvenuti sui CubeSat lanciati nell'ultimo decennio e dell'affidabilità osservata in questi sistemi. Per condurre quest'analisi è stato creato un database con tutti i CubeSat lanciati fino dicembre 2013. L'informazione, ricavata da fonti pubbliche (internet, pubblicazioni in riviste internazionali, etc.), riguarda sia argomenti generali (data di lancio, obiettivo, etc.) sia dati su relativi guasti. Quest'ultima informazione è dopo usata per realizzare una valutazione quantitativa dell'affidabilità di queste missioni tramite analisi non-parametrici e parametrici, dimostrando che i guasti seguono una distribuzione di Weibull.

SOMMARIO

Nella terza sezione diversi metodi, basati sui concetti di *fault prevention*, *removal* e *tolerance*, sono proposti per incrementare la *dependability*, e in particolare l'affidabilità, di CubeSat e le loro missioni. In particolare, tre diversi metodi sono stati sviluppati: 1) dopo un'analisi delle attività realizzate durante i cicli di vita dei CubeSat da parte degli sviluppatori, si propongono delle attività da implementare durante tutte le fasi di progetto per aumentare la possibilità di un successo della missione, 2) aumentare l'affidabilità tramite la verifica dei CubeSat, adattando la normativa internazionale ECSS per essere applicata ai CubeSat, 3) aumentare l'affidabilità a livello di missione tramite l'implementazione di architetture distribuite rispetto alle classiche monolitiche.

I diversi metodi sviluppati in questa tesi di dottorato sono stati applicati a progetti reali in sviluppo al Politecnico di Torino dentro l'ambito del programma e-st@r condotto dal CubeSat Team del Dipartimento di Ingegneria Meccanica e AeroSpaziale. In particolare, i CubeSat e-st@r-I, e-st@r-II e 3STAR sono stati usati come *test case* dei tre diversi metodi proposti.

Inoltre, parte della ricerca presentata in questa tesi è stata condotta nell'ambito di un periodo di ricerca presso l'*European Space Research and Technology Centre* dell'Agenzia Spaziale Europea in Noordwijk (Paesi Bassi). Concretamente, è stato completato il database sui CubeSat lanciati, l'analisi delle attività condotte dagli sviluppatori di CubeSat e l'individuazione delle possibili azioni da implementare durante il ciclo di vita di questi satelliti per aumentare il tasso di successo delle loro missioni.

To my parents Conxita and Guillem

To my brother Marc

ACKNOWLEDGMENTS

The acknowledgements are probably the most difficult chapter to be written in the whole thesis. There are no useful references to deal with this section. I wish I will not forget anybody… I wish I will state all of you in the correct order… Anyhow, my sincere thanks to all of you.

To Dr. Sabrina Corpino, for introducing me in the space field and into the research world. To always trust in me and to encourage me to follow on even in the hard moments; to make me grow professional and personally. Thank you so much! To Prof. Sergio Chiesa, for his valuable professional and personal lessons.

To Eng. Piero Galeone, for his support on my research and to allow me to conduct my internship in ESA/ESTEC. To Eng. Charles Lahorgue, for his useful advises during my stage in ESTEC. Thanks to both for your great effort on guiding me in my research.

To all colleagues and friends of the CubeSat Team and Politecnico di Torino, especially to Nicole, Fabrizio, Fabio, Raffaele, Lorenzo, Guido and Maria Antonietta.

Thank you very much to all my colleagues and friends of ESTEC, for all good times we spend together, and specially all colleagues from the Education Office. Many thanks also to my friends in Italy and in La Seu, for your support and encouragement.

Finally, I would like to thank the people who always supported me and make me to reach this milestone in my life. To my mum Conxita and my dad Guillem who, with their support and love to me, help me to achieve all my dreams. To my brother Marc and my sister-in-law Lucia, for being always on the other side of the phone, for your valuable advises. Without you, I never could finish my PhD.

Thank you!

LIST OF FIGURES

LIST OF FIGURES

LIST OF FIGURES

LIST OF TABLES

NOTATIONS

ACRONYMS

A	Analysis
A-ADCS	Active Attitude Determination and Control Subsystem
ADCS	Attitude Determination and Control Subsystem
AIV	Assembly, Integration and Verification
ANS	Astronomische Nederlandse Satelliet
AOCS	Attitude and Orbit Control System
AR	Acceptance Review
ASAP	Ariane Structure for Attached Payloads
ASSET	AeroSpace Systems Engineering Team
BFT	Basic Functional Test
Cal Poly	California Polytechnic State University
CA	Criticality Analysis
CAD	Computer-Aided Design
CDR	Critical Design Review
CDS	CubeSat Design Specification
CoG	Centre of Gravity
COMSYS	Communication Subsystem
COTS	Commercial-Off-The-Shelf
CRECTEALC	Centro Regional de Enseñanza de Ciencia y Tecnología del Espacio para America Latina y el Caribe
CVCM	Collected volatile Condensable Materials
CW	Continuous Wave
DIMEAS	Dipartimento di Ingegneria Meccanica e AeroSpaziale
DoD	Department of Defence
DR	Decommissioning Review

NOTATIONS

e-st@r	Educational SaTellite at politecnico di toRino
ECSS	European Cooperation on Space Standardization
EMC	ElectroMagnetic Compatibility
EPS	Electrical Power Subsystem
ESA	European Space Agency
ESD	ElectroStatic Discharge
ESTEC	European Space Research and Technology Centre
ET	Event Tree
ETA	Event Tree Analysis
FFT	Full Functional Test
FMEA	Failure Modes and Effects Analysis
FMECA	Failure Modes, Effects and Criticality Analysis
FRR	Flight Readiness Review
FT	Fault Tree
FTA	Fault Tree analysis
FYS!	Fly Your Satellite!
GCS	Ground Control Station
GDP	Gross Domestic Product
GENSO	Global Educational Network for Satellite Operations
GEOID	GENSO Experimental Orbital Initial Demonstration
Hi-Rel	High-Reliability
HumSat	Humanitarian Satellite
I	Inspection
IE	Initiating Event
IST	Integrated System Test
LEO	Low Earth Orbit
MCR	Mission Concept Review
MDR	Mission Definition Review
MGCS	Mobile Ground Control Station
MLE	Maximum Likelihood Estimator

NOTATIONS

MoI	Moment of Inertia
MT	Mission Test
MTTF	Mean-Time-To-Failure
MTTR	Mean-Time-To-Repair
NASA	National Aeronautics and Space Administration
OBC	On-Board Computer
OBDH	On-Board Data Handling
ORR	Operational Readiness Review
OSCAR	Orbiting Satellite Carrying Amateur Radio
P-POD	Poly-PicoSatellite Orbital Deployer
p.d.f.	Probability Distribution Function
PA	Product Assurance
PCB	Printed Circuit Board
PDR	Preliminary Design Review
PRA	Probabilistic Risk Assessment
PRR	Preliminary Requirements Review
QR	Qualification Review
RAMS	Reliability, Availability, Maintainability and Safety
RBD	Reliability Block Diagram
RML	Recovered Mass Loss
RoD	Review of Design
S/N	Signal-To-Noise
SDR	System Definition Review
SEL	Single Event Latch-up
SEU	Single Event Upset
SMAD	Space Mission Analysis and Design
SPOT	Satellite Pour l'Observation de la Terre
SRR	System Requirements Review
SRRe	Shipment Readiness Review
STARLab	Systems and Technologies for Aerospace Research Laboratory

NOTATIONS

T	Test
TML	Total Mass Loss
TV/TC	Thermal-Vacuum/Thermal-Cycling
UNOOSA	United Nations Office for Outer Space Affairs
UV	Ultra-Violet
VCD	Verification Control Document
VEGA	Vettore Europeo di Generazione Avanzata

SYMBOLS

$A_{(t)}$	Availability function of time
θ	Characteristic life of Weibull distribution
$f_{(t)}$	Density function of time until failure
$D_{(ti)}$	Dispersion of reliability around $\hat{R}_{(t)}$
x_n	Estimation of $f_{(r)}$ equation for Newton-Raphson Method
p_i	Estimator of the conditional probability of failing in interval I, given that a unit enters this interval in the Kaplan-Meier estimator
λ	Failure rate
m	Number of intervals in the Kaplan-Meier estimator
n_i	Number of operational units right before t_i
d_j	Number of units that failed in the j-th interval $(t_{j-1},t_j]$
r_j	Number of units that survive interval j and are right-censored at t_j
$R_{(t)}$	Reliability function of time
r	Root of $f_{(r)}$ equation for Newton-Raphson Method
γ	Shape parameter of Weibull distribution
$f_{(r)}$	Wee-behaved function for Newton-Raphson Method

CONTENTS

CONTENTS

CONTENTS

1

INTRODUCTION

Space missions are evolving continuous and rapidly. Traditional high mass and cost spacecraft are being overpassed by new small-satellite missions. Actually, the main objective is to create smaller, lower-cost, more responsive systems capable of doing more and doing it more quickly and at lower cost. This concept led to assure that it is necessary to reinvent space as described by James R. Wertz in Space Mission Engineering: The New SMAD. He defined "reinventing space" as the use of modern technology and old-fashioned drive, determination, and some willingness to accept risk to do much more, much faster, with fewer resources.

Gathering this concept, new missions conducted with small-satellites are being developed all around the World. The use of this type of spacecraft gives different advantages:

- Reduce cost
- Reduce mission risk (i.e. risk as the product of reliability and the cost of failure. Reducing cost of failure, the mission risk is reduced)
- Possibility to develop different mission architectures that are not feasible with traditional satellites
- Use state-of-the-art technologies for future applications
- Faster responsive missions

The boost on fast-delivery and low-cost projects requirements shall be combined with the achievement of certain level of performances to correctly conduct the designed missions.

Traditionally, the use of small and relatively simply satellites has been adopted to reduce project costs and schedule. However, it is said that this type of satellites, and particularly for CubeSats, are characterised to be affected by a low reliability and hence, an unacceptable mission rate of success. The cause to be the origin of these events has been usually assumed to be the academic field (and hence, education as main objective) where this type of spacecraft

are being developed, focusing the attention on the nominal design without considering possible non-nominal mission. However, in the last years the interest on CubeSats for other-than-educational objectives led the need to increase their dependability to achieve an acceptable mission rate of success.

Nevertheless, all these evaluations are being made from general observation of small-satellite missions but no precise study on CubeSat's failures, reliability analysis and methods to increase their dependability is present in literature.

Hence, the objective of the present study is to fill this gap in the study of dependability and its attributes, and identify different methods to increase them for missions developed with small-satellites and, in particular, by CubeSats. The present research framework is included in the activity of the CubeSat Team of the Politecnico di Torino within the ASSET group. The AeroSpace Systems Engineering Team group of the Mechanical and AeroSpace Engineering Department (DIMEAS) deals with design and manufacturing of small-satellites since many years. Within this group, the CubeSat Team is in charge of design and develop CubeSats as well as new methodologies in support of these activities.

1.1 Thesis lay-out

As previously stated, the objective of the present research study is to establish methods for dependability analysis to be applied to small-satellite missions. The final goal is to use the studied methods to improve small-satellite (and in particular CubeSat) missions dependability to assure an acceptable mission rate of success. Concretely, the efforts are concentrated in three main fields: 1) increase satellite's reliability by conducting good practices during the whole life-cycle, 2) increase satellite's reliability by applying tailored international standards, and 3) increase reliability from the mission point of view. Table 1 shows a block diagram of the thesis lay-out.

1.1 Thesis lay-out

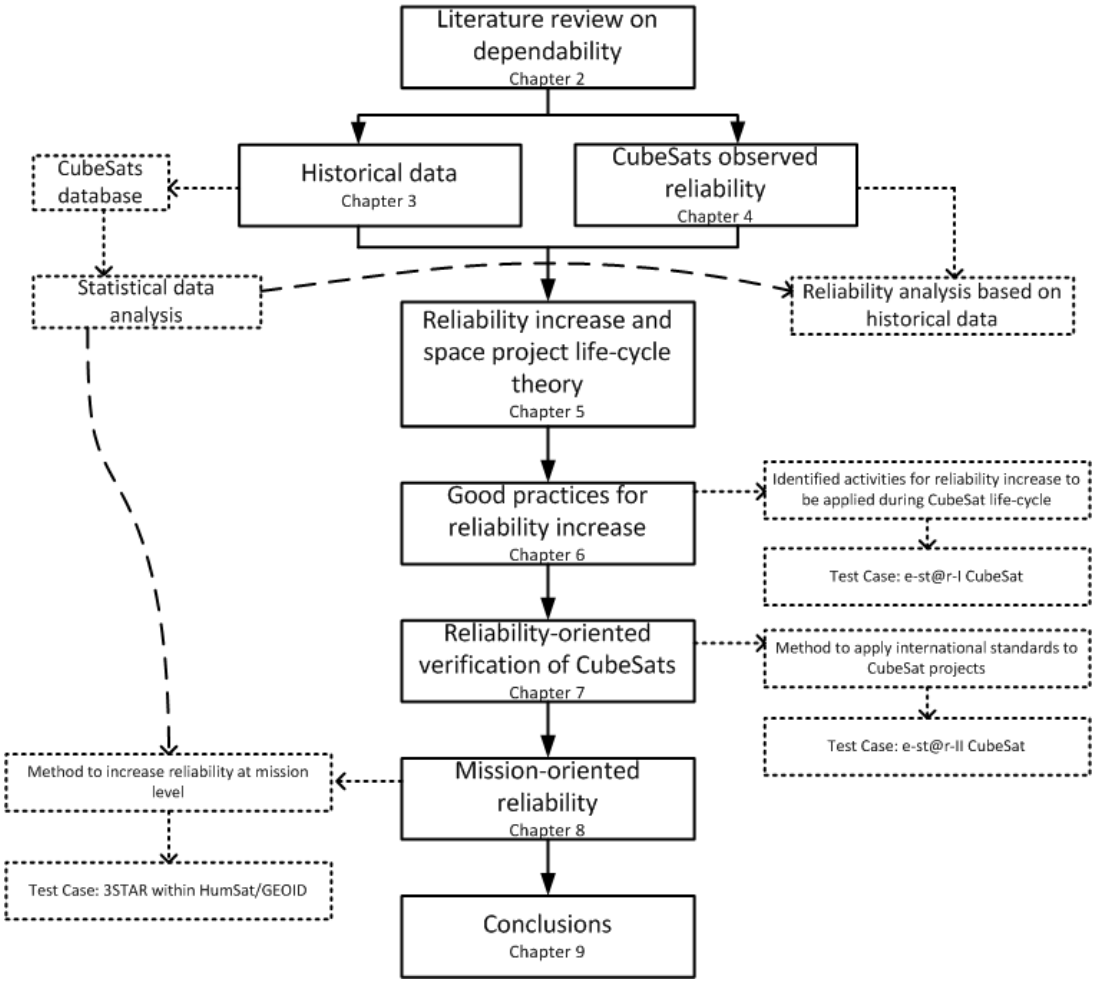


Figure 1: Thesis lay-out block diagram

In Chapter 2 basics on dependability are detailed. The concept of dependability is presented together with its attributes from which it is evaluated, the events that affect the system reducing its dependability (i.e. threads) and the way to make a system more dependable (i.e. means). Moreover, measurements to assess dependability attributes are also explained. Finally, dependability models and techniques are discussed in order to obtain a wide background for further steps conducted in the next chapters.

The evolution of space systems is assessed in Chapter 3. The constant evolution of space sector, requiring better results while keeping contained costs, led to think on small-satellites as a key-systems to develop today the future's missions. A general overview is provided regarding the constant miniaturisation observed during the last decades. Going in-deep to this aspect, a

1 INTRODUCTION

survey and assessment of all on-orbit CubeSats is conducted and detailed. The chapter is concluded with an analysis of observed failures and their main causes.

In Chapter 4 we conducted an analysis of CubeSat missions' reliability. The target is to obtain the reliability of CubeSats that are already on-orbit. We used two different methods: non-parametric and parametric. To conduct non-parametric analysis, Kaplan-Meier estimator is used, taking into account censoring data with staggered entries. Parametric analysis has been conducted by means of Weibull plot and Maximum Likelihood Estimation techniques. Finally, we conducted a comparison among the methods results.

An analysis of CubeSat's life-cycle is conducted in Chapter 5. This assessment is used to identify the main three ways to increase reliability of CubeSats and related missions. Moreover, we provide an explanation of space systems life-cycle phases and related activities. Focusing the attention on verification phase, we explain the different verification methods commonly used for requirements verification.

In Chapter 6 we analyse the activities conducted by CubeSat developers during their CubeSat's life-cycle. The gathered inputs were used to establish good practices to be applied during development, manufacturing, verification and operations of CubeSats to increase their mission rate of success. This activity was conducted within an internship in the Education Office of ESA/ESTEC under supervision of dependability section expert.

Verification phase activities of space system life-cycle are analysed and assessed in Chapter 7. The study proposes the implementation and tailoring of international standards to fit CubeSat projects requirements. In particular, tailoring of ECSS is proposed to address fast-delivery and low-cost CubeSats verification campaign in order to increase its reliability. E-st@r-II CubeSat is then used as case study for the present analysis.

New approach to assure acceptable reliability is stated in Chapter 8. In particular, the possibility to increase mission rate of success by increasing reliability at mission level instead of at system level. Different mission architectures are evaluated in terms of reliability and mean-time-to-failure. The proposed method is thus applied to 3STAR CubeSat as part of HumSat/GEOID program as a case study.

1.1 Thesis lay-out

Chapter 9 presents the conclusions of the present research, were contributions of this thesis and obtained results are summarised.

2

BASICS ON DEPENDABILITY

Dependability of a system is its ability to deliver its intended specified level of services to the end users so that they can justifiably relay on and trust the services provided by the system.

Practically, the concept of dependability is an integration of attributes (which evaluation represents a way to assess the dependability of a system), threats (i.e., events that affect in someway the dependability of a system) and means (i.e., the way in which the dependability of a system is increased).

The origin of dependability concept is set during the first generation of electronic computers (late 1940's to mid-50) where practical techniques were employed to improve their reliability to cope with components unreliability. The increase of interest on fault tolerance and systems reliability during 1960's and 1970's led to the study of dependability of an encompassment, not only of reliability, but also other attributes. In 1980's Jean-Claude Laprie started to use *dependability* as a concept for study of fault tolerance and systems reliability without the need to extend the concept of reliability. The work was synthesized by the same author in 1992 in the book *Dependability: Basic Concepts and Terminology*

2.1 Dependability attributes

As already specified above, the dependability is evaluated with the assessment of different attributes (see Table 1). These attributes are: reliability, availability, maintainability, safety (i.e., the so called RAMS), integrity and confidentiality, which are usually referred to computing systems but they could be extend to space systems (as detailed later on). The concurrent existence of availability, integrity and confidentiality is represented by the security attribute.

Table 1: Dependability and security attributes tree and definitions

Dependability attributes	**R**eliability	Reliability *R(t)* of a system at time *t* is the probability that the system operates without a failure in the interval *[0,t]*, given that the system was performing correctly at time 0. Thus, reliability is a measure of the continuous delivery of correct service
	Availability	Availability *A(t)* of a system at time *t* is the probability that the system is functioning correctly at the instant of time *t*
	Maintainability	Maintainability *M(t)* of a system is a measure of the ability of the system to undergo maintenance or to return to normal operation after a failure
	Safety	Safety *S(t)* of a system at time *t* is the probability that the system either performs its function correctly or discontinues its operation in a fail-safe manner in the interval *[0,t]*, given that the system was operating correctly at time 0. Thus, safety can be considered as an extension of reliability, namely reliability with respect to failures that may create safety hazards
	Integrity	Integrity of a system is the probability that errors or attacks will not lead to damages to the state of the system, including data, code, etc.
	Confidentiality	Confidentiality of a system is a measure of the degree to which the system can ensure that an unauthorized user will not be able to understand protected information in the system

Security

2.2 Dependability threads

Threads are events that affect the system reducing its dependability. This dependability impairment is usually defined in terms of faults, errors, or failures. A common feature of the three terms is that they give us a warning that something in the system is going wrong. The differences among the three threads it that, in the case of a fault, the problem occurred on the physical level; in the case of an error, the problem occurred on the computational level; in the case of a failure, the problem occurred on a system level. The definitions of these threads are:

- A **fault** is a physical defect, imperfection, or flaw that occurs in some hardware or software component. For example, a short circuit between two adjacent interconnects or a broken pin.

- An **error** is a deviation from correctness or accuracy in computation, which occurs as a result of a fault. Errors are usually associated with incorrect values in the system state. For example, a circuit or a program computed an incorrect value, or incorrect information was received while transmitting data.
- A **failure** is a non-performance of some action which is due or expected. A system is said to have a failure if the service it delivers to the user deviates from compliance with the system specification for a specified period of time. A system may fail either because it does not act in accordance with the specification, or because the specification did not adequately describe its function.

2.3 Dependability means

Generally, there are two ways to approach to obtain a dependable product. The easiest approach consists in first designing the system, and then making it as much dependable as required. This approach is expensive and ineffective; if dependability is taken into account only in the latest phases of designing, any design modification will lead to a cost increase and time delay.

Nowadays an evaluation of system dependability is performed early in the design process. Thus, if the result is not acceptable, changes are introduced in the first design phases before manufacturing process.

Different techniques are available for designing dependable systems: i.e., dependability means: the methods and techniques enabling the development of a dependable system. Normally, they are classified in 4 complementary categories:

- Fault prevention
- Fault removal
- Fault tolerance
- Fault forecasting

2.3.1 Fault prevention

Fault prevention is a set of techniques attempting to prevent the introduction or occurrence of faults in the system in the first place. Fault prevention is achieved by quality control techniques during the specification, implementation, and fabrication stages of the design process. For hardware, this includes design reviews, component screening, and testing. For software, this includes structural programming, modularization, and formal verification techniques.

A rigorous design review may eliminate many specification faults. If a design is efficiently tested, many of its faults and component defects can be avoided. Faults introduced by external disturbances, such as lightning or radiation, are prevented by shielding, radiation hardening, etc. User and operation faults are avoided by training and regular procedures for maintenance. Deliberate malicious faults caused by viruses or hackers are reduced by firewalls or similar security means.

2.3.2 Fault removal

Fault removal is a set of techniques targeting the reduction of the number of faults which are present in the system. Fault removal is performed during the development and operations phases of system life cycle. Three activities are conducted during fault removal at development phase: verification, diagnosis, and correction. Verification is the process of checking whether the system fulfils requirements established during design phase. Diagnosis is the activity conducted, if verification of certain requirements is not achieved, to identify the fault that leads to the unfulfillment of the requirements. Once the fault(s) is(are) identified, they are corrected.

Fault removal during operations consists of corrective and preventive maintenance. Preventive maintenance is conducted before fault occurs, proceeding with parts replacement. Corrective maintenance is conducted after fault takes place in order to return the system into its operational conditions.

2.3.3 Fault forecasting

Fault forecasting is a set of techniques used to estimate the number of faults present in a system, their possible future occurrence, and their consequences on the system. Fault forecasting is conducted by performing an evaluation of the system behaviour with respect to fault occurrences or activation. They evaluation can be conducted in qualitative and/or quantitative way. Qualitative evaluation aims at assessing the failure modes or events combinations that lead to system failure. Quantitative evaluation aims at assessing in terms of probabilities at which extend a dependability attribute is satisfied.

2.3.4 Fault tolerance

Fault tolerance targets the development of a system that correctly operates in the presence of a fault. Thus, fault tolerant techniques assume that faults may arise anyway, and aim at reducing their effects (i.e., the misbehaviours). These techniques are typically based on redundancy. Redundancy design techniques are classified in three groups: hardware redundancy, information redundancy and time redundancy.

2.3.4.1 Hardware redundancy

The system is implemented using more hardware than that needed for implementing the system functionalities. The redundant hardware is used for dealing with faults and can be classified in three groups: passive redundancy, active redundancy and hybrid redundancy.

Passive redundancy

Passive redundancy is usually based on fault masking, the process of assuring that only correct values, in the case of electronics, or more generally the correct functionalities get passed to the system output in spite of the presence of a fault. Concretely, the hardware needed to implement the system is replicated more than two times, fed with the same input. Each domain produces its own output and then, a majority voter decides the output to be committed to the user on the basis of the outputs coming from the different domains. Obviously, the voter must be fault-free; otherwise, failures may happen. Moreover, if the same fault exists in all the modules, the passive redundancy architecture fails.

Active redundancy

Active redundancy is an alternative to passive redundancy. It implements fault detection, i.e., the process of determining that a fault has occurred within a system. Moreover, it may also possibly implement fault location, fault containment and fault recovery. Fault location is the process of determining where a fault has occurred in the system. Fault containment is the process of isolating a fault and preventing the propagation of its effect throughout the system. Fault recovery applies a reconfiguration of the system to isolate the faulty component from the rest of the system and regain operational status.

Hybrid redundancy

As it names states, hybrid redundancy is a combination of passive and active redundancy. In this case, N primary modules are used plus M are spares. A switch selects a certain number of modules out of N primary outputs to be voted by the voter. A configuration module detects the primary modules whose outputs differ from the voter output. Each faulty primary module is replaced by a spare one.

2.3.4.2 Information redundancy

Information redundancy is based on the store of more data than those needed by the application. The redundant data added to the original data is used to detect and possibly correct errors affecting the original data. Information redundancy is usually applied to computer field. Some examples of information redundancy are: parity codes and hamming codes.

2.3.4.3 Time redundancy

Time redundancy is also commonly used in computer field. It is based in using more time needed for an input processing. The additional time is devoted to detect and possibly correct errors occurred during the processing.

2.4 Dependability attributes measurements

Different measurements are assessed to evaluate and quantify dependability attributes. The most used (i.e., failure rate, mean-time-to-failure, mean-time-to-repair and mean-time-between-failure) are detailed in the present section.

2.4.1 Failure rate

Failure rate, expressed with Greek-letter λ, is the expected number of failures per unit time. For example, if a component fails, on average, once every 10000 hours, then it has a failure rate λ=1/10000 failures/hour. The failure rate is highly useful in estimating the time to failure (or time between failures), repair crew size for a given repair policy, the availability of the system, and in estimating the warranty cost. It can also be used to study the behaviour of the system's failure with time.

The failure rate is a function of time. This evolution over a system's life-time is usually characterised, for hardware, by the bathtub-shaped function showed in Figure 2.

Figure 2 reads as follow: assume a population of N identical components functioning at time T=0. They experience a high failure rate at the beginning of the operation time due to weak or substandard components, manufacturing imperfections, design errors, and installation defects. As the failed components are removed, the time between failures increases which results in a reduction of failure rate. This Early Life Region with a decreasing failure rate is known as *infant mortality region*. Time T_1 represents the end of the early failure-rate region.

2 BASICS ON DEPENDABILITY

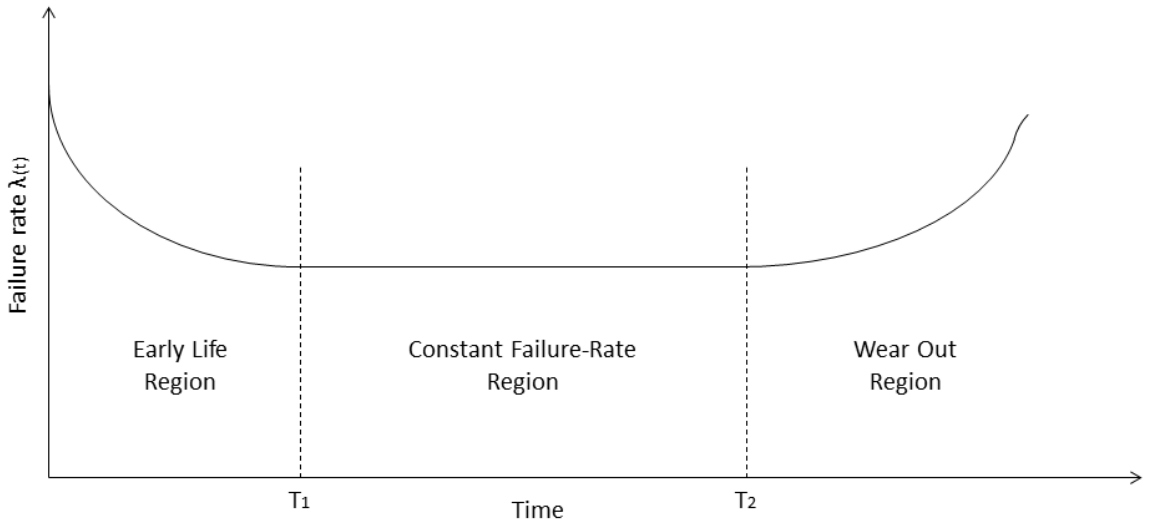


Figure 2: General evolution of failure rate over a life-time of a hardware system (i.e., bathtub-shaped function)

At the end of the early life region, the failure rate will eventually reach a constant value. In this region (i.e., between T_1 and T_2), the failures do not follow a predictable pattern, but they occur randomly. The third region, after T_2, is known as Wear Out Region. It is noticed when the failure rate starts to increase significantly more than the constant failure-rate value, and the failures are no longer attributed to randomness but are due to the age and wear of the components. In this region, a boost of the failure rate is observed due to the fact that components reach their designed life.

Obviously, not all components follow the bathtub-shape trend. Most electronic and electrical components do not exhibit wear out region. Some mechanical components may show a gradual transition between first and third regions, without facing a constant failure rate. Moreover, the length of each region depends on each component.

Different failure-time distributions are present in literature. Since the goal of the present research thesis is to deal with small-satellites missions' dependability, only failure-time distributions that fit with analysed data will be described in the required section.

2.4.2 Mean-Time-To-Failure

Mean-Time-To-Failure (i.e., MTTF) is one of the most widely used measurements of reliability, mainly applied for non-repairable systems. It is defined as the expected of the occurrence of the first failure. Hence,

$$MTTF = \int_0^\infty t f_{(t)} dt \tag{2.1}$$

The MTTF may be expressed directly in terms of the system reliability by substituting the following expression in equation (2.1):

$$f_{(t)} = -\frac{dR_{(t)}}{dt} \tag{2.2}$$

$$MTTF = -\int_0^\infty t \frac{dR_{(t)}}{dt} dt = -tR_{(t)}|_0^\infty + \int_0^\infty R_{(t)} dt \tag{2.3}$$

Since $tR_{(t)} \to 0$ as $t \to 0$ and $tR_{(t)} \to 0$ as $t \to \infty$, then equation (2.3) can be written as:

$$MTTF = \int_0^\infty R_{(t)} dt \tag{2.4}$$

In general, MTTF is meaningful only for systems that operate without repair until the first failure occurs. For most of the systems, this statement is not valid because maintenance is conducted before the next mission, repairing possible failures and restoring fully operational conditions to the system. In case of space systems, this assertion is usually not applicable and the pure definition of mean-time-to-failure applies.

2.4.3 Mean-Time-To-Repair

Mean-Time-To-Repair (i.e., MTTR) of a system is the average time required to repair the system divided by the sum of the individual failure rates. It depends on multiple variables: fault recovery mechanism used in the system, location of the system, location of space modules (on-site versus off-site), maintenance schedule, etc.

The MTTR mathematical expression is:

$$MTTR = \frac{\sum_{i=1}^{n} \lambda_i t_i}{\lambda_{tot}} \tag{2.5}$$

Where:

- λ_i = i-th failure rate
- λ_{tot} = sum of the individual failure rates

Obviously, for a space system is almost impossible to apply classical repairmen (e.g. as repair conducted on the Hubble space telescope). In section XX, the concept of MTTR is approached from the mission point of view.

If in a system occurs *n* failures during its lifetime, the total time that the system is operational is then *n·MTTF*. Similarly, the total time the system is being repaired is *n·MTTR*. Then, the availability is given by:

$$A_{(\infty)} = \frac{n \cdot MTTF}{n \cdot MTTF + n \cdot MTTR} = \frac{MTTF}{MTTF + MTTR} \tag{2.6}$$

2.4.4 Mean-Time-Between-Failure

Mean-Time-Between-Failure (i.e., MTBF) of a system is the average time between failures of the system. Usually, it is computed for repairable systems. Indeed, if a system is repairable and that repair makes the system perfect, then the relationship between MTBF and MTTF is established as defined in Eq. (2.7).

$$MTBF = MTTF + MTTR \tag{2.7}$$

2.5 Dependability models and techniques

A wide number of models are nowadays used to evaluate systems dependability. The present section aims at depicting a general overview and description of most common models and techniques to evaluate dependability. Techniques used for further studies in the present thesis will be further explained in future sections.

2.5 Dependability models and techniques

2.5.1 Reliability Block Diagrams (RBD)

Reliability Bloc Diagrams show the logical connections between components of a system, and thus, also the failure logic of the system. RBD performs the system reliability and availability analyses on large and complex systems using block diagrams to show network relationship. It is worth to remark that RBD is not necessarily the same as a block schematic diagram of the system's functional layout. Indeed, for systems involving complex interactions construction of the RBD can be quite difficult, and a different RBD will be necessary for different definitions of what constitutes a system failure.

It is usually conducting a reduction of reliability block diagram to obtain a simple system which can then be analysed using the formulae for series and parallel arrangements. Generally, a system can contain a series, parallel, or combination of series and parallel connections to make up the network.

Some properties of the modelling diagram are:

- Arranging several components along a path means connecting them by an "and" operation
- Arranging several components in parallel paths represents an "or" operation
- If a component appears in several expressions of the Boolean system function, it must be put in a corresponding number of parallel paths of the reliability diagram

Thus, in the system function of a non-redundant system, all components are connected by an "and" operation. All components must be faultless to forma faultless system.

Generally speaking, successful operational systems require at least one maintained path between the system input and the system output. Hence, a fault case is a combination of the possible values of the binary random variables indicating which components are faultless and which are not. Boolean algebra expressions are used to describe the minimum combination of failures required to cause a system failure. Minimal cut-sets represent the minimal number of failures that can cause the system to fail.

2.5.2 Fault Tree Analysis (FTA)

Fault Tree Analysis (FTA) is a reliability/safety design analysis technique which starts from consideration of system failure effects (i.e., the top event). The analysis is conducted assessing what failure or event (or their combination) in the next lower level is/are required to produce the top failure. Thus, this technique shows the logical connection between failure events in relation to defined top events. Moreover, it is used to quantify the top event probabilities, in the same way as in block diagram analysis. Failure probabilities are usually calculated based on failure rates of each basic event. Note that each FTA is conducted for a unique and well defined undesirable event and hence, the construction of different fault trees is required to study each top event.

FTA is useful in order to identify the causes of a failure or other weaknesses that can result in a system failure, including human errors. Then, it will allow to identify upgrades for the system in order to avoid failures or decrease their probability to occur. To conduct the FTA, specific steps are followed, as depicted in Figure 3.

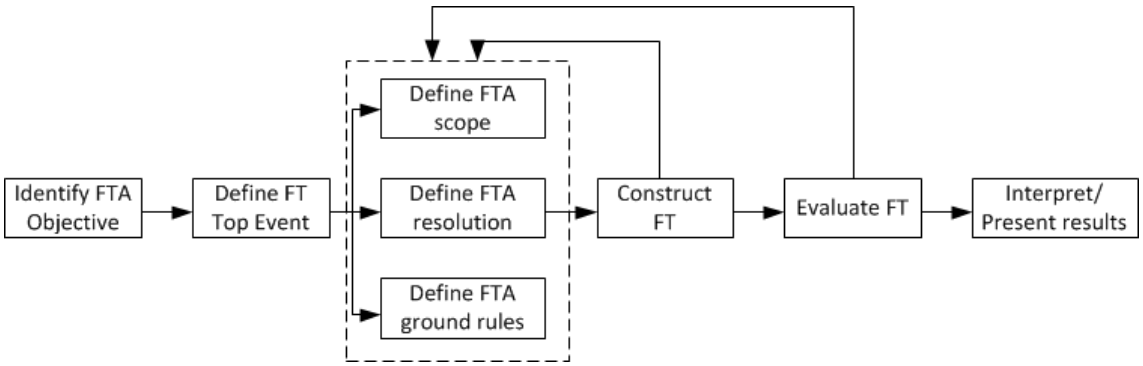


Figure 3: FTA definition steps

Generally, steps are conducted sequentially. However, steps 2 (define FTA scope), 3 (define FTA resolution) and 4 (define FTA ground rules), can be conducted in parallel. Moreover, steps 3 and 4 can be iteratively modified after steps 5 (construct Fault Tree) and 6 (evaluate Fault Tree) are being carried out.

In particular, the steps are the following:

1. Univocally define the top event
2. Define the FTA scope: identify what failures and events will be taken into account and what will not be considered, taken also into account the mission phase for which the FTA is being conducted
3. Define the FTA solution: identify the lowest level of detail at which the FTA will be developed
4. Define the FTA ground rules: define the procedure and the nomenclature for the events, gates, etc.
5. Construct the Fault Tree
6. Evaluate the Fault Tree: qualitative and quantitative assessment of top event probability of occurrence
7. Interpretation and presentation of results

2.5.3 Event Tree Analysis (ETA)

Event Tree Analysis is an inductive technique conducted to identify and evaluate all accidental sequences from the occurrence of an initiating event. It utilises a visual logic tree structure, the Event Tree. The objective of the Event Tree Analysis is to determine whether the initiating event will develop into a serious mishap or if the event is sufficiently controlled by the safety systems and procedures implemented in the system design. Then, an Event Tree Analysis can result in many different possible outcomes from a single initiating event, and it provides the capability to obtain a probability for each outcome.

The ETA technique is based on the following definitions:

- Accident scenario: series of events that ultimately result in an accident. The sequence of events begins with an initiating event and normally is followed by one or more pivotal events that lead to the undesired end state.
- Initiating event (IE): failure or undesired event that initiates the start of an accident sequence. The IE may result in a mishap, depending upon successful operation of the hazard countermeasure methods designed into the system.

- Pivotal events: intermediary events between the IE and the final mishap. These are the failure/success events of the design safety methods established to prevent the IE from resulting in a mishap. If a pivotal event works successfully, it stops the accident scenario and is referred as a mitigating event. If a pivotal event fails to work, then the accident scenario is allowed to progress and is referred as an aggravating event.
- Probabilistic risk assessment (PRA): comprehensive, structured, and logical analysis method for identifying and evaluating risk in a complex technological system. The detailed identification and assessment of accident scenarios, with a quantitative analysis, is the PRA goal.
- Event Tree (ET): graphical model of an accident scenario that yields multiple outcomes and outcome probabilities. ETs are one of the most used tools in a PRA.

An ET distils the pivotal event scenario definitions and presents this information in a tree structure that is used to help classify scenarios according to their consequences. The accident scenario concept (i.e. how mishap is reached) is shown in Figure 4.

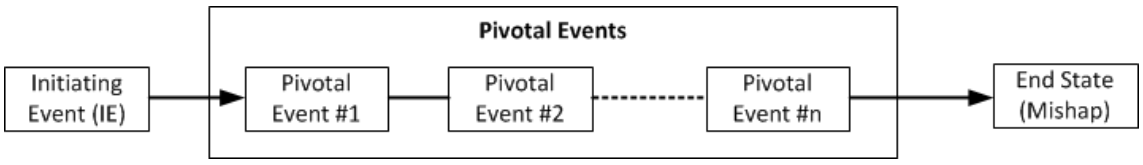


Figure 4: Accident scenario concept

The headings of the ET are the IE, the pivotal events, and the end states. The tree structure below these headings shows the possible scenarios ensuring from the IE, in terms of the occurrence or non-occurrence of the pivotal events. Each different path through the tree is a distinct scenario. According to a widespread but informal convention, where pivotal events are used to specify system success or failure, the “down” branch is considered to be “failure”. Figure 5 displays the event tree concept.

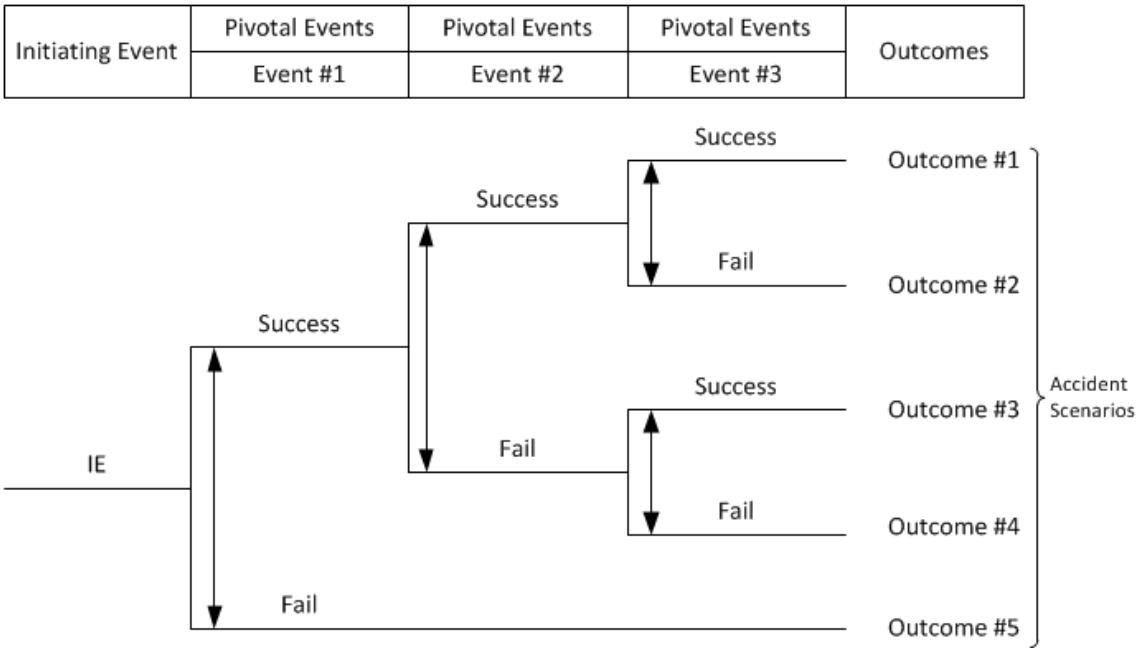


Figure 5: Event tree concept

2.5.4 Failure Modes, Effects and Criticality Analysis (FMECA)

Failure Modes, Effects and Criticality Analysis (FMECA) is probably the most widely used and most effective design reliability analysis method. It is a systematic analysis of all possible ways in which a component may fail, considering each failure mode as different voice. The FMECA highlights single point failures requiring corrective action; aids in developing test methods and troubleshooting techniques; provides estimates for system critical failure rates; provide a quantitative ranking of system and/or subsystem failure modes relative to mission importance; and identify parts & systems most likely to fail.

Therefore, the development of a FMECA during the design phases of a space system, the overall costs will be minimised by identifying single point failures and other areas of concern prior the manufacturing. The FMECA also provides a baseline or a tool for troubleshooting to be used for identifying corrective actions for a given failure.

Usually, the FMECA is conducted by performing, first a FMEA and then the CA. The FMEA will be sued as the foundation of the Criticality Analysis. At the end, a common scheme for the FMECA is used, as shown in Figure 6.

FAILURE MODES AND EFFECTS ANALYSIS (FMEA)
For use of this form, see TM 5-698-4; the proponent agency is USACE.

SYSTEM: Mechanical System
PART NAME: Industrial Water Supply
REFERENCE DRAWING:
MISSION: Provide Temperature Control to Room
DATE (YYYYMMDD): 20050819
SHEET: 1 of: 1
COMPILED BY: AAA
APPROVED BY: BBB

ITEM NUMBER	ITEM/FUNC-TIONAL ID	POTENTIONAL FAILURE MODES	FAILURE MECHANISM	FAILURE EFFECTS			DETECTION METHOD	COMPEN-SATING PROVISION	SEVERITY CLASS	REMARKS
				LOCAL EFFECTS	NEXT HIGHER LEVEL	END EFFECTS				
100.0	Ind cool water /supply water to condenser at 75° F & 1000GPM	Provide water greater than 75°F	cooling tower malfunction, pump degraded, fan will not start							
100.1		Provide water less than 75°F	Fan will not turn off							
100.2		Provide water less than 1000GPM	Degraded Pump							
100.3		Provide no water	broken pipe							
100.4			blockage in pipe or pump failure							

Figure 6: FMECA scheme (FMECA for C4ISR facilities, Headquarters, Department of the Army)

2.5.5 Markov analysis

Markov analysis is a steady-state technique that takes into account, on the contrary of previous methods, the interaction of components failures. Moreover, the present method allows to take into account the dynamics of the system, i.e., to take into account when the system is repaired. Assuming that a system can be in one of two states (e.g. failed, non-failed), the probability of being in one or other at a future time can be valuated using state-space analysis (e.g., Markov analysis).

Markov analysis is a special class of stochastic process. The basic assumption is that the behaviour of the system in each state is memoryless. The transition from one state of the system is determined only by this state and not by the previous state or the time at which it reached the present state.

2.5 Dependability models and techniques

Two major constraints shall be considered prior applying Markov analysis:

- The process must be homogeneous (i.e., probabilities to change from one state to another shall be constant). Hence, it is possible to use the method only when the failure rate is constant.
- Future states of the system are independent of all past states except the immediately preceding one. As stated above, the system in each state is memoryless, and it does not take into account historical events.

3

SHRINKING SPACE

3.1 Small Satellites description

Historically, the evolution of satellites technologies led to achieve mission objectives through small number of reliable, high capable and complex satellites. The reliability was usually reached applying redundancies on high reliable, expensive components. Generally speaking, big satellite projects are characterised by wide number of requirements to comply with constraints from different potential users and payloads.

However, in the last decades the use of new architectures based on small satellites arose. In particular, it was stated the idea to complement classical mission architectures based on conventional monolithic spacecraft with small satellites. Small satellites are simpler than conventional satellites; they usually have a single payload with limited capabilities. Despite that, the increase during these last years of technology miniaturisation while increasing capabilities led to an achievement of better performances on small satellites.

Moreover, these type of spacecraft are characterised by a shorter life-cycle and hence, developed in shorter time. Usually they are designed by a small team at a moderate cost. Due to the low budget and then, minimum cost, small satellites are equipped with fewer components and are characterised by less complexity. These characteristics led more freedom to engineers to use newer and less expensive technologies, such as state-of-the-art electronics. Definitively, most of the small satellite projects objectives are a compromise between what the designer would like and what it can be afforded with the satellite, what is called trading on requirement.

3 SHRINKING SPACE

The main advantage of miniaturising spacecraft, as already stated, is the reduction of cost and development time. These key drivers allow different institutions, which sometimes cannot affords the cost and/or design time of conventional satellites, to undertake the development of space projects. The modest on-orbit capabilities of this type of spacecraft led to most simple architectures and hence, reduced mass. These characteristics gave other advantages to small satellite developers. First of all, the reduced mass and volume of the spacecraft permit to fill small empty spaces on large launchers, allowing the insertion in-orbit of small satellites as piggy-back payload. Secondly, the physical characteristics of small satellites facilitate on-ground transportation. Indeed, they can be carried in a car or in an airplane seat, for example.

The advantages of small satellites have been gathered by different institutions. Military space projects usually foresaw larger spacecraft that were vulnerable from enemies' aggressive attacks. They address this weakness mainly with reliable components and defensive countermeasures that contributes to mass and cost increase. Using many small satellites will allow to reduce potential aggressive attacks by using more vulnerable systems, with similar capabilities, but becoming more difficult target. Educational institutions, at this turn, envisage a perfect opportunity to provide hands-on experience projects to space engineering students. The reduction of cost and size allow this type of institutions to afford practical space projects driven by educational, technological and scientific purposes. Moreover, these different key drivers of educational space projects led to possible collaborations between educational institutions and space agencies and companies.

Typically, a small satellite is a spacecraft with a mass lower than 500 Kg. With the evolution of these satellites, a more precise definition and classification of them was needed. Actually, the most widely adopted terminology and classification of satellites is the following:

Table 2: Satellites classification by mass

General classification	Detailed classification	Mass
Big satellites	-	More than 500 Kg.
Small satellites	Mini-Satellites	100 to 500 Kg.
	Micro-Satellites	10 to 100 Kg.
	Nano-Satellites	1 to 10 Kg.
	Pico-Satellites	0.1 to 1 Kg.
	Femto-Satellites	10 to 100 gr.

3.2 Historical evolution of small satellites

Small satellites are not an innovative evolution of spacecraft. First artificial satellites were characterised to be small and simple with respect to actual conventional satellites. Anyhow, they were innovative systems at that time. These first satellites, which nowadays can be classified as small satellites, were small because the limitations of maximum launch capabilities of available launchers.

Space Age began with Sputnik-1, the first artificial satellite orbiting Earth, launched on 4th October 1957. It had a spherical-shaped structure of 58 cm. diameter and 83.6 Kg. mass. It was only equipped with two frequency radios for on-ground tracking. America's Vanguard project represents also the beginning of space conquest. Vanguard-3 satellite also had a spherical-shaped structure of 50.8 cm. diameter and 22.7 Kg. mass. Its experiments allowed scientific community to define the low edge of Van Allen Belt.

Radio-amateur community quickly envisaged the possibility to use these small satellites for communications and educational purposes. Indeed, already in the '60 they started to develop OSCAR (Orbiting Satellite Carrying Amateur Radio) satellites with the objective of facilitate communications between amateur radio stations. The first one, OSCAR-1, was launched in 1961 and to date over 70 OSCARs have been launched.

3 SHRINKING SPACE

During the ’60s, ’70s and mid-80s, the nations with space-technology capabilities focused their attention to develop more and more sophisticated spacecraft to achieve higher on-orbit performances. Moreover, the increase of interest on human spaceflights, including the lunar landings, led to an evolution on boosters’ technology obtaining larger rockets. These new launchers allowed the on-orbit insertion of larger satellites in different orbits, including higher orbits not possible to reach before. Then, the evolution of launchers performances, together with the need of larger, more capable and more complex satellites led to growth of satellites in terms of mass and size.

Nonetheless, small satellites continued to be developed without much attention either from public or aerospace engineering interest. Thank to continuity on small satellites development, simple and less expensive technologies continued to be tested on-orbit. Moreover, during this period many countries started to develop their own space-technology capabilities reaching space through launches of small satellites. For example, Spain’s first satellite was IntaSat, a small satellite launched as a secondary payload on a Delta launcher in 1974. The satellite, with an expected operational life of two years, was equipped with an ionospheric beacon for ionospheric irregularities and scintillations studies. Another example is the ANS (Astronomische Nederlandse Satelliet), the first satellite from The Netherlands, launched also in 1974. The objective of the mission was to observe celestial objects in UV and X-ray sources.

Despite the continuous increasing trend of satellites mass, since mid-80s, space agencies and private companies reconsidered the use of small satellites, as can be observed in Figure 7. For example, radio-amateur community demonstrated, thanks to OSCAR project, the use of small satellites for global mail services applying *store and forward* communications.

3.2 Historical evolution of small satellites

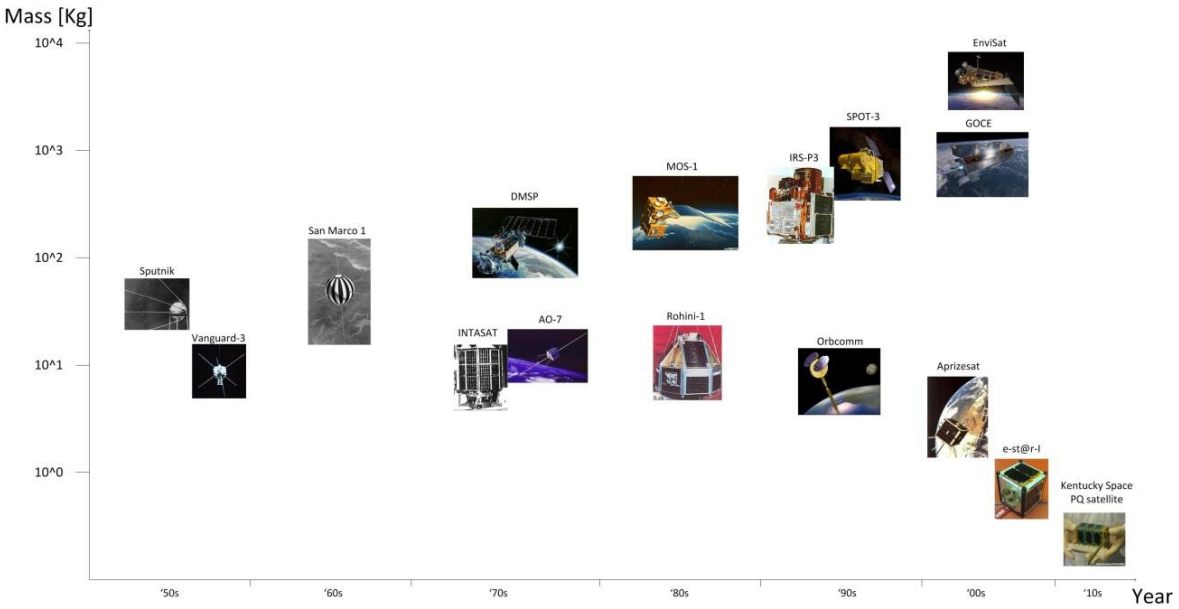


Figure 7: Satellites mass evolution

The emerging interest on these satellites led to establish some initiatives to increase development of small satellites. NASA's *Small, Self-Contained Payloads program* offered individuals or groups opportunities to fly small experiments aboard the Space Shuttle. The main three categories of users were educational, foreign and commercial, and U.S. government. The experiment was launched through a container installed in the Space Shuttle payload bay. In the European side, possibility to launch small-satellites was also provided. ASAP (Ariane Structure for Attached Payloads) were developed to allow up to 6 satellites of 50 Kg. maximum each on Arian V launcher. Due to the popularity and success of the ASAP program, it was expanded to accommodate larger payloads with a mass of up to 100 Kg.

Summarising, various circumstances required the reassessment of the role of conventional and small satellites, and boost the development of the later. In particular:

- Multipurpose missions require high technology development base with high investments on space research and industry. Moreover, this could limit space access for some nations.
- Increase society pressure to cost-constrained budgets for space activities

3 SHRINKING SPACE

- Technology miniaturisation that allows reduction of satellite mass while maintaining similar technical performances
- New initiatives of space agencies to allow the launch of small satellites

During the last two decades some conventional multi-payload high-mass satellites have yet been developed. Well-known examples of this type of satellites could be SPOT-3 or EnviSat. The first one is a 1800Kg. satellite launched in 1993 with two identical visible high-resolution optical instruments for Earth observation. EnviSat was an Earth observation mission of ESA devoted to study and monitor Earth's environment on various scales, from local through regional to global. Its mass at launch, which took place in 2002, was 8140 Kg. Although new conventional satellites have been developed, the boost of the interest on small satellites design considerably increased from the beginning XXI century.

3.2.1.1 CubeSat Standard

Following the trend of cost-reduction and fast-delivery, the CubeSat standard was defined in 1999 by Prof. Bob Twiggs from Stanford University and Prof. Jordi Puig-Suari from Cal Poly. The standard was stated to allow people with little or no experience in space missions and systems design to start with an open mind to incorporate new ideas and concepts into designs and missions that have no historical restrictions.

The physical standard was then based on a 10x10x10 cm. cube (i.e. a cube of 1lt. volume) of 1.33 Kg. as maximum mass (first the standard established a maximum mass of 1Kg. but NASA and CalPoly have recently adopted this new mass limit). The basic 10x10x10 cm. cube is the basic unit of a CubeSat and it is called "1U" CubeSat, as shown in Figure 8. It is scalable in different U-basis, being 2U and 3U the most common developed CubeSats.

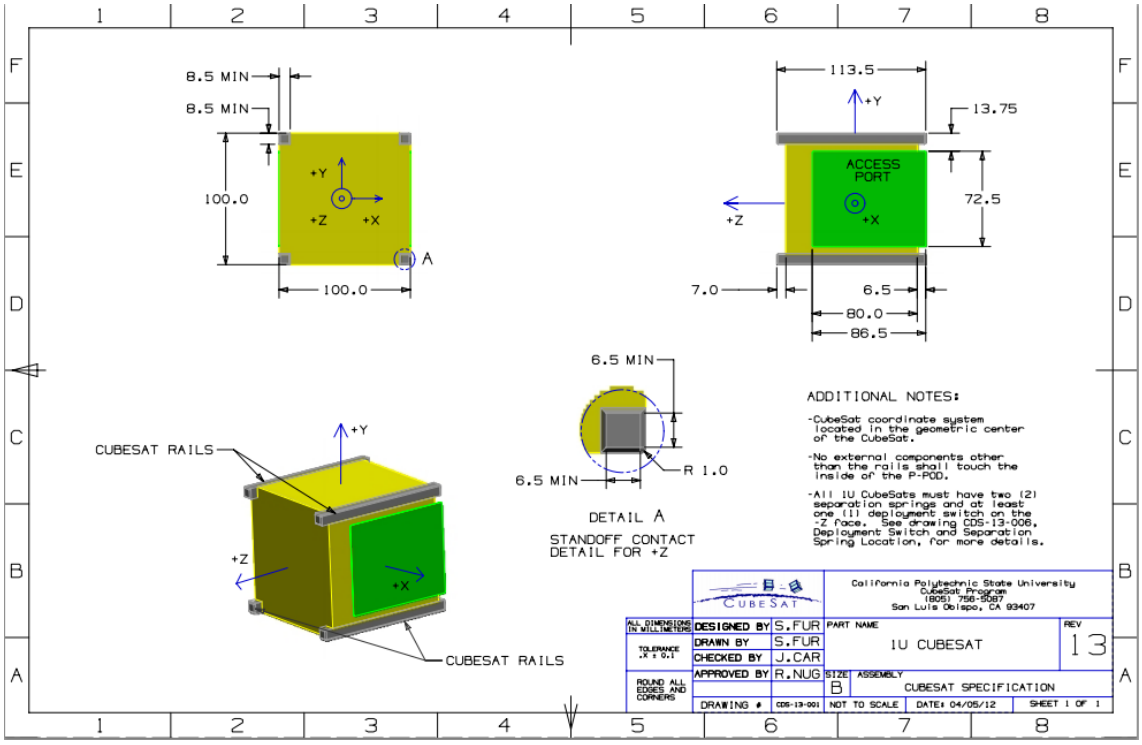


Figure 8: CubeSat Design Specification (CDS rev.13, CalPoly, 2014)

From educational point of view, the CubeSat philosophy was to give a common standard to university students to allow them the design of a small satellite in a reduced period of time (e.g. around 2 years) and launch it at a low cost. The reasonable cost of this type of satellite was fixed at $100000. The standard mission of a CubeSat was defined to be: 1) technology demonstration to allow increase of technology readiness level of certain technology providing flight heritage, or 2) accommodate a scientific instrument as primary mission payload.

As far as engineering point of view regards, the standard gives a common mechanical interface with launch by means of standard orbital deployers. The first deployer, called Poly-PicoSatellite Orbital Deployer (P-POD), was developed by Cal Poly. It is possible to accommodate in it up to three 1U CubeSats or different combinations of units resulting in a total of 3U. The increase of number of designed CubeSats due to its advantages in terms of cost and time-development made that different commercial companies provide launch opportunities using self-developed deployers.

3.3 Survey and Analysis of 10 years of CubeSats

A survey of launched CubeSats in the last 10 years has been conducted as well as an analysis of failures occurred in CubeSats based on the gathered information. All these data is detailed in the present section. First of all, a database has been created by the author. Data from public sources (i.e. websites, articles from international journals, etc.) have been used to create it. The information included on the database encompasses all general data regarding launched CubeSats, launch information, failures occurred, if any. The complete list of database contents is detailed in Table 3.

Table 3: Database contents

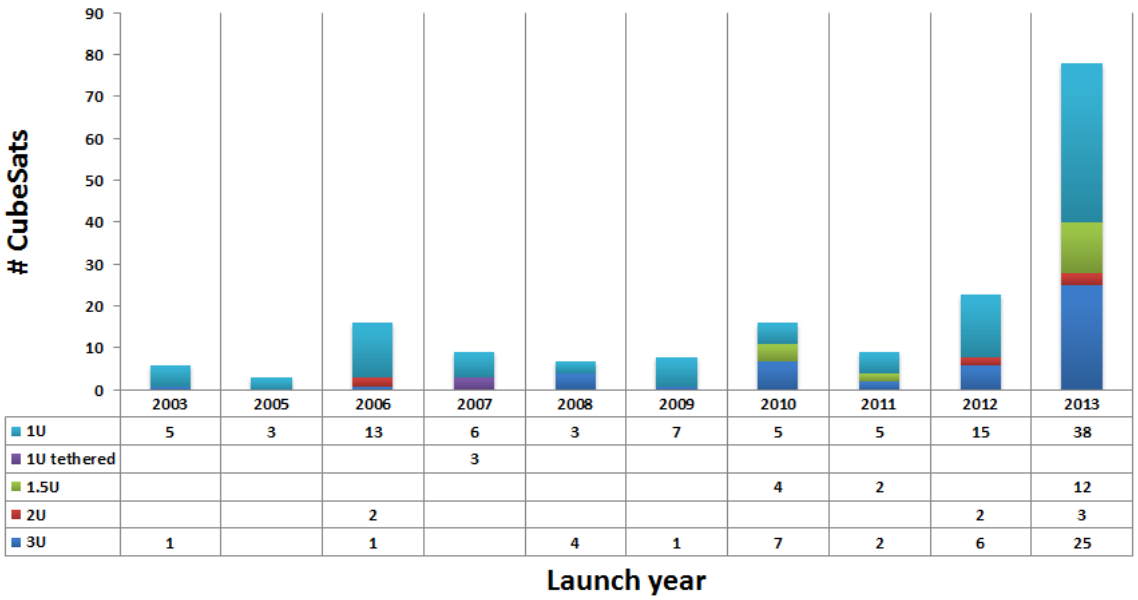
General data	Launch information	Failures information
CubeSat name	Launch date	Status
CubeSat type	Launch site	Year of failure
Type of institution	Launch vehicle	Failure mode
Developer	Deployer	Failure cause
Country		Failure effect
Objective		Restoring action

This section is divided in two parts. In the first one, general analysis of the database is conducted. This analysis encompasses the evaluation of the launched CubeSats evolution by type and year, their geographical distribution, the development institutions, the launch evolution by type and institution, and the evaluation of the objectives. The second part of the analysis, an assessment of CubeSat failures is conducted, focusing the attention on the contribution of each subsystem to the total number of failures. The identification of possible causes is also conducted.

3.3 Survey and Analysis of 10 years of CubeSats

3.3.1 General analysis

The first multiple launch CubeSat mission, involving 6 CubeSats as a secondary payload took place on June 30th, 2003. The insertion in-orbit was conducted with a Rockot KS launcher of Eurockot Launch Services form the launch site in Plesetsk, Russia. Ten years later, at the end of 2013, 175 CubeSats have been launched and it is evident that there is a considerable boost of developed CubeSats during the last years, as shown in Figure 9.



	2003	2005	2006	2007	2008	2009	2010	2011	2012	2013
1U	5	3	13	6	3	7	5	5	15	38
1U tethered				3						
1.5U							4	2		12
2U			2						2	3
3U	1		1		4	1	7	2	6	25

Figure 9: Number of launched CubeSats per class and year

In previous figure it can be clearly identified a considerably increase of launched CubeSats in the period 2010-2013. In particular, a peak is observed in 2013 when almost 45% of the total CubeSats were launched. This growth can be traced back to several reasons:

- Interest of universities to establish hands-on experience approach projects to students and applied research activities
- The nature of this type of satellites allures industries the interest on CubeSats development as a way of cost-reduction, fast-response to accomplish different objective as for example in-orbit technology demonstration
- Technological progress (e.g. technology miniaturisation) allowed the implementation of new systems and mission architectures; constellation/swarm

mission architectures, instead of classical monolithic configuration, are being developed, like Flock-1 constellation

- The support of space agencies on CubeSat development and launch. For example ESA Education Office's CubeSats on VEGA Maiden flight project and Fly Your Satellite! Programme (which call for proposals took place on 2008 and 2013 respectively) and NASA's ELaNa (which first call for proposals was in 2010)
- Availability of shared launches due to the fact that these small satellites can fill empty spaces on big launchers as piggy-back payloads

The increase of CubeSats created a high demand of promptly availability of low-cost launches. To cope with this need, new launch provider companies came into the market. An in-depth analysis of the data shows a clear contribution of 1U CubeSats to the total amount. In detail, a total of 103 1U platforms have been launched, which represents over 60% of the total number of launched CubeSats. Nonetheless, during the last half of the last decade, significant boost on number of developed 3U CubeSats is observed. 1.5U and 2U platforms have also been launched, but they represent less than 10% of the total. Usually, universities starts their space projects developing 1U CubeSats, mainly to keep the design simple using the most popular configuration, and to limit the cost investment. For example, the CubeSat Team at Politecnico di Torino developed its first 1U CubeSat, e-st@r-I, which was launched in 2012; thanks to the experience gained by that project, a 3U CubeSat, 3STAR, is under development now. In some cases, university teams continue to develop 1U CubeSats or started first space project working on a 3U. New mission objectives (e.g. technology demonstration, Earth observation or scientific purposes) also require to allocate greater volume and mass of the CubeSat for the payload. Moreover, to conduct certain type of missions, bus performances (e.g. attitude determination and pointing accuracy) shall be better and could require higher mass and/or volume. All these factors led to the need to enlarge mass and volume of CubeSats.

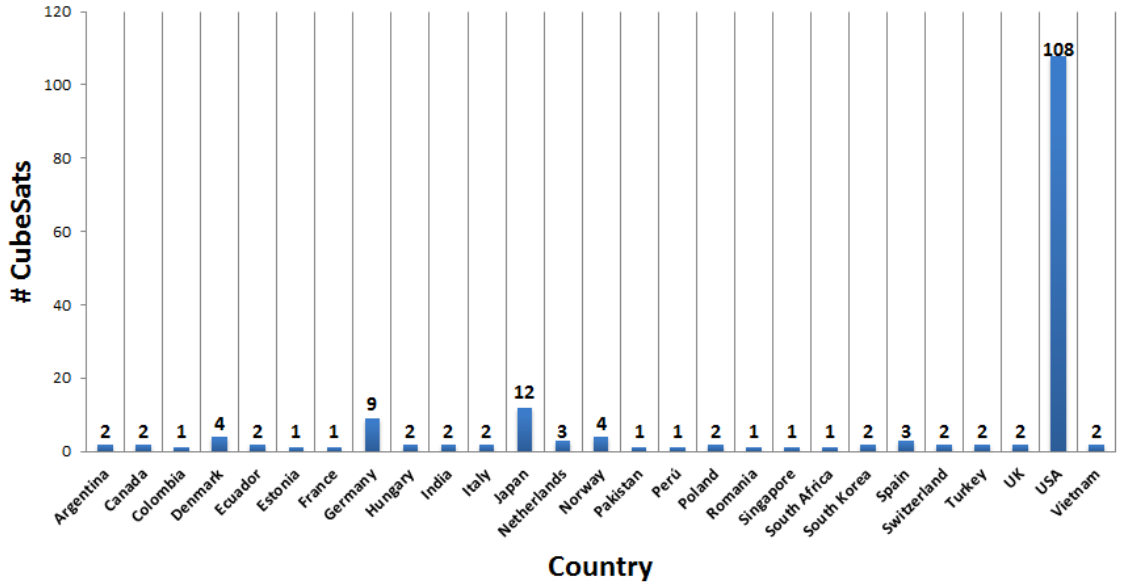


Figure 10: CubeSats geographical distribution

Geographical distribution shows a clear predomination of America (mainly North America) and Europe as regions where most of the CubeSat projects have been run; Asia and Africa follow while no CubeSats developed in Oceania have been launched. In particular, over 60% of CubeSats have been developed in the United States of America. The following country is Japan, with 7% of CubeSats. The other CubeSats have been developed in 25 different countries, with Germany (9 CubeSats), Norway and Denmark (4 CubeSats each) on highest-ranking, as illustrated in Figure 10 and Figure 11.

3 SHRINKING SPACE

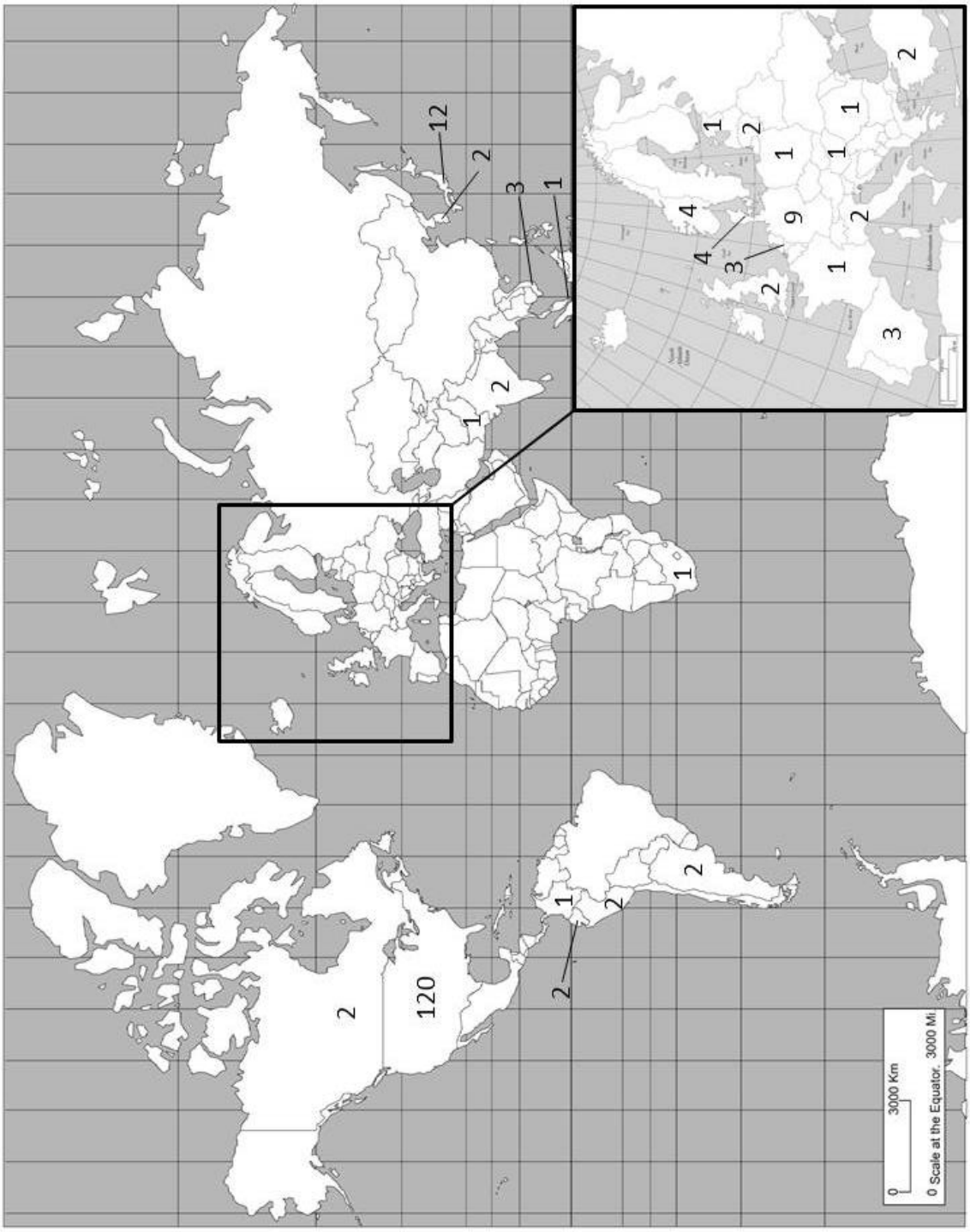


Figure 11: CubeSat geographical distribution on a map

3.3 Survey and Analysis of 10 years of CubeSats

The geographical distribution of CubeSat projects is strongly correlated to national budgets for space activities. USA is the country with highest percentage of Gross Domestic Product (GDP) invested in space activities and, indeed, is the country where major part of CubeSats have been developed. Most of the developed CubeSats are distributed by countries following the order of the space activities budget. However, two unexpected observation arise: first, the fourth country by number of developed CubeSats, Denmark, has one of the lowest space activities budget with respect to most of the European and North American countries; second, no CubeSats have been developed in Russia Federation and Popular Republic of China, respectively the second and third country by percentage of GDP invested in space field.

Next analysis covers the evaluation of developed CubeSats by type of institution. To conduct this, only the main institution is considered (i.e. if a university is developing a CubeSat within a collaboration with a research institution, the former has been considered as the developer institution). On the whole, it has been observed that most of the CubeSats have been developed within universities, as it is shown in Figure 12.

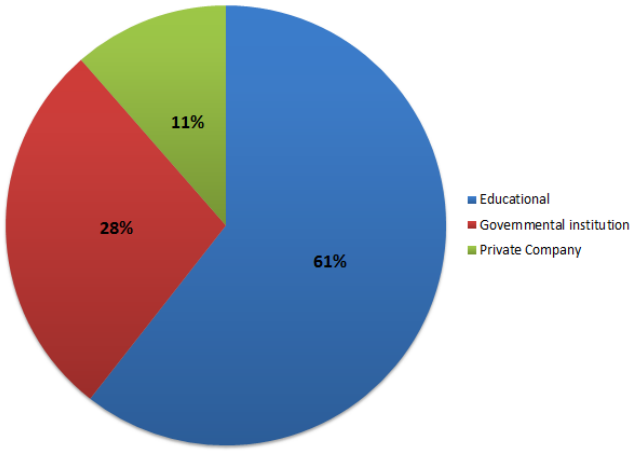


Figure 12: CubeSats distribution by development institution

3 SHRINKING SPACE

However, the ability of a rapid design and a development of a low-cost spacecraft, and hence a quicker and cheaper access to space, woke-up the interest in CubeSats development by governments and private companies. To date, more than the 35% of CubeSats have been designed and manufactured by these types of organizations.

CubeSats have been developed within universities since the very beginning of the 21st century and, in general, the number of them inserted into orbit continues to increase, as can be seen in Figure 13. On the other hand, governmental organisations and private institutions have not started to launch CubeSats until mid-2000s. But the number of CubeSats developed by governmental organisations has increased considerably in the last five years while private institutions started in mid-2000 to develop this type of satellites, with a boost in 2013.

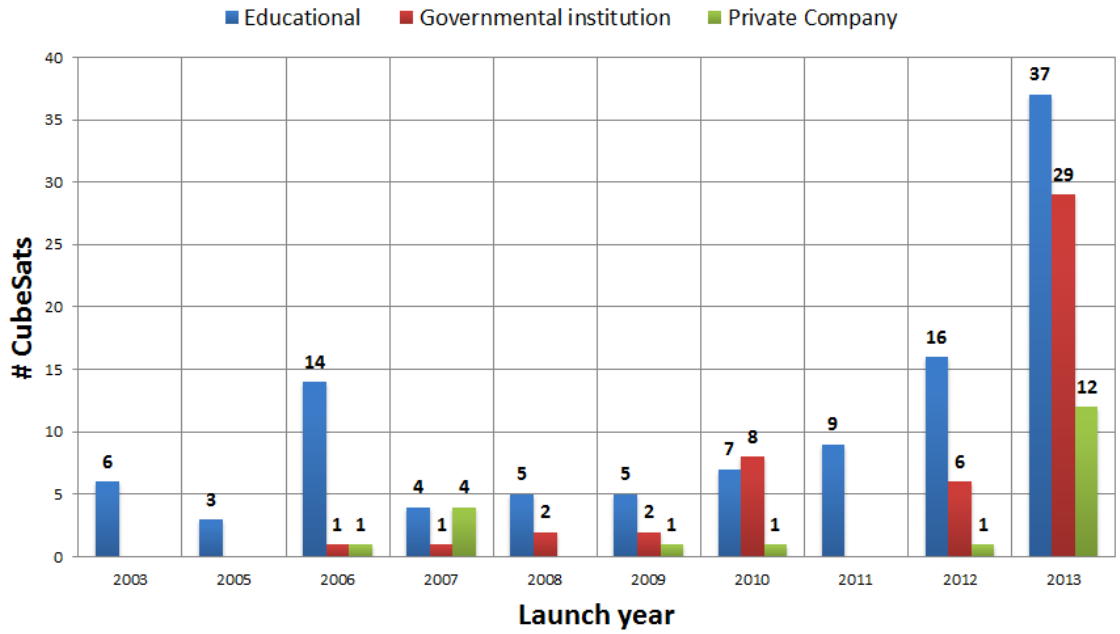


Figure 13: Launched CubeSats by development institution and launch year

The strong relation between CubeSats and universities is quite evident and consequently most CubeSat programs have an educational objective, as illustrated in Figure 14. However, the mission objectives of the CubeSats are moving gradually from pure educational purpose to technological and scientific objectives. Moreover, most of the educational CubeSats have a secondary objective, usually technology demonstration. Earth observation and scientific purposes are also popular mission objectives of some of these CubeSats.

3.3 Survey and Analysis of 10 years of CubeSats

CubeSats missions beyond Low Earth Orbit are being studied, and one CubeSat for technology demonstration for future missions to the Moon has already been launched. Furthermore, members in the CubeSat community are also starting to propose the use of CubeSats for interplanetary missions.

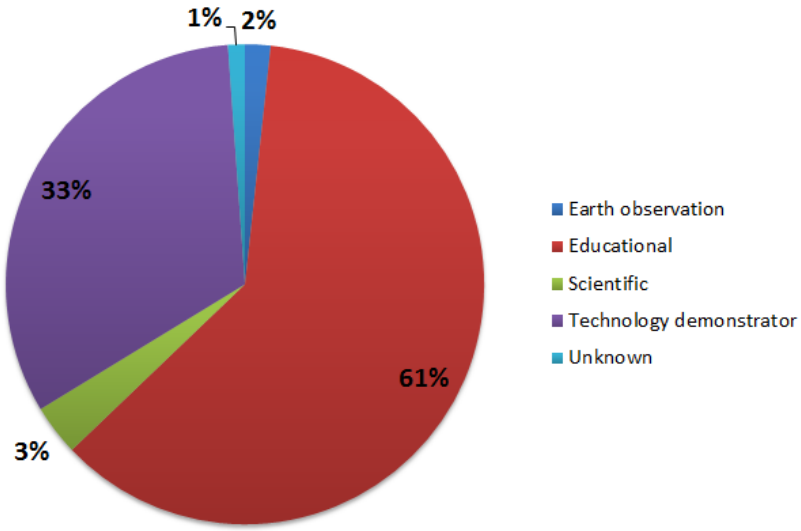


Figure 14: CubeSats primary objective

3.3.2 CubeSats failures, causes and effects

The desired evolution of CubeSats from pure educational systems to commercial/scientific satellites requires an improvement of their rate of success. The rate of success of previous missions is evaluated in the present section.

The CubeSats, as stated above, born in the universities and hence, the challenge is to find solutions that achieve the desired objectives at lower possible cost. However, this handicap will led to a reduction of mission success as detailed up ahead.

3 SHRINKING SPACE

The failure of a Dnepr launcher in 2006 led to the destruction of 14 CubeSats (representing up to 11% of the total launched CubeSats, as depicted in Figure 15) and became the worst tragedy within the CubeSats community. Almost 30% of CubeSats experimented a failure on orbit. On the other hand, a substantial 49% of the developers declared the achievement of mission objectives, as illustrated in Figure 16.

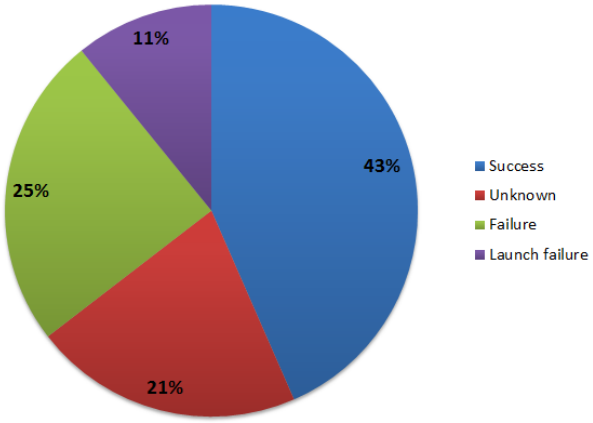


Figure 15: CubeSats failures

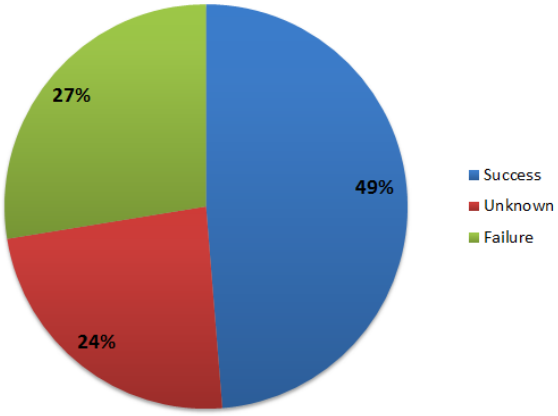


Figure 16: CubeSats failures excluding launch failures

CubeSats mission success is unknown for over 24% of the total number of satellites. However, a considerably high number of developers updates their webpage until launch. Sometimes they are reticent to inform about possible failures and usually the information are updated only when mission success is achieved. Nonetheless, the authors often verified that, when a CubeSat developer updates the “unknown” information, usually a failure was observed. Hence, most of unknown mission success have high chances to be declared as failure. Assuming this premise, the failure rate increases over 50% of the mission success. Figure 17 depicts failure subdivision by subsystems where they were observed.

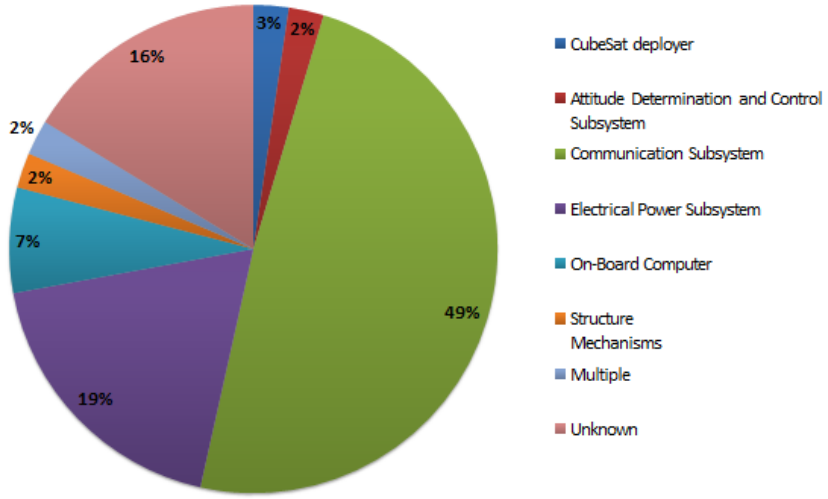


Figure 17: CubeSats failures by subsystem where failure has been individuated

The process of tracing back subsystems failures contribution to satellite loss is complex. Identifying the top event that caused each failure would require the implementation of specific techniques (e.g. root cause analysis) for each event. This analysis has not been done because it would overstep the goal of this paper, the statistical evaluation of failures based on CubeSat developers' public declarations. For example, failures on communication subsystem have been allocated to this subsystem when declared by the developer, even if no communication link have never been established, and hence, it could be caused by a failure on another subsystem (e.g. on the EPS).

Communication subsystem, electrical power subsystem and on-board computer are the subsystems on which the majority of the failures have been observed, as shown in Figure 17. On the other hand, up to 16% of failures could not be allocated to any subsystem and were classified as unknown.

It is then evident that major contributions to satellite failures are due to communication subsystem failures, as expected, which represent almost 50% of the total failures. Failures on this subsystem were divided between CubeSats for which no link had ever been established, and those from which a signal has been received and then lost. Low signal-to-noise ratio and impact of radiations on the communication subsystems were identified as main causes on communication subsystem in the second case. The low signal-to-noise ratio led to the

impossibility to decode or download telemetry. Radiations effects on communication subsystem led to stop communications instead. However, some failures produced by radiations have been solved after a power drain that cleared radiations effect. In case no communication occurs after insertion into orbit, nothing can be inferred about the failure cause. The failure itself can be traced back to subsystems other than the COMSYS, as said before. Several causes are proposed by some CubeSat teams, such as that the antenna could not be deployed correctly, or that the entire satellite remained in the deployer.

Failures in the electrical power subsystem represent 19% of the total failures. In particular, batteries and solar panels are the single components where most failures were observed. Batteries are usually the most critical components of the EPS. They usually have a tight operative range of temperature with respect to the other EPS components (i.e. electronics and solar panels) and hence, if temperature rises over designed temperature values, batteries could be permanently damaged leading to the partially or completely loss of the mission. In effect, batteries failure led to the possibility to have (in the better case) an active satellite during sunlight, when the solar panels produce energy to switch-on the CubeSat. Most of the failures on the EPS are detected just after the CubeSat insertion into orbit or just after a few months from the deployment, and all of them caused by a failure on the batteries or power converter systems. Some failures occurred on solar panels, but they were less critical as they led to degradation, and not the loss, of the power generation.

Besides, On-Board Computer failures represent around 7% of the total failures, mainly due to radiation effects (e.g. single event latch-up) and design weakness (e.g. permanent damage when writing on the memory due to an erroneous write process on the memory chip). Failures have been observed also in other subsystems, but their number is negligible with respect to the above detailed failures. Failures on structures & mechanisms, Attitude Determination and Control Subsystem and due to deployer failure represent 2% of the total.

4

CUBESATS MISSIONS RELIABILITY

4.1 Introduction

In chapter 3 has been individuated that CubeSat missions are considerably affected by failures. In particular, considering the assumptions given in section 3.3.2, failures took place on the 50% of CubeSats inserted in-orbit. In the present chapter an analysis of CubeSats missions' reliability is conducted. The study is divided in two sections: the first one contains reliability analysis using non-parametric approach while the second section details the conducted parametric analysis

4.2 Considerations prior analyses

Prior any analysis is conducted on the data contained in the database; it is worth to remark the following considerations and assumptions taken into account for the analyses:

- Analysed data has been gathered from public sources and contained in a database (explained in section 2). Hence, the reliability on the information lies also on the trustworthiness of the public available information.
- The analysis is based on real data. Hence, it take into account that the CubeSats and, by extension, all their components have been subjected to real environment (i.e., not simulated). Then, the operation conditions are be different among all satellites.
- The satellites from which no information about the mission success is available have been excluded from the analyses. Then, a total amount of 113 satellites have been taken into account to conduct the analyses.

- It is necessary to highlight that, obviously, all CubeSats have been developed with different approaches, methods, procedures, etc. Then, each unit under consideration is different from the others.

4.3 Non-parametric analysis of CubeSats missions reliability

In a non-parametric analysis no probability distribution is assumed a priori and hence, it is used to infer the probability distribution that the analysed data follows. Indeed, this type of analysis is also called model-free. This kind of analysis is characterised to take into account very few assumptions. In particular, the advantages that no-parametric methods have over parametric methods are:

- They can be used to test population parameters when the variable is not normally distributed.
- They can be used when the data are nominal or ordinal.
- They can be used to test hypotheses that do not involve population parameters.
- In most cases, the computations are easier than those for the parametric counterparts.
- They are easy to understand.

However, there are also drawbacks in using non-parametric analyses with respect to parametric analyses. In particular:

- They are less sensitive than their parametric counterparts when the assumptions of the parametric methods are met. Therefore, larger differences are needed before the null hypothesis can be rejected.
- They tend to use less information than the parametric tests. For example, the sign test requires the researcher to determine only whether the data values are above or below the median, not how much above or below the median each value is.
- They are less efficient than their parametric counterparts when the assumptions of the parametric methods are met. That is, larger sample sizes are needed to overcome the loss of information.

4.3 Non-parametric analysis of CubeSats missions reliability

In our case it has been used the Kaplan-Meier estimator due to the fact that we deal with right-censored data, as explained later on. To conduct the reliability analysis, pre-processing on the database has been conducted. In particular, it has been individuated launch date and failure date (if failure occurred). Then, it has been established the observation window and assessed if any observed satellite data is censored or not. In the next sections each of these concepts as well as the procedures and obtained results of the analysis are detailed.

4.3.1 Censored data

In some circumstances, mainly when a study deals with real data, missing observations occur. This event can take place for many reasons: for example, during a test of high reliable components, it is usual that not all of them fail by the end of the time allotted for the test. In some engineering studies, some of the units on test may be withdrawn from the test for various reasons or may fail due to a cause that is not under study. Such incomplete data observations in reliability studies are called *censored items*. Although the failure time information on such an item is incomplete, there is usually still some information in the time data that is available in the item and so the censoring time should always be recorded in a study.

So data can be classified as complete data and censored data. In case of censoring, its classification is stated according to type and order. Hence, we have the following data classification:

- **Complete**: in this case the value of each sample unit is observed or known.
- **Right censored**: also referred as *suspended* data, it is the most common case of censoring. In the case of life data, these data sets are composed of units that did not fail. The term *right censored* implies that the event of interest (i.e., the time-to-failure) is to the right of our data point (i.e., end of observation window). Hence, if the units were to keep on operating, the failure would occur at some time after our data point.
- **Interval censored**: also called *inspection data* by some authors, it reflects uncertainty as to the exact times the units failed within an interval. This type of data

frequently comes from tests or situations where the objects of interest are no constantly monitored.

- **Left censored**: in this case, a failure time is only known to be before a certain time but the exact time is unknown. This is identical to *interval censored data* in which the starting time for the interval is zero.

In our case, we have right censored data because we exactly know the insertion time that corresponds to the moment in which each satellite starts to operate (i.e. date of insertion into orbit), but we do not know all failure times. Indeed, some CubeSats have reached their end-of-life or continue to be active after the observation window that has been established between the date of the first CubeSat launch (i.e. 30th June 2003) and 31st December 2013. Furthermore, for obvious reasons, dates of enter into operations for each CubeSat do not coincide. Hence, we have to face with staggered entry. Both points, right censoring and staggered entry, will be addressed in section 4.3.3, where application of Kaplan-Meier estimator for CubeSats Reliability analysis is detailed. The abovementioned characteristics (i.e., right censoring with staggered entry) are represented in Figure 18.

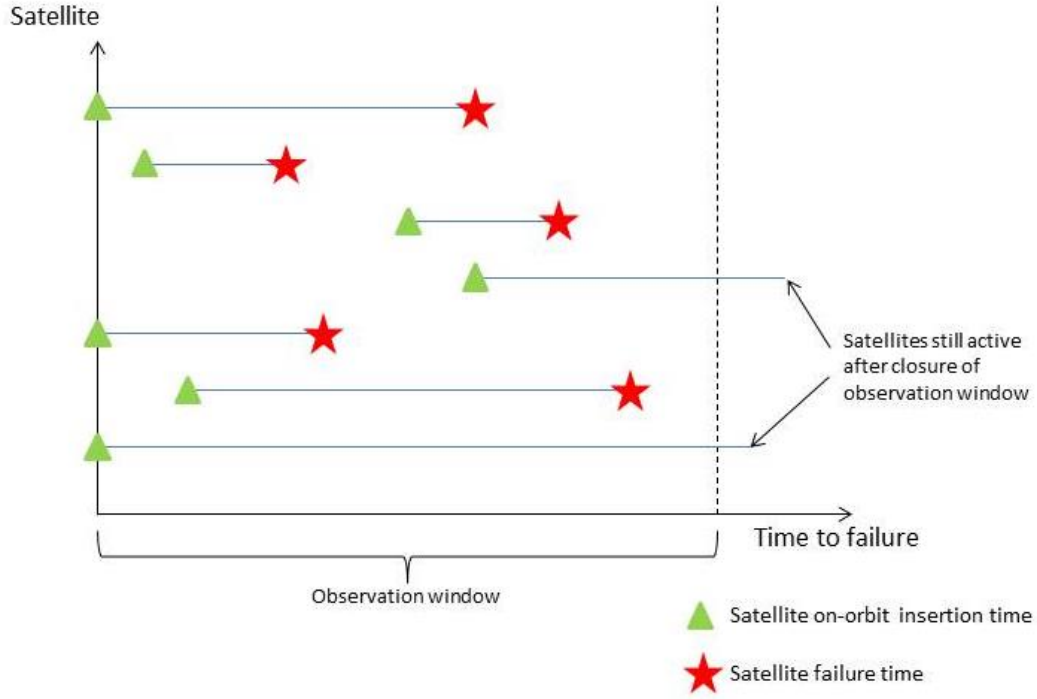


Figure 18: Representation of right censored generic data with staggered entries

4.3 Non-parametric analysis of CubeSats missions reliability

4.3.2 Kaplan-Meier estimator

The Kaplan-Maier estimator was proposed by Edward L. Kaplan and Paul Meier in a paper published in 1958, being one of the most cited works in science. The reason for this achievement is that they provide a simple solution to evaluate the true survival function of a certain population of dataset with incomplete measurements of all members of a random sample.

Different presentations of Kaplan-Maier estimator are proposed in literature. In this thesis, we provide a simple notation according to application suggested by Meeker and Escobar.

Supposing that *n* units start operating at time zero, if a unit does not fail in interval *I*, it is either censored at the end of interval *I* or it continues to operate into interval *i+1*. Information is available on the status of the unit at the end of each interval. First, all failure times shall be collected and arranged in ascending order. Assuming that censoring takes place, only *m* failure times (with m<n) are observed. It is necessary to define the size of *risk set*, the number of units that are alive at the beginning of interval *i* (i.e., those at risk to failure), because each $t_{(i)}$ can represent either failure or censoring time. The size of risk set is:

$$n_i = n - \sum_{j=0}^{i-1} d_j - \sum_{j=0}^{i-1} r_j \qquad i = 1, \dots, m \tag{4.1}$$

Where:

- n denote the number of operational units right before t_j
- d_j denote the number of units that failed in the *j-th* interval $(t_{j-1}, t_j]$
- r_j denote the number of units that survive interval *j* and are right-censored at t_j
- m is the number of intervals (i.e., number of observed failures)

4 CUBESATS MISSIONS RELIABILITY

Kaplan and Meier denoted that

$$\hat{p}_i = \frac{n_i - 1}{n_i} \qquad i = 1, \dots, m \tag{4.2}$$

is the estimator of the conditional probability of failing in interval *i*, given that a unit enters this interval. More precisely:

$$\hat{p}_i \text{ estimate of } P\left(T_F > t_{(i)} + \delta_t | T_F > t_{(i)}\right) \tag{4.3}$$

The other major contribution of Kaplan and Meier was to notice that:

$$\begin{aligned} P\left(T_F > t_{(i)}\right) = P(T_F > \delta_t) \text{ x } P\left(T_F > t_1 + \delta_t | T_F > t_{(1)}\right) \\ \text{x } P\left(T_F > t_2 + \delta_t | T_F > t_{(2)}\right) \text{ x } \dots \text{ x } P\left(T_F > t_{(i)} + \delta_t | T_F > t_{(i)}\right) \end{aligned} \tag{4.4}$$

Substituting equation (3.2) on the right-hand side of equation (3.4) and recalling the definition of Reliability, we derive the Kaplan-Meier estimator of the reliability function for censored data:

$$R_{(t)} \equiv P(T_F > t) \tag{4.5}$$

$$\hat{R}_{(t)} = \prod_{\forall i | t_{(i)} \leq t} \hat{p}_i = \prod_{\forall i | t_{8i)} \leq t} \frac{n_i - 1}{n_i} \tag{4.6}$$

It is necessary then to take into account possible special cases on dataset. In particular, two cases can be faced and they are handled as following:

- If more than one failure takes place at the same time t_i, we observe multiplicity of *m* (i.e., m_i units failing at the same time). In this case, equation 4.2 is replaced by:

$$\hat{p}_i = \frac{n_i - m_i}{n_i} \tag{4.7}$$

- If censoring time is exactly equal to a failure time t_i, then it is assumed that censoring time takes place immediately after the failure, because it is considered that a unit that is censored at a given time can survive an infinitely small period of time.

4.3.3 Kaplan-Meier plot for CubeSats Reliability

We apply the Kaplan-Meier estimator previously defined to the dataset from the CubeSats database. We have a sample of 113 CubeSats corresponding to all launched CubeSats until December 2013 from which data about failures is available. In the sample, 36 CubeSats have been affected by a failure. The ordered number of failure and censoring times in days of all these satellites is provided in Table 4.

4 CUBESATS MISSIONS RELIABILITY

Table 4: Failure and censoring times and quantity of launched CubeSats between June 2003 and December 2013

Time [days]	Nº failures	Nº censored	Time [days]	Nº failures	Nº censored
0	15	8	665	0	1
30	5	17	670	2	0
25	0	2	790	0	4
60	2	0	820	0	1
90	3	0	880	0	1
95	1	0	940	0	1
120	3	0	1095	0	5
125	1	0	1125	0	2
155	0	1	1245	0	1
185	2	0	1430	0	1
210	1	1	1550	0	2
215	1	0	1670	0	1
140	0	5	3065	0	4
300	0	1	2430	0	4
455	0	7	2555	0	1
515	0	3	2980	0	1
545	0	1	3830	0	1

The first point to be addressed before proceeding with reliability evaluation is to deal with staggered entry of all data. Obviously, CubeSats have not been inserted into orbit at the same time. Hence, for the reliability assessment the insertion of all CubeSats have been set at the same t=0 in the time scale, as if all of them were launched and inserted into orbit at the same instant of time. In this way, it has been possible to analyse the data with the same time reference. Using data gathered in Table 4 in equation 4.6 and equation 4.7, the CubeSats' mission reliability evaluation is conducted.

4.3 Non-parametric analysis of CubeSats missions reliability

The Kaplan-Meier plot of CubeSats reliability is shown in Figure 19.

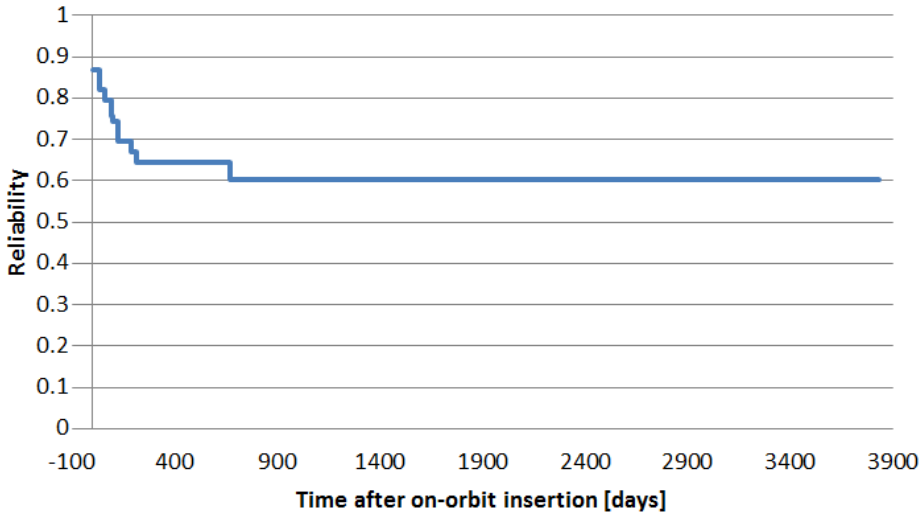


Figure 19: Kaplan-Meier plot of CubeSats reliability

Figure 19 reads as follow: for example, after a successful launch, CubeSats reliability drops down to approximately 69% after six months. In particular:

$R_{(t)} = 0.69497$ for t=185 days

After one and a half year, the CubeSats observed reliability drop down to 64%. Exact results for each time value detailed in Table 4 are provided in Table 5.

Table 5: CubeSats observed reliability

Time [days]	Reliability	Time [days]	Reliability	Time [days]	Reliability
0	0.867257	140	0.644182	1125	0.603921
30	0.819076	300	0.644182	1245	0.603921
25	0.819076	455	0.644182	1430	0.603921
60	0.794255	515	0.644182	1550	0.603921
90	0.757025	545	0.644182	1670	0.603921
95	0.744614	665	0.644182	3065	0.603921
120	0.707384	670	0.603921	2430	0.603921
125	0.694973	790	0.603921	2555	0.603921
155	0.64973	820	0.603921	2980	0.603921
185	0.669702	880	0.603921	3830	0.603921
210	0.657066	940	0.603921	-	-
215	0.644182	1095	0.603921	-	-

4 CUBESATS MISSIONS RELIABILITY

Remarkable outputs are obtained from the previous analysis. First of all, the observed reliability of CubeSats suddenly decreases down to 86% just at the beginning of the mission. This decrease of the reliability is due to the fact that a remarkable number of CubeSats failed just after insertion into orbit (hence, they are probably affected by infant mortality). As can be observed, 15 of 36 failures took place just after the expulsion from the deployer. Secondly, reliability drop stabilises after certain time of about 3 years. Two main reasons are the possible causes for this event: 1) most of the failures took place on CubeSats during the first years of operations and 2) CubeSats missions are usually designed for a 1-2 years mission life and thus, most of them arrived at the end of the mission within 3 years.

4.3.4 Confidence intervals

A point estimate (in our case Kaplan-Meier estimator), by itself, can be misleading, as it may or may not be close to the quantity being estimated. Indeed, it gives the maximum likelihood of reliability but no information regarding the dispersion around $\hat{R}_{(t)}$. Then, confidence intervals are one of the most useful ways of quantifying uncertainty due to "sampling error" arising from limited sample sizes. Confidence intervals have a specified "level of confidence", typically 90% or 95%, expressing one's confidence that a specific interval contains the quantity of interest.

To calculate the confidence intervals, the calculation of variance or standard deviation to derive upper and lower bounds is required. In particular, as suggested by Meeker and Escobar [1], we use Greenwood's Formula to evaluate the Kaplan-Meier estimator variance. The Greenwood's Formula states as:

$$\widehat{Var}_{\left[\hat{R}_{t_{(i)}}\right]} = \left[\hat{R}_{(t_{(i)})}\right]^2 \sum_{j=1}^{i} \frac{\hat{p}_j}{n_j\left(1-\hat{p}_j\right)} \tag{4.8}$$

Then, the 95% confidence interval is determined by the following equation:

$$R_{95\%(t_i)} = \hat{R}_{(t_i)} \pm 1.96\widehat{Var}_{\left[\hat{R}_{t_{(i)}}\right]} \tag{4.9}$$

4.3 Non-parametric analysis of CubeSats missions reliability

Equations (4.8) and (4.9) have been applied to the dataset of CubeSats failures together with Kaplan-Maier estimated CubeSats reliability. The obtained 95% confidence interval curves are shown in Figure 20.

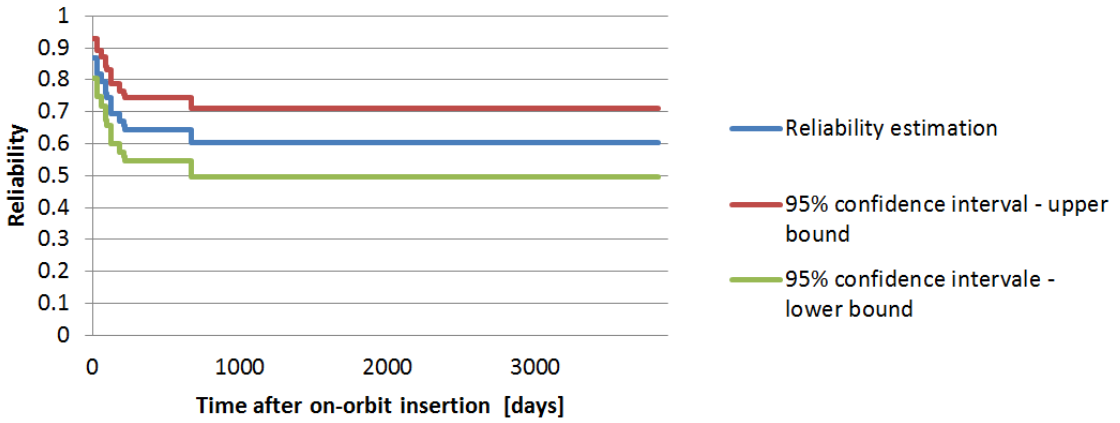


Figure 20: CubeSats reliability estimation with 95% confidence interval

Figure 20 reads as follow: after, for example, six months the observed CubeSats reliability is between 57.3% and 76.6% with a 95% of likelihood. These two values are the lower and upper 95% confidence levels. Moreover, the most likely estimation of observed CubeSats reliability for t=6months is 69.5% approximately.

As can be observed in Figure 20, the dispersion of reliability around $\hat{R}_{(t)}$ increase with time increasing. This event can be observed by the gap growing between both upper and lower bounds of confidence interval. The dispersion assessment is reported in Figure 21, as percentage of gap between both limits as time increases. The value is calculated with equation (4.10).

$$D_{(t_i)} = \left[upper\ bound\ R_{95\%(t_i)}\right] - \left[lower\ bound\ R_{95\%(t_i)}\right] = \\ = 3.92\sqrt{\widehat{Var}_{\left[\hat{R}_{t_{(i)}}\right]}} = 3.92\left[\hat{R}_{95\%(t_i)}\right]\sqrt{\sum_{j\le i}\frac{m_j}{n_j(n_j-m_j)}} \quad (4.10)$$

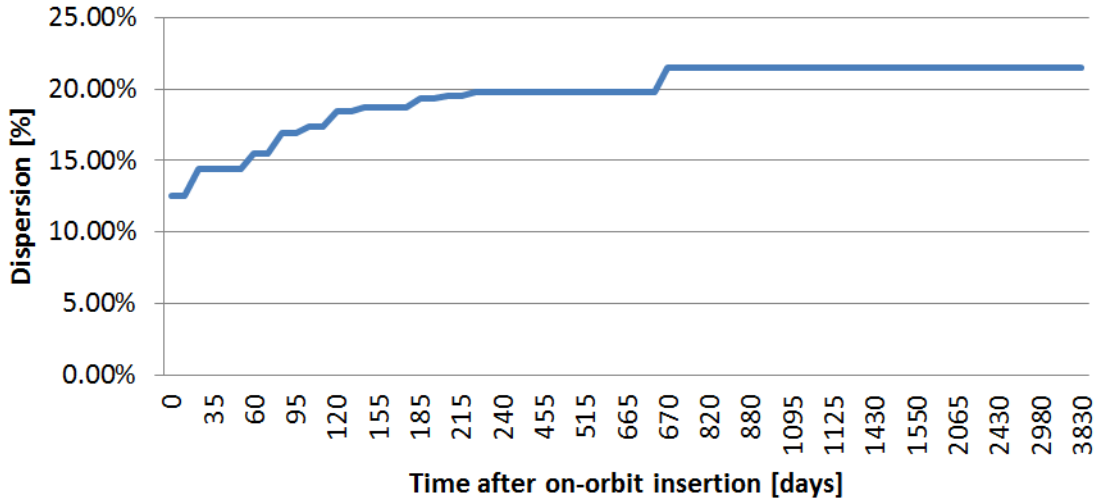


Figure 21: Dispersion of 95% confidence interval of observed CubeSats reliability

It is shown that the higher the time after on-orbit insertion, the higher the dispersion around $\hat{R}_{(t)}$. This fact is mainly due to relatively reduced amount of data. Unfortunately, this drawback cannot be faced until more data will be available.

4.4 Parametric analysis of CubeSats missions reliability

Non-parametric analysis is a powerful tool because no probability distribution of the studied dataset shall be predefined before the analysis. However, some weaknesses arise when using this type of analysis, as stated in section 4.3. To cope with these drawbacks, a parametric analysis of CubeSats data is conducted and detailed in this section.

Previous non-parametric analysis suggested that observed CubeSat reliability follows a Weibull distribution. To verify this statement and, if confirmed, calculate the two parameters of basic Weibull distribution, two techniques have been used: first, Weibull plot and then Maximum Likelihood Estimator. Before addressing these two points, a recall of Weibull distribution is reported.

4.4.1 Weibull distribution

Weibull distribution is one of the most widely used lifetime distributions in engineering. It is used when data cannot be represented linearly with time. Moreover, it gives high flexibility

and, with an appropriate selection of shape parameter γ (as it will be shown later), it can take on the characteristics of other type of distributions. More precisely, the Weibull distribution can model an increasing failure rate, a decreasing failure rate (infant mortality), and constant failure rate (i.e., an exponential distribution).

Weibull distribution is characterised by two parameters, the shape parameter γ, dimensionless, and the characteristic life θ, expressed in unit of time (usually years). For this type of distribution, the failure rate, p.d.f. and reliability adopt the following expressions:

$$\lambda_{(t)} = \frac{\gamma}{\theta}\left(\frac{t}{\theta}\right)^{\gamma-1} \tag{4.11}$$

$$f_{(t)} = \frac{\gamma}{\theta}\left(\frac{t}{\theta}\right)^{\gamma-1} e^{-\left(\frac{t}{\theta}\right)^{\gamma}} \quad t > 0 \tag{4.12}$$

$$R_{(t)} = e^{-\left(\frac{t}{\theta}\right)^{\gamma}} \tag{4.13}$$

The variation of shape parameter γ is detailed in Table 6, which points out the flexibility of this distribution:

Table 6: Weibull distribution characteristics with respect to different β values

γ value	Model characteristics	Representation
0<γ<1	As t→0, $f_{(t)}$→∞	Infant mortality
γ=1	As t→∞, $f_{(t)}$→0 $f_{(t)}$ decreases monotonically	Exponential distribution
1<γ<2	$f_{(t)}$=0 at t=0	Increasing concave λ
γ=2	$f_{(t)}$ increases until certain time when starts decreasing	Rayleigh distribution
γ>2		Increasing convex λ
2.6<γ<3.7		Normal distribution

A graphical representation of Weibull distribution for different shape parameter γ with fixed characteristic life $\theta = 1\ year$ can be observed in Figure 22.

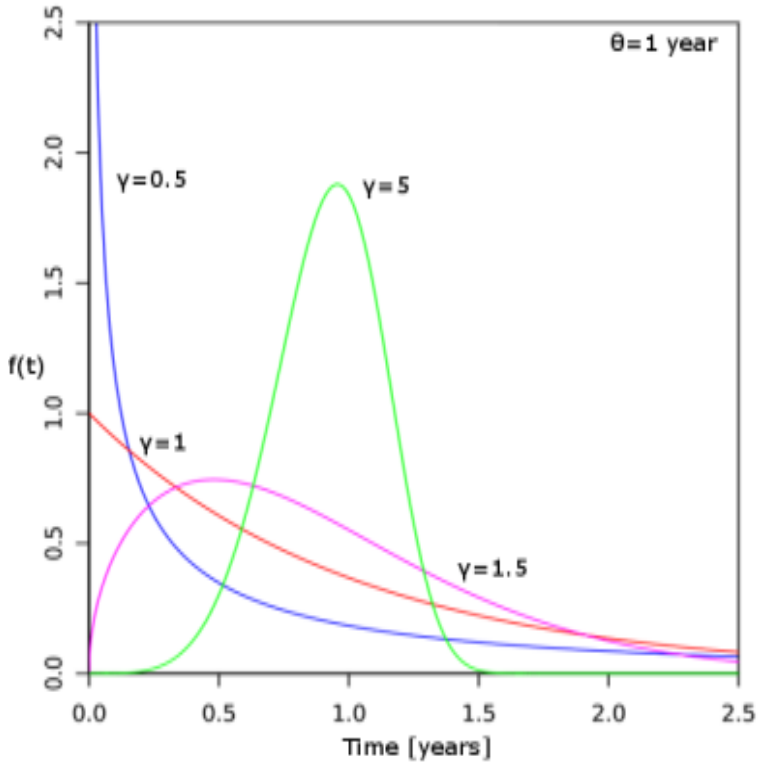


Figure 22: Weibull distribution for different γ values with fixed $\theta = 1\ year$

4.4.2 Weibull plot

The Weibull plot is a graphical technique widely used to assess if dataset follows Weibull distribution. The concept which states on the basis of the Weibull plot is the following: after appropriate operation on reliability expression of Weibull distribution (as explained later on this section), if the data follows a linear trend, then this data follows a Weibull distribution.

Applying the natural logarithm in both sides of reliability expression for Weibull distribution (i.e., eq. (4.13)):

$$ln\left(R_{(t)}\right) = -\left(\frac{t}{\theta}\right)^{\gamma} \tag{4.14}$$

4.4 Parametric analysis of CubeSats missions reliability

Then, taking again the natural logarithm of the negative of the two sides of the previous equation (4.14), we obtain:

$$ln\left[-ln\left(R_{(t)}\right)\right] = \gamma ln(t) - \gamma ln(\theta) \tag{4.15}$$

At this point, a change of variable is applied at equation (4.15):

$$\begin{cases} y = ln\left[-ln\left(R_{(t)}\right)\right] \\ x = ln(t) \end{cases} \tag{4.16}$$

The obtained expression is the equation of a line with the slope equal to the shape parameter γ:

$$y = \gamma x - \gamma ln(\theta) \tag{4.17}$$

The obtained equation (4.17) is equivalent to equation (4.14). These operations are useful from the moment when we would like to determine if the dataset we are working with follows a Weibull distribution. Through non-parametric analysis it has been obtained the estimation of observed CubeSats mission reliability $\hat{R}_{(t_i)}$. We therefore can plot $y = ln\left[-ln\left(\hat{R}_{(t_i)}\right)\right]$ individuated in expression (4.16) as a function of natural logarithm of the time from into orbit insertion (i.e., $ln(t_i)$). If these discrete points, which are the observed failure times gathered in the database, follows a linear or quasi-linear trend, then it can be affirmed that the data we are dealing with follows a Weibull distribution.

Then, from the expression of the regression line of the plotted data it could be possible to obtain shape parameter γ from the slope of the curve and characteristic life θ as the intersection of the line with the y axis. Hence, least-square fit is used to provide an approximation of the line's equation and evaluate both Weibull parameters. The Weibull plot of our data with regression line and line's equation is shown in Figure 23.

4 CUBESATS MISSIONS RELIABILITY

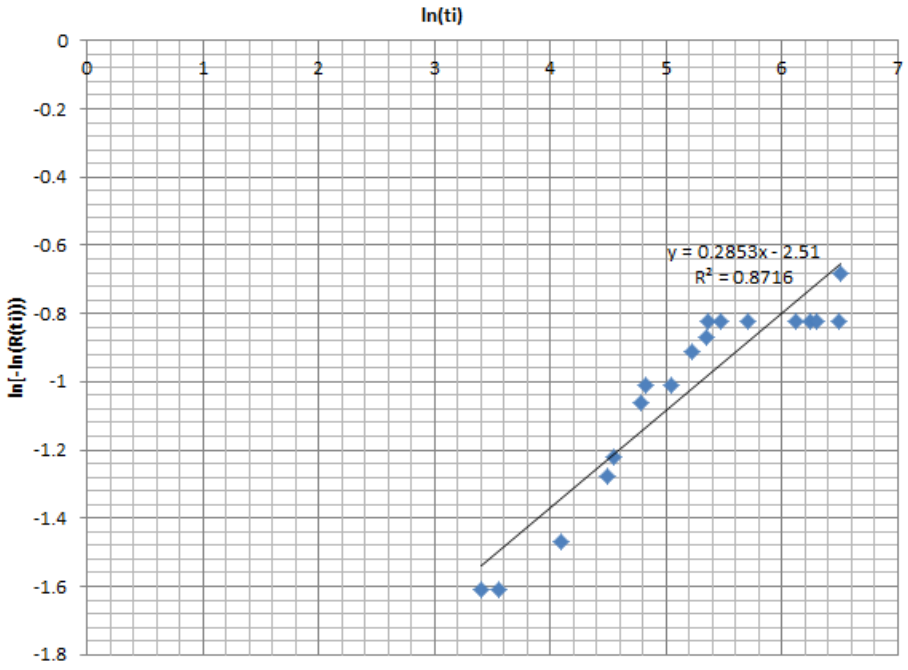


Figure 23: Weibull plot of Kaplan-Meier observed CubeSats Reliability

As it can be observed, failures occurred at t=0 (i.e., the CubeSat have been never operated) were withdrawn from the study. This action was conducted because the insertion of these satellites in the plot would biased the results because ln(0)→∞ with the assumption that the CubeSats were functionally operative before the deployment. However, these CubeSats were never started to operate; then, they failed already before starting the operative phase and hence, the failure took place before the insertion into orbit.

The results drawn in Figure 23 are well aligned, and a regression analysis provides the following results:

$$y = 0.2853x - 2.51 \qquad \text{with } R^2 = 0.8716$$

These results provide good indication that analysed data follows Weibull distribution. At the beginning of this section it has been stated that, from non-parametric analysis, it seemed that observed CubeSats reliability follows a Weibull distribution. After the present evaluation, this statement can be effectively affirmed.

4.4 Parametric analysis of CubeSats missions reliability

As a result of the previous analysis, shape parameter and characteristic life has been obtained. Concretely:

$$\gamma = 0.2853 \qquad\qquad \theta = 6619.4\ years$$

First result observed is, as expected, a shape parameter quite lower than 1. This indicates an important role of infant mortality on CubeSats reliability. A comparison between observed CubeSat reliability calculated with Kaplan-Meier estimator and plot of Weibull distribution with obtained shape parameter and characteristic life by means of Weibull plot is shown in Figure 24.

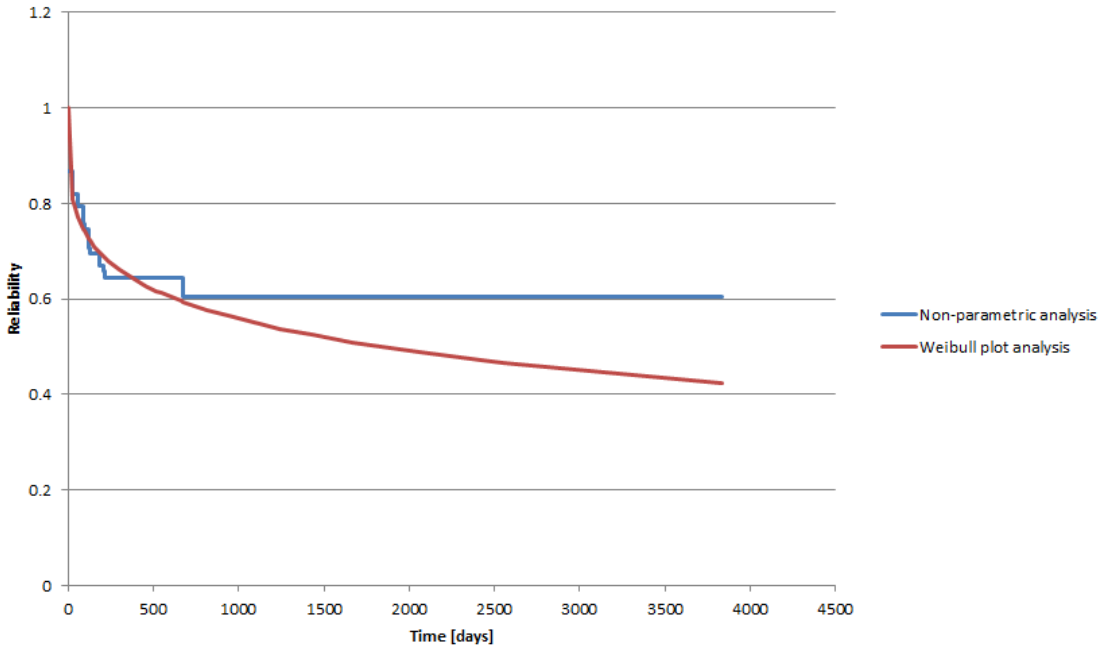


Figure 24: Kaplan-Meier estimated observed CubeSats reliability and Weibull distribution

The comparison shown in Figure 24 points out that CubeSats reliability follows Weibull distribution during first two years after insertion into orbit. After this period, the lack of data (i.e., only few CubeSats still remain operative and then, the sample size is extremely small) causes a divergence between observed reliability calculated with non-parametric analysis and Weibull distribution. These results are also confirmed by the coefficient of determination obtained from the regression line obtained in the Weibull plot (i.e., $R^2 = 0.8716$), which

indicates that data can be quietly approximated by the Weibull distribution, even if the value is not quite near to the unit.

Then, the interest of the models remains within the years and a half, as shown in , where Weibull model follows the observed reliability. Indeed, during this period, as can be observed, this value of Weibull model remains within 4 percentage points of the observed reliability.

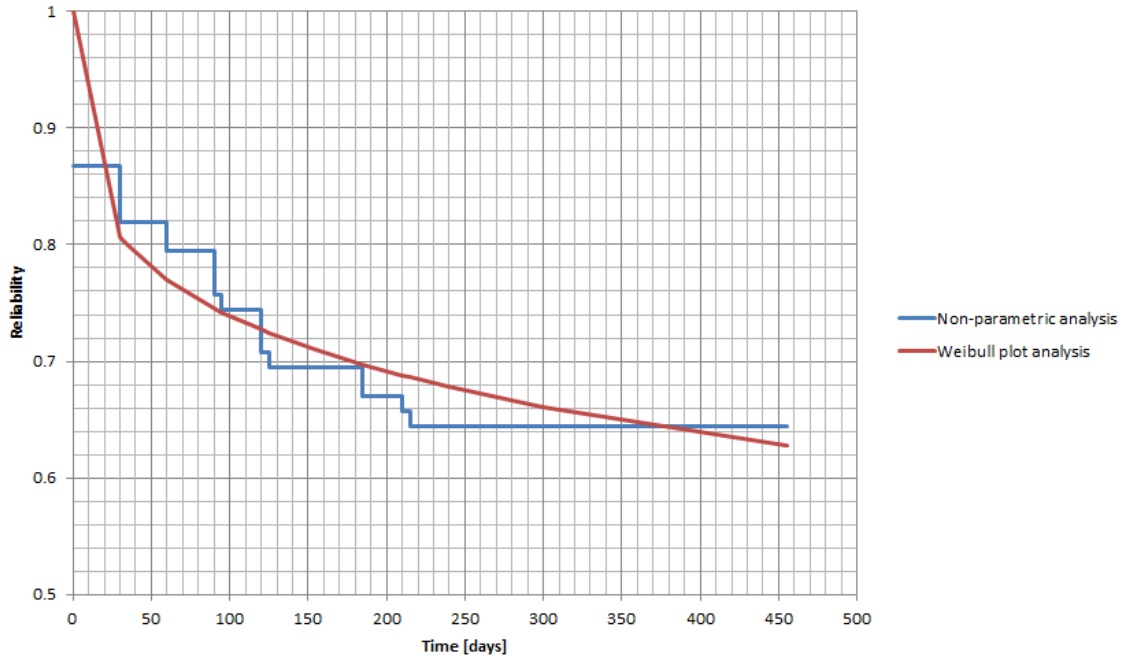


Figure 25: Kaplan-Meier estimated observed CubeSat reliability and Weibull distribution (1.5 years)

4.4.3 Maximum Likelihood Estimator (MLE) for Weibull distribution

The Maximum Likelihood Estimator (MLE) is a method for estimating the parameters of a probability distribution based on the likelihood function. The likelihood function is the joint probability of an observed sample as a function of the unknown parameters. The MLE is based on the concept that the values of the parameters that maximise the likelihood function are the "best" estimates.

Thus, the objective is then to determine the best estimates of the parameters using the likelihood function. This is accomplished by developing the likelihood function for the observations and obtaining its logarithmic expression. Then, this logarithmic expression is

differentiated with respect to the unknown parameters and set the expressions equal to zero. These expressions are then solved simultaneously to obtain the best estimates of the parameters that maximise the likelihood function.

In section 4.4.1 probability distribution function and reliability function of Weibull distribution was presented as:

$$\lambda_{(t)} = \frac{\gamma}{\theta}\left(\frac{t}{\theta}\right)^{\gamma-1} \tag{4.18}$$

$$R_{(t)} = e^{-\left(\frac{t}{\theta}\right)^{\gamma}} \tag{4.19}$$

Where γ is the shape parameter and θ is the characteristic life.

In previous sections it has been demonstrated that the data under evaluation follows Weibull distribution. New, the MLE method is used to estimate both parameters. The likelihood function of Weibull distribution for data subjected to right-censoring is:

$$L_{(\gamma,\theta,t)} = \prod_{i=1}^{n}\left[\frac{\gamma}{\theta}\left(\frac{t_i}{\theta}\right)^{\gamma-1} e^{-\left(t_i/\theta\right)^{\gamma}}\right]\prod_{j=1}^{m}\left[e^{-\left(t_i/\theta\right)^{\gamma}}\right] \tag{4.11}$$

Where n is the total number of observed failures, and m is the total number of censored CubeSats. To fit the parameters that maximise the likelihood function, the derivatives of the logarithmic function (i.e., $l_{(\gamma,\theta,t)} = ln\left(L_{(\gamma,\theta,t)}\right)$) of equation (4.11) with respect to γ and θ. This procedure results in the following equations, where $\hat{\gamma}$ and $\hat{\theta}$ are the estimated shape parameter and characteristic life, respectively:

$$\frac{\partial l}{\partial \gamma} = \frac{n\theta^{\gamma}}{\gamma}\left(\frac{1}{\theta^{\gamma}} - \frac{\gamma ln(\theta)}{\theta^{\gamma}}\right) + \sum_{i=1}^{n}\left[ln(t_i) - \left(\frac{t_i}{\theta}\right)^{\gamma} ln\left(\frac{t_i}{\theta}\right)\right] - \sum_{j=1}^{m}\left[\left(\frac{t_j}{\theta}\right)^{\gamma} ln\left(\frac{t_j}{\theta}\right)\right] \tag{4.12}$$

$$\frac{\partial l}{\partial \theta} = -\frac{n\gamma}{\theta} + \sum_{i=1}^{n}\frac{\gamma t_i}{\theta^{\gamma+1}} + \sum_{j=1}^{m}\frac{\gamma t_j}{\theta^{\gamma+1}} \tag{4.13}$$

The MLE is obtained by solving previous equations simultaneously. In particular, equation (4.13) is set equal to zero and the obtained expression of $\hat{\theta}$ is substituted in equation (4.12). This equation is then solved using Newton-Raphson method to obtain $\hat{\gamma}$. Once the estimated value of the shape parameter is known, the estimated value of the characteristic life is then calculated substituting $\hat{\gamma}$ in equation (4.13) and solving for $\frac{\partial l}{\partial \theta} = 0$. Newton-Raphson method is described in Appendix A. In order to allow a more readable thesis. The estimated shape parameter and characteristics life using Maximum Likelihood Estimator confirmed the results from the Weibull plot.

4.5 CubeSats vs. all-satellites missions reliability

Saleh and Castet assessed the observed reliability of all satellites launched between 1990 and October 2008. The purpose of the present section is to evaluate the reliability difference between CubeSats and all type of satellites in order to give a comparison based on spacecraft mass.

The information used by Saleh and Castet was obtained from SpaceTrak database and used for the study purpose. In the study, Weibull parameters have been estimated for all satellites. These parameters are:

$$\hat{\theta} = 8316\ years \text{ and } \hat{\gamma} = 0.3875$$

A graphical comparison of estimated reliability of satellites classified by divided by mass is shown in Figure 26.

4.4 Parametric analysis of CubeSats missions reliability

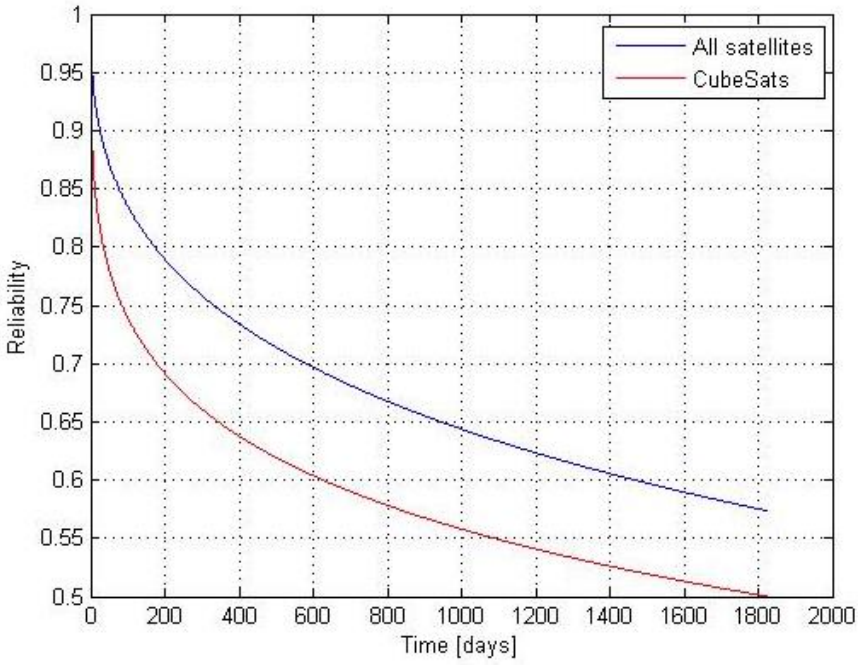


Figure 26: Estimated reliability of spacecraft assessed by Weibull fit (all satellites vs. CubeSats)

It is clearly evident that the reliability of CubeSats is considerably lower than those for all satellites. Thus, it is imperative to adopt actions to increase CubeSat's reliability and CubeSat's mission rate of success.

5

SPACE SYSTEMS LIFE-CYCLE AND RELIABILITY INCREASE

5.1 Identification of activities for reliability increase

The analysis of CubeSats missions highlighted a considerable number of failures occurred on this type of satellites. Thus, it is absolutely necessary to increase missions' rate of success. An analysis of differences between conventional satellites and CubeSats was conducted to determine where the attention should be focused to increase CubeSats reliability and their mission rate of success.

Conventional satellites usually have a low tolerance against risk. Hence, as shown in Figure 27, this characteristic led to an increase of reliability mainly achieved with high number of redundancies. As a consequence, the complexity of the satellite increases and as a consequence, design complexity increases too. Therefore, a boost of testing complexity is observed in order to verify all stated requirements. Altogether, these characteristics led to an overall mass and cost rise. Due to all this high parameters (i.e. high reliability, redundancies, complexity, mass and cost), a low risk is tolerated for this type of projects.

5 SPACE SYSTEMS LIFE-CYCLE AND RELIABILITY INCREASE

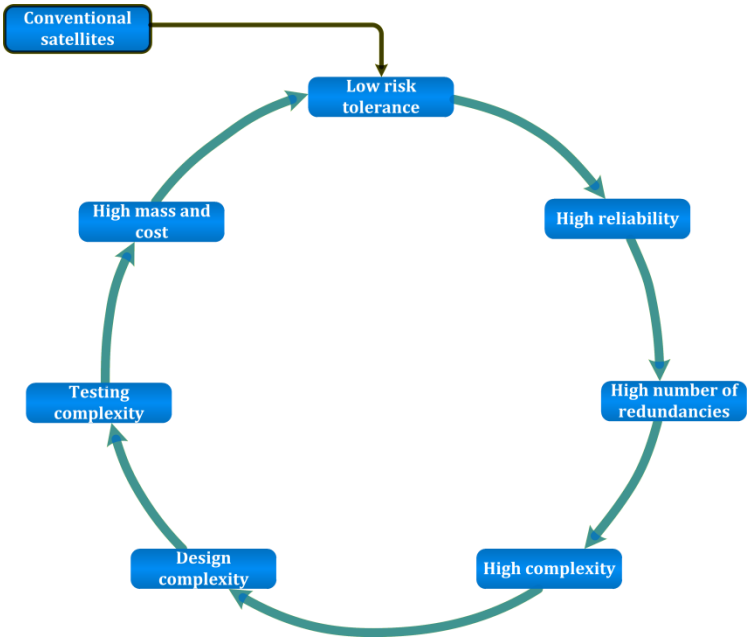


Figure 27: Consequences on conventional satellites life-cycle due to their low risk tolerance

On the other hand, as can be observed in Figure 28, traditionally small-satellites, and in particular CubeSats, are characterised to be projects that tolerate higher risk with respect to conventional satellites.

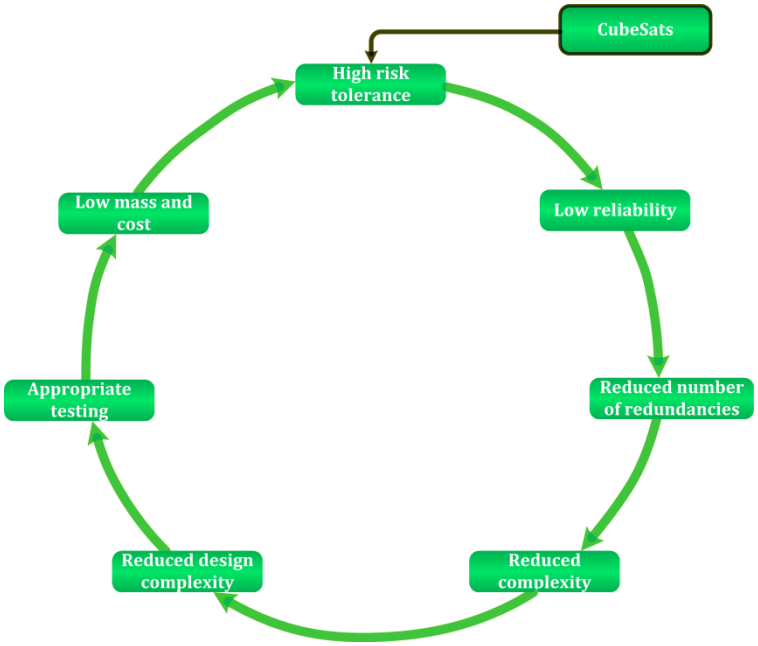


Figure 28: Consequences on CubeSats life-cycle due to their high risk tolerance

5.1 Identification of activities for reliability increase

Hence, lower reliability is observed, as described in chapter 4. One reason of the lower reliability is due to low number of redundancies that, at their time, led to a reduction of system complexity. Appropriate testing shall be then conducted for this type of satellites in order to verify the stated requirements, but maintaining the cost down. All these characteristic led to lower mass and cost spacecraft and the circle is closed accepting higher risk with respect to conventional satellites projects.

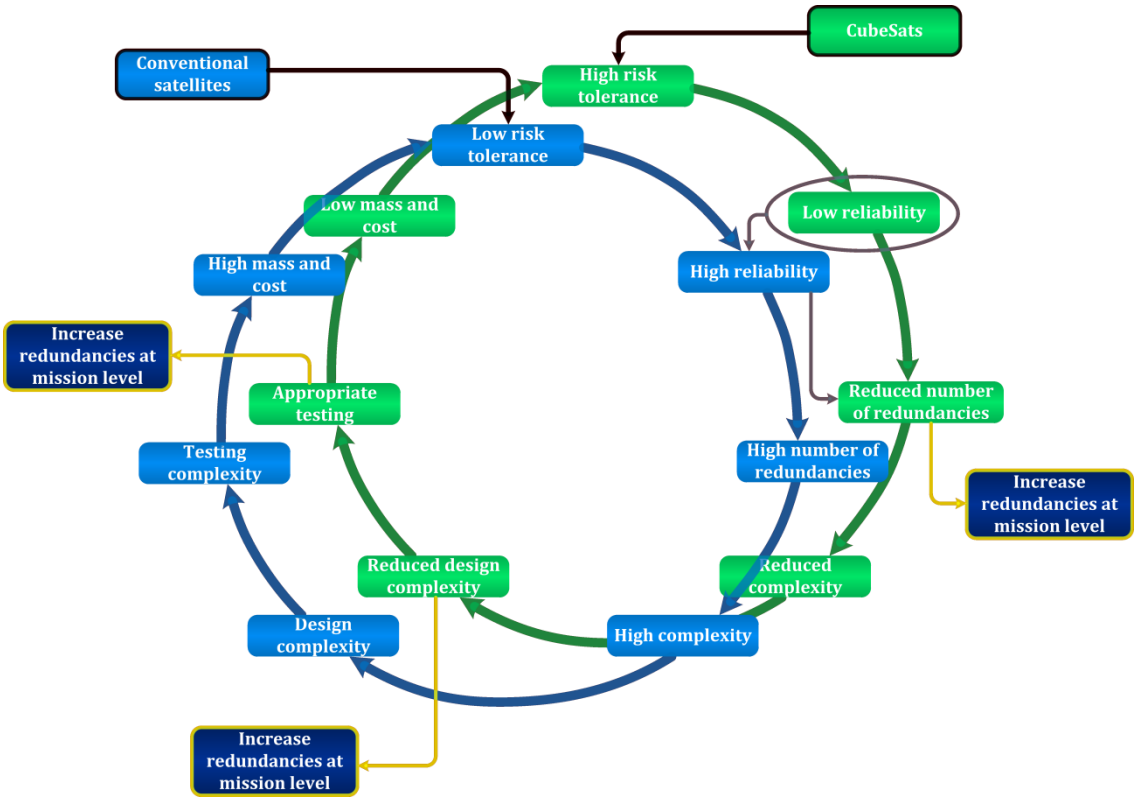


Figure 29: Three methods for CubeSat's reliability and mission rate of success increase

Considering the differences between these two types of spacecraft, three methods have been individuated to increase CubeSat's reliability and mission rate of success, as shown in Figure 29. These methods are applied at different stages of the CubeSats life-cycle, which is explained in following sections. In particular the activities are:

- Guidelines for CubeSats life-cycle activities: based on the *fault prevention technique* concept (i.e. reduce and prevent the possible failures and hence, increase mission rate of success), the objective of these activities is to assess actions to be conducted

by CubeSat developers during all phases of the project (i.e., design, manufacturing, verifications and operations). Best practices to be conducted during CubeSats life-cycle phases are identified and stated.

- Reliability increase through verification – standards tailoring: in this case *fault removal technique* applies. The use of standards to conduct verification activities is crucial to carry out them in a systematic way. However, most of them are difficult to be applied on small-satellites projects, and specially to CubeSat projects. Standards key-points for verification activities have been identified and ECSS standards have been adapted to fit CubeSats projects taking into account their main drivers (i.e., low cost and fast delivery).
- Mission-oriented reliability – redundancies at system level: based on *fault tolerance technique* concept, the research is based on the study of reliability at mission level applying redundancy techniques at system level. New mission architectures (e.g. swarm-like constellations) are individuated as architectures that can lead to achieve mission objectives even if reliability of each system (i.e. CubeSat) of the constellation remains lower than conventional satellites.

5.2 Space system life-cycle

Life-cycle activities of space projects are conducted in a system engineering approach driven by well-established phases and milestones. Depending on the organisation that is taken into account, the phases that broke down space projects are slightly different in the nomenclature, but are mostly identical in the content and milestones. A comparison between ESA and NASA space program development phases and milestones from is detailed in Figure 30.

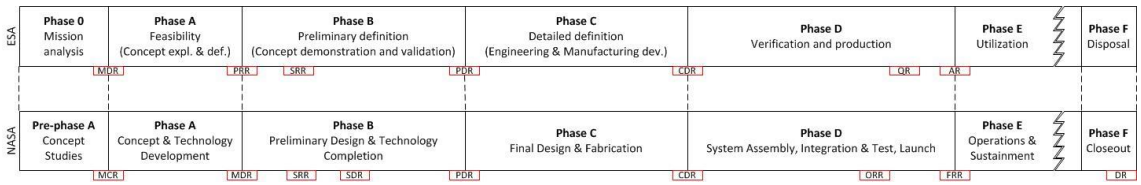


Figure 30: Space program development phases comparison (ESA, NASA, DoD)

5.2 Space system life-cycle

Duration of each phase depends on the nature of the project. Large and complex space missions can be require 10 to 15 years to complete phases A to D, and the operation phase can last from 5 to 15 years. Small-satellites instead are characterised by lower time for development (e.g. 12 to 18 months) and operations (e.g. 6 months to several years). ESA phases classification notation has been taken into account as reference.

The objectives of each of these phases are the following:

Table 7: Objectives of space program development phases

PHASE	DESCRIPTION
Phase 0	During phase 0 a high-level study is conducted. Usually different mission concepts are evaluated and assessed prior the final one is selected in phase A.
Phase A	In this phase the selection of an optimum and cost-effective system concept from different number of possible options that are considered is conducted. Moreover, it is conducted a feasibility demonstration of the project by means of design and analysis. Finally, in this phase is required to conduct a technical solution definition that shall allow to conduct a realistic performance, schedule, planning and cost data study for all subsequent phases. Generally, the outputs of phase A are preliminary information on mission, launcher, payload requirements and target performance specification. Usually, phases 0 and A have a relative low-cost impact on the budget in terms of real spent money. However, the cost implications from the decisions took in these phases in the future is remarkable. Ultimate cost of the mission will depend on decisions taken during early phases of the design.

Phase B	Three main objectives shall be achieved in this phase. First, the definition of the system and subsystem designs in a certain detail in order to allow to proceed with the minimum of problems to conduct the detail design during phase C. Second, subsystem requirements and design specifications, subsystem and equipment design and development plans, programme schedules and a full proposal for next phase are produced. Finally, some advanced activities of phase C are initiated (e.g. detailed design of critical parts)
Phase C	Usually, this is one of the longest phases. It encompasses development and manufacture. Specifically, during this phase detailed design and analyses are completed. Moreover, preparation of manufacturing drawings and special procedures, and manufacture execution are conducted. Prototypes are manufactured and tested at this phase
Phase D	Phase D is also known as Assembly, Integration and Verification phase. As the previous expression indicates, during this phase the assembly and integration of components and subsystems are conducted to obtain the system. Moreover qualification and acceptance verifications are conducted to flight hardware
Phase E	This phase encompasses delivery of the spacecraft to the launch site and support of the launch campaign as well as in-orbit operations
Phase F	During phase F disposal activities are conducted. The objective of this phase is to implement the disposal plan defined during design phases, document lessons learned and produce baseline mission report

To achieve the abovementioned objectives, certain activities shall be conducted during spacecraft life-cycle. Concretely, technical activities of a project life-cycle can be represented by the well-known Vee-shaped model, as represented in Figure 31. The higher level inputs are

the stakeholder requirements and constraints which are used to define mission statement and objectives, and the input requirements and constraints are analysed, elicited and refined.

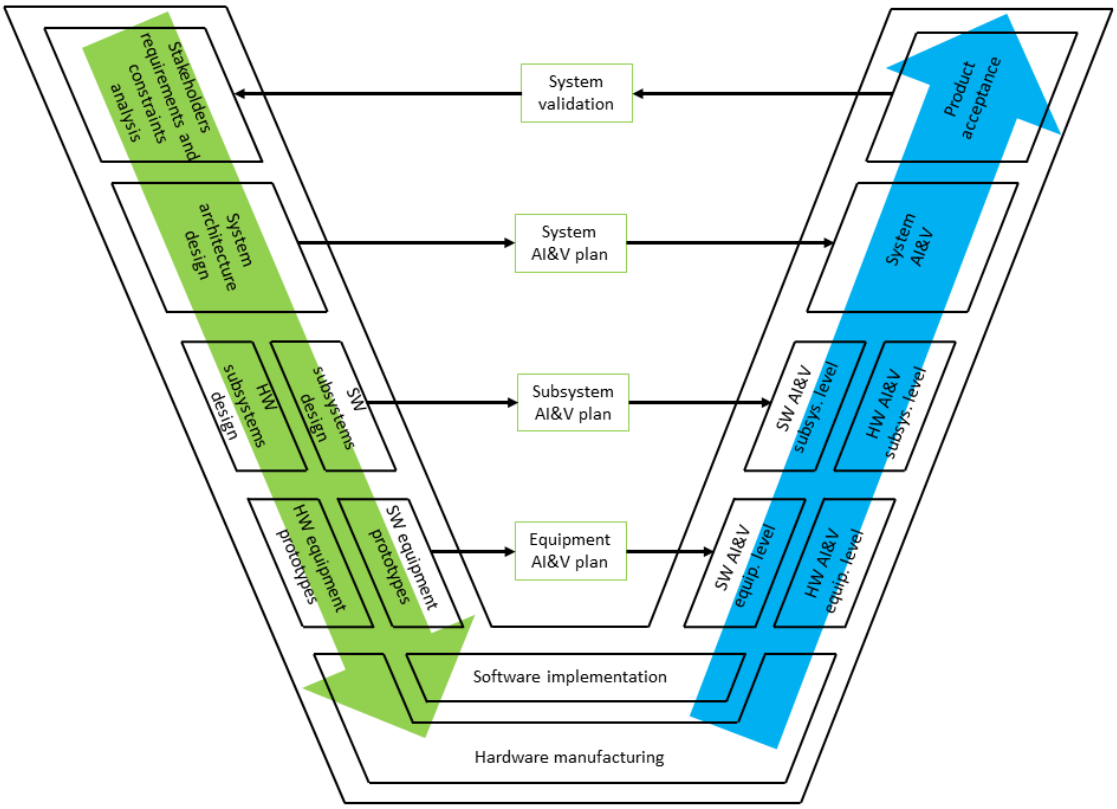


Figure 31: Vee-shaped model

The obtained outputs are moved as inputs to the next step, at which the system architecture design is conducted. Several steps are conducted to refine system functions and allocating them to the different components of the system. The next level the design of subsystems is conducted, defining requirements and developing models (i.e. software models, prototype hardware models, etc.). Last step of design encompasses equipment design. The activities that apply are similar to those conducted at system and subsystem level, but focusing the attention to the components.

Once all the design is completed, the hardware items are manufactured and the software modules are implemented. At the end of the process both hardware and software is available

for verification activities. Some unit testing may be performed in parallel with implementation, especially for software.

The right branch of the Vee-shaped model includes all activities related to assembly, integration and verification. Integration is conducted at various levels (i.e. components, subsystem and system). While assembly and integration is conducted, verifications are performed in parallel. First, at component level the software is integrated and verified. Then, components are assembled and integrated to obtain subsystems that are verified. Finally, all subsystems are also assembled and integrated to obtain the final flight system that is verified at system level. At the end of the process, all the requirements stated during the design steps (i.e. left side of the Vee-shaped model) shall be verified and closed out. Last step consists on product acceptance that validates the system and demonstrates to stakeholders that the spacecraft fulfils their requirements and constraints.

The verification activities conducted on the right branch of the model are defined and planned during design phases. Indeed, one of the outputs on each step on the left-side of the model is the verification matrix, which details all the requirements, the verification method and the level at which it shall be verified. This input is used to define and plan the verification campaigns that are conducted during verification phase.

5.2.1 Verification methods

Different methods are available to accomplish verifications. It is up to AIV engineer(s) that is(are) developing verification plans to establish, together with engineers in charge of the design, the method(s) that will be used to verify each requirement. The methods available to conduct verifications are four, as detailed in Table 8.

Table 8: Verification methods

METHOD	DESCRIPTION
Test (T)	It is a verification method in which technical means, such as special equipment, instrumentation, simulation techniques, or the application of established principles and procedures, are used for the evaluation of the system, subsystems and/or equipment to determine compliance with requirements at any level of assembly within the system assembly hierarchy. To conduct tests, the use of elaborate instrumentation and special test equipment to measure the parameters that characterise the requirements may be used. Then, data obtained from tests is analysed as an integral part of the test program (note: not to be confused with "analysis" as verification method explained later on). Normally, testing is the preferred method for requirements verification and it is usually used in three main cases: 1) analytical techniques do not produce adequate results, 2) presence of certain failure modes that could compromise personnel safety, adversely affect flight systems or payload operations, or can induce the loss of the mission, 3) for components that are directly associated with critical system interfaces. Tests can be generally divided in two main groups: 1. Functional tests: electrical or mechanical performance tests conducted on flight or flight-configured hardware and/or software at conditions equal to or less than design specifications. Its purpose is to establish that the satellite performs satisfactorily in accordance with design and performance specifications. Functional tests normally are performed at ambient conditions. Moreover functional tests (or reduced functional tests) are conducted before and after each environmental test or major move in order to verify system performance prior to the next test/operation. 2. Environmental tests: usually performed on flight or flight-configured

	hardware and/or software to assure the satellite will operate correctly in its flight environment. These kinds of tests usually include vibration, acoustic and thermal vacuum tests. Furthermore, environmental tests are normally combined with functional tests to verify correct functionality while the satellite is subjected to specific flight environment.
Analysis (A)	Analysis is the assessment of data by generally accepted analytical techniques to determine that the satellite meets specified requirements. Analysis techniques encompass wide range of activities: statistics evaluations, CAD modelling, computer and hardware simulations, etc. Generally, this technique is used when tests cannot adequately or cost-effectively address all the conditions under which the system must perform it, or when certain requirement cannot be verified without analysis.
Inspection (I)	Inspection determines requirements close-out by the visual examination of the satellite using standard quality control methods, without the use of special laboratory procedures or equipment. Direct physical attribute examinations, such as check-out, dimensions, weight, physical characteristics, etc., are the classical inspection activities.
Review of Design (RoD)	Review of Design is a method that encompasses activities mainly related to documentation review. Examinations of drawings, design documentation, software version descriptions, computer program code are classical activities of the review of design process. These activities are generally conducted during Preliminary and Critical Design Reviews.

6

LIFE-CYCLE GOOD PRACTICES

The previous study highlighted the need to identify ways to increase the reliability of CubeSats and the mission rate of success. One way to do so, as already introduced before, is to conduct precise activities that could help to increase the previous mentioned parameters. To be able to identify the best activities to be conducted during all phases of CubeSat's life-cycle, a wide and detailed questionnaire has been prepared (see Appendix B). This questionnaire was then distributed to all CubeSats developers requiring them to give detailed information regarding their projects.

6.1 Questionnaire content

The purpose of this study was to gather as much information as possible about all the activities conducted in the whole life-cycle of CubeSat by the developers. The survey was divided in five sections:

1. General information: this section is devoted to gather general information about the spacecraft such as CubeSat type, launch information, objectives and mission description among other.
2. Design information: inputs regarding design phase are requested in this section. The developed models and activities conducted during phase B and C are gathered.
3. Handling information: actions taken during the handling of the CubeSat. Particularly, the information about the protections adopted if the CubeSat should be brought among different facilities
4. Verification: this section aims at gathering information about all the activities related to the verification campaign. Concretely, it has been divided in three sub-sections:

a. Preparation: information about the verification campaign preparation is requested. Concretely, information about the verification planning and set-up has been asked.
b. Execution: in this sub-section information regarding verification input values (e.g. temperature ranges, number of sensors, etc.) as well as justification about this values is required
c. Results: the results of the verification campaign are asked (e.g. if failures have been observed, during what tests, etc.).

5. Integration into the deployer and operations: all the information about the activities after the CubeSat has been integrated into the deployer as well as the activities and results of the operations are required.

6.2 Questionnaire feedbacks

The questionnaire was distributed to all CubeSat developers that, at the moment of the release (i.e., January 2014), launched a CubeSat. However, few feedbacks were received. Despite this setback, valuable inputs have gathered from the received answers from which correlation between life-cycle activities and failures have been evaluated and are in the base of the stated recommendations. The received information is detailed in the next sub-sections:

6.2.1 General information

The information gathered in the first section of the questionnaire shows that most of the CubeSats have been developed with a main educational objective and few of them for technology demonstration, validating the obtained data from public sources. As far as the budget is concerned, only half of CubeSats followed the original principle of developing 1U CubeSat with around 100k$. the others have been developed with a higher budget (e.g., one 1U and one 3U have been developed with a budget of 300k€ and 2M€ respectively). Regarding the type of CubeSats, the most developed are 1U, followed by 3U and then 2U. Taking into account the failures, half of feedback answered that they CubeSats are still active,

one quarter are non-active and one quarter have already deorbited. It is worth to remark that half of the deorbited satellites were never been active.

These data confirms the previous statistical analysis from public data and gives, even the low sample numbers of feedbacks, quite confidence of the results.

6.2.2 Design information

The first information regarding the design is to stabilise the model philosophy followed by the developers. Half of them decided to follow an hybrid approach, while the rest are divided in the same way between protoflight and prototype approaches. The application of a precise standard is not yet done by most of the CubeSat teams. Indeed, only one (partially) applied a standard, while the others only followed the CubeSat Design Specification. Following similar trend, only 2 of them conducted reliability analysis to reduce the probability to suffer a failure.

In general, at subsystem level, few simulations are conducted. Usually they are limited at EPS, ADCS and thermal subsystems simulations. On the other hand, CAD model at subsystem and system level is always conducted.

It is also important to analyse what type of components are used. The provided answers by the developers show that all of them followed the CubeSat standard spirit and few to non Hi-Rel components are used in their satellites.

During the manufacturing of the satellite it is important to assess the characteristics of the subsystems (e.g. correct functionality, mechanical characteristics, etc.). Most developers conducted functional tests at subsystem level which lead to the verification of correct functionality of these parts. On the other hand, no many teams performed environmental tests on the subsystems. Concretely, few of them conducted thermal, mechanical and/or radiations tests on some subsystems or components.

Finally, most of them foresaw some kind of redundancy. Some applied redundancy on processors while some of them applied redundancies to critical subsystems as well as to avoid single point failures.

6.2.3 Handling information

The required information in this section was aimed at assessing the foreseen protections against hazards which can damage the satellite while it is being transported among different facilities. All the developers protected their respective CubeSat against shocks. On the contrary, only few of them protected the satellite against other hazards like humidity, contamination and electrostatic discharges.

6.2.4 Verification

Most of the key actions to be conducted to assure (or at least increase the probability of) a mission success are conducted during phase D of a project life cycle. The verifications are one of the main activities which help to demonstrate that the spacecraft will be able to survive the different environments that it founds during its life cycle and it will conduct the designed mission.

6.2.4.1 Verification preparation

The first step to follow in the verification process is to plan the campaign. All teams established a step-by-step procedure for all tests, while only part of them planned the whole verification campaign in an AIV plan. There are also few of them that didn't established the expected results before the tests.

Regarding the sensors position, for mechanical tests they are placed along the three axes. In case of thermal tests, the sensors are usually placed on the internal critical points of the satellite. Their positions are established in different ways: 1) some teams determined them by means of thermal analysis, 2) few from experts advises and 3) in a sensitive way.

6.2.4.2 Verification execution

The verification execution includes the assessment of what verifications have been conducted at system level, the values of the applied loads and temperatures, the number of cycles in the TV/TC tests and the criteria adopted to establish these values.

Unfortunately very few teams detailed the load levels and temperature limits of the tests. On the other hand, most of them answered the way in which they established them. All of the teams used the information provided by the launch authority regarding the vibration loads. As

far as the temperatures and number of cycles for the TV/TC tests are concerned, half of the teams gathered the information from a thermal analysis. The others established the temperatures from previous experience (sometimes with the support of experts) and from the datasheet of the components. Usually the number of cycles is limited by time and costs constrains. The radiation levels have been established, by the team which conducted the verification by means of test, using a commercial software which determined them.

6.2.4.3 Verification results

The results of the verifications pointed out that in most of the cases failures are observed and identified. This allows the teams to fix them before satellite launch and avoid that the failure takes place on-orbit. Indeed, only one of the CubeSat teams answered they didn't observe any failure during the tests. On the other hand, the rest of the developers individuated at least one failure during the tests. Concretely, most of them were noticed during thermal-vacuum/thermal-cycling tests. Also some failures took place during the functional tests and few of them due to vibration tests. This information leads to take a clear conclusion that, among thermal, vibration and functional tests, the more stressing and harmful for the satellite are thermal tests.

Once the failures are observed and identified, the teams proceeded to fix them and, in most of the cases, re-test the satellite. In principal, the tests conducted again were those devoted to demonstrate some functionalities which could be affected by the failures fixing actions even if some of them didn't conduct the test during which the satellite failed.

6.2.5 Integration into the deployer and operations

One of the advantages of the CubeSat standard is, as explained before, that there is no necessity to design the adaptor to install the satellite into the launcher. Then, the satellite design shall take into account to conduct health-checks and batteries recharge activities while it is inserted into the deployer. As far as this topic is concerned, most of the times the CubeSat shall remain installed without the possibility to access them for a relevant number of days. Indeed, the received answers show that an average of 100 days passes between the CubeSat integration into the deployer and the launch date.

The correctly insertion of the CubeSat on-orbit is always confirmed by the launch and/or deployer provides while few times is only assessed by the reception of the first radio signal. On the other hand, most of the times there is not any confirmation of the correct deployment of the antenna.

Regarding the reception of the satellite signal in the first hours after the on-orbit insertion is usually conducted except from some teams. The main problems are the failure of the satellite after the deployment (i.e. never heard) or the low formation of the team to manage the ground control station. On the contrary, most of the CubeSats which were heard in the first hours after the deployment has established a strong communication link to decode the signal. Only few of them were unable to decode the signal due to different causes like interferences with other CubeSats and/or subsystem failures. Taking into account the CubeSat signals which have been decoded during early operation phase, the most of them showed a nominal telemetry values. Some off-nominal values have been observed, mainly for temperature out-of-range (lower temperature than expected) and high number of reboots.

As far as nominal mission operations are concerned, only two CubeSats had observed no failures. Most of the CubeSats have suffered at least a failure. The failures go from failures which were solved and the satellites were restored into its nominal configuration (mainly due to radiations) to failure lead to mission loss (from design errors to corrupted software on the on-board data handling).

6.3 Correlation between mission success and computed actions

The correlation between the inputs given in the survey answers are conducted in this paragraph. The first general correlation is mandatory to state, even if it is intuitive to say: the more analysis and tests are conducted, the most possibility to have a mission success there are. Concretely, a relation between the number of simulations, mainly at subsystem level, and mission success is observed. Another important state concerns the redundancies: the satellites where some kind of redundancy is present, especially redundancies to avoid single point failures, show a high mission success rate.

As far as assumed protection during CubeSat transport regards, in general it could be said that, intuitively, the more protections are applied, the high rate of mission success could be observed. Anyhow, the analysed data does not show a strong correlation in this case. Indeed, some CubeSats which have only been protected against shocks during their transport succeed at conducting the mission.

Concerning the verification planning and execution, the more detailed they are, the more failures are observed during the verification phase and not after on-orbit insertion. The verification execution conducted to failures identification. These observations lead to the necessity to apply recovery actions on the satellite to restore its nominal condition after the failure. The received feedback show a relation between re-tests the CubeSat after restoring it from a failure and its mission success. Indeed, generally the satellite which has been re-tested has not been affected by a failure (at least the same failure identified during the verification campaign) while on-orbit. On the other hand, the fact that failure(s) has(ve) been observed lead to a cost increase and time delay.

6.4 Recommendations and good practices

The aim of the present section is to provide a list of recommendations and good practices to be conducted during the entire life-cycle of a CubeSat. As introduced at the beginning of the chapter, these advices are devoted to increase the probability of CubeSat mission success.

The statements have been divided in different groups following the classical space program development phases. In particular, general considerations applying to all phases are stated. Then, the advises are stated in the phase(s) where they should be applied: design phase (where phase B and C have been gathered in one single phase), manufacturing (or procurement) and operation. The disposal phase has not been taken into account because, due to the nature of this phase, it is not possible to undertake actions to improve the possibility of mission success.

6 LIFE-CYCLE GOOD PRACTICES

General considerations

1. Correct practices: in general way, it is very important to think about all the actions and activities to be conducted during the entire life-cycle of the CubeSat as well as the needs and the schedule specifying when they are going to be conducted. This will help to have a clear view of the whole project. It is also recommended to conduct periodically peer-reviews which can be very useful to check the correctness of the performed activities.
2. Good coordination: the presence of a system engineer role is highly advised to coordinate the team. Usually a precise set of activities is assigned to each team member. Anyhow the coordination among all members shall be conducted and a periodically meeting is advised to allow all team to know the present status of the project, the work conducted and the future planned activities.

Design

1. Think to the future: it is important, since the very early design phase, to think about future activities to be carried out which may require to take some considerations during the design phases. Concretely, it is important to take into account the requirements for verification phase (and the needs) from the beginning of the project:
2. Recharge batteries during mission test: a mission test is necessary to assess the capability of the satellite to conduct the mission. This test last more than the mean time that CubeSat batteries last without recharging. Hence, it is necessary to envisage (i.e. state the requirement) the possibility to recharge the batteries through umbilical connector (when solar simulator is not available) while the satellite is switched-on.
    a. Recharge batteries during TVC test: during thermal-vacuum cycling test it is mandatory, following the ECSS standard, to conduct functional tests during maximum and minimum temperatures. This requirement implies that it is necessary to be able to switch-on the satellite while it is inside the

thermal-vacuum chamber. Moreover, it will be necessary to recharge the batteries during the TVC test.

b. Communications during TVC tests: as specified in the previous point, during the TVC test it is required to conduct a functional tests. Sometimes, depending on the facilities, it is not possible to establish a RF communication link. Hence, it is highly recommended to design a communication link through physical umbilical connector in order to test the complete functionalities of the CubeSat without the necessity to communicate in radio-frequency.

c. Introduce thermistors in the project: during the TVC it is necessary to monitor temperature inside the CubeSat. Hence, the installation of thermistors shall be foreseen. Usually these the equipment used to monitor the internal temperatures during the test are not the same as those installed to measure temperatures while in orbit. It is necessary to envisage the location and type of the thermistors, as well as to install them during the final assembly and integration activities.

d. Restore ready-to-launch configuration: after the tests the satellite shall be restored in the launch configuration. Main activities could consist on delete storage memory where all the mission data is stored, fold the antenna, etc. All this operations shall be designed in a way that they could be conducted with the satellite completely assembled.

3. Electrical connector for sensors: internal thermocouples and accelerometers, are required inside the satellite to monitor the temperatures (and the accelerations) during the TVC test (and vibration tests). It is encourage to foresee a connector where all these sensors are connected. In that case it will not be necessary to cut and isolate the wires (reducing the risk of power arcing and/or electrical discharges). Moreover it will provide a plug-and-play interface to retrieve the data from that sensor.
4. Avoid single point failures: reduce single point failures via software redundancies if possible and/or hardware redundancies.

6 LIFE-CYCLE GOOD PRACTICES

Methodology

1. Classical Vee approach: CubeSats are low-cost, fast-development satellites. Anyhow the design, manufacturing, verification and operations shall be conducted as much similar to traditional projects as possible. In this context, the classical Vee approach is highly recommended for CubeSats projects. Starting from the mission statement definition (i.e. stating the purpose of the project), the mission objectives, requirements and constraints, as well as the system requirements shall be then derived. These steps are crucial to achieve a good project. Moreover, during the requirements definition, it is also necessary to establish at what level, stage and what methodology(ies) will be used to verify them.
2. Documentation: the documentation of all activities of the project is crucial for different reasons. First of all, the documentation will help to have a smooth continuity on the project, avoiding information gaps if some members leave the team. Second, the documents are very useful to conduct peer-reviews which will help to assess that the team is achieving the established objectives. Finally, it will also be possible that some of the documents could be required by launch authority to accept the CubeSat to be launch. In this last case, the documentation of the project during the all phases will be also useful to avoid the necessity to produce it quickly if required by third parties, which can lead to specify errors and uncertainties due to the short available time.
3. Consider all ICDs: one of the intrinsically a characteristic of a CubeSat project is that usually the launcher is unknown during the development of the satellite. Indeed, most of the times the launch is bought when the project is already in an advance stage. To avoid the possible limitations on wide available deployers available on the market, it is highly recommend to take into account ICDs of all deployers. These will give a set of requirements that, if followed, will allow to be accepted for any deployer to launch the CubeSat.

6.4 Recommendations and good practices

Analysis

1. Thermal analysis: thermal aspects shall be taken into account from the beginning of the project. Most of the components on a CubeSat are COTS and they are usually very sensitive to temperature. In that case, a thermal analysis is needed to assess the maximum and minimum envisaged temperatures. Iterative analysis shall be conducted to refine the results when data from the subsystems is available. This analysis will give, from the obtained temperature ranges, the information to assess if some kind of thermal protection is necessary. Regarding these points, it could also be interesting to obtain, from the providers, any information about thermal behaviour of the components. Form the results of the questionnaire as well as from inputs from experts a good range of temperatures to design (and test) a CubeSat could be between -20ºC and +80ºC. Nevertheless, this limit shall not be taken as a mandatory input. Indeed, the very important consideration to be always taken into account is not to damage the satellite.
2. Radiations analysis: as stated before, the COTS components usually used in CubeSats are not HiRel and hence are very sensitive to radiations. It is highly recommended to conduct radiation analysis taking into account different orbits to evaluate if protection against radiations is required. Regarding this topic, the active components and circuits are usually the most affected parts by radiations. Different software tools are available on the market to conduct this study.
3. Mechanical analysis: it is important to conduct the mechanical analysis as much precise as possible to assure that the structure and all subsystems withstand the designed loads. When these are not available, different solutions could be applied (e.g. make a general envelope which covers the maximum loads of all possible launchers, use NASA-GEVS, etc.). It is necessary to remark that the quasi-static loads analysis shall be conducted applying different combinations of the longitudinal and lateral loads.

6 LIFE-CYCLE GOOD PRACTICES

EPS design

1. Subsystems powering: it is important to allow the system to isolate possible failures. One way to conduct this protection is design the power lines in series, which each one feeds one subsystem. Controlling each line separately from the others will allow to isolate a possible failure.
2. Design a detailed power budget: to assess that enough power is available on-board is crucial for the mission. The power budget shall be updated while the design is on-going. When new data is available (e.g. precise consumption of a component, better if tested) the power budget shall be updated.
3. Design a detailed energy budget: the energy budget will be used to assess the instant required energy. A decreasing trend of energy budget (even when the power budget is positive) could cause a degradation of the mission results

AOCS design

1. Redundancy: high numbers of failures in AOCSs of satellites are due to failures on the gyros. A redundancy of gyros (if present) is recommended.
2. Back-up mode: a back-up mode is always advised if possible. In the case of the AOCS it could be foresee attitude determination using only part of the available sensors (e.g. using accelerometers and determine angular velocity by computing the derivative).

COMSYS design

1. Increase the link margin: usually it is advised to have a minimum link margin of 6dB. Usually, during the design phases, the final orbit is not known. Due to this fact, it is necessary to assume the worst case to compute the link margin. Moreover, it is advised to try to increment the margin to assure a strong link even if possible failures and/or anomalies took place (e.g. high tumbling rate, antenna remains folded).
2. Back-up line: the ability to communicate with the satellite is crucial to control the mission and to obtain data from the bus and payload. The communication

subsystem could be redundant and a back-up link could help to increase the possibility to communicate with the satellite if the primary communication line fails.

3. Independent processor: it is possible that the communication between the communication subsystem and the others subsystems fails. In that case, the COMSYS processor should be able to send basic telemetry/signal (if possible with basic telemetry which shows the possible failure). This will maintain a communication link between space and ground segments and will allow operators to evaluate the problem and decide a possible action to recover the satellite.
4. Emergency batteries: the EPS is a crucial subsystem and, unfortunately, could fail and/or have an anomaly. Non-rechargeable battery(ies) could be installed and used in case the EPS fails or an anomaly is observed. With this improvement the communications between both segments can be guaranteed and it gives time to operators to assess and take corrective/restoring actions (or at least obtain enough data which could help the assessment of the failure).
5. Frequency drift avoidance: the frequency stored in the COMSYS could suffer a drift for various reasons (e.g. temperature, radiations, etc.). One of the possibilities is, if applicable (e.g. if the frequency is programmed in a memory), to implement an external reset that could restore the original designed frequency.

OBDH design

1. Different communication lines: to have different communication lines between the OBDH and the rest of the subsystems. This redundancy on the communication could help to reduce the risk of losing one subsystem due to a communication protocol failure. Each communication subsystem should have nominal link and redundant link.

Mechanisms design

1. Possibility to dismount: it is very important to allow the possibility to disassemble the satellite. During the verification campaign failures can take place. If this happens, it is probably required to have access to the internal part of the satellite or

even disassemble part of them.. E.g. screw the solar panels: it is highly recommended instead of glue them. In that case, they can be disassembled without the risk of breaking them.

Design for radiations protection

1. Boards' configuration: the internal boards' layout configuration could help to protect the most sensible components with respect to radiations. Different physical configurations shall be evaluated to assess the most convenient one which protects these most sensible components. In particular, in the most internal parts of the CubeSat the most sensible components shall be placed. In that case, they can be partially protected by the rest of boards.
2. Protection: the abovementioned radiation analysis will provide information about the risk to be affected by radiations. If this risk is considered too high, the necessity of implement a protection arise and the components shall be protected by means of radiation shielding.
3. Restart the system: a watchdog should be implemented to guarantee a reboot of the system if it remains stuck. It could be also useful to implement a command, sent from ground, to restart the system. The possibility to restart/reboot the system (cut off the power and restore it) could be useful to restore the configuration after radiation effects (e.g. SEU).
4. Failures due to radiations isolation: SEL could take place. In that case it is important to isolate the failure in order to avoid failure propagation. In particular the isolation could be conducted applying resistors on the electric path.
    a. Latch-up Protection Technology circuit: introduce the LPT circuit. When SEL is detected, the LPT circuit shuts down the chip and holds it powered-down for a present time.
    b. Silicon-On-Insulator devices could be used to reduce the probability to have a SEL.

6.4 Recommendations and good practices

Maintainability

1. Order and simplicity: sometimes the failures could occur due to a "chaotic" internal configuration. Indeed, the high amount of wires could increase the risk of damaging them during the assembly and integration process. To avoid this problem (or reduce it), it is recommended to substitute the wires, whenever was possible, with printed circuit boards. For the connections that should be conducted by wires, it is advised to gather them as much as possible and to assess, during the design, where they will pass to assure an easy assembly process.
2. Accessibility: during on-ground operations or recovery actions (if necessary after possible failures during tests) it could be necessary to access inside the CubeSat. The high accessibility will help during these tasks.
3. Spares: during the development of the project the components are tested. It is possible that some of them were damaged during these tests. In other cases it is possible that the provider stops the production of some component while the project development is on-going. To avoid schedule delays in the first case and the necessity of changing some component which could imply a cost increase (and probably a schedule delay) it is important to have spare parts available.

Design for ESD protection

1. Avoid floating conductors: floating items like wires may cause an electrostatic discharge. In that case it is worth recommended to avoid and substitute them by printed circuits.
2. Isolation: if the previous point could not be applied in all cases and floating conductors are present, it is necessary to isolated them with space certified silicon adhesive. If not, a power arcing (i.e. corona effect) could take place.
3. Shielding: an electrostatic discharge could also take place between two electronic contacts. To avoid them it is advised to isolate them, for example varnishing all electrical contacts.

4. Ground: all circuitry should have a chassis ground reference. Keep everything inside a grounded Faraday Cage. Also all conductive layers of thermal blankets (if any) should be grounded (as already specified in the CDS).

Dependability

1. FMECA: to conduct this type of study is highly encourage to find critical points which can lead to failure. It could be started from the beginning of the project, and concretely it shall be started at least when subsystems definition is available.
2. Risk analysis: to conduct a risk analysis by subsystems to individuate the most critical. Then the proper actions shall be conducted to reduce the criticity and the likelihood. It is also important to assess the availability risk in terms of facilities, time, people and money. Finally, it is also necessary to assess the components manipulation risk/hazard (also to the people, e.g. beryllium).

Avoidance of certain materials

1. Kapton: this material is produced for space applications with a low out-gassing rate. Anyhow, it is affected by atomic oxygen. Hence, it is necessary to reduce the use of this material in critical parts in the exterior of the CubeSat.
2. Aluminium alloy: ESA has an alert on aluminium alloys 7000 series due to degradation observed in several cases. Hence, it is recommended to use aluminium alloys 6000 series.
3. Cadmium and Zinc: these two materials are highly volatile metals and hence their use in space is forbidden.
4. RoHS: in EU this directive has been stated and limits the use six hazardous materials (lead, mercury, cadmium, hexavalent chromium, polybrominated biphenyls and polybrominated diphenyl ether). To follow this directive will be mandatory in the near future.

6.4 Recommendations and good practices

Manufacturing (and/or procurement)

1. Incoming inspection (correct state): it is important, when parts/components are acquired, to establish an "incoming procedure" which establishes the steps to follow to assure that the received product meets the desired requirements. In particular, it is necessary to conduct at least a functional test to assure that the component follows the expected behaviour as specified in the datasheet.
2. User Manual: it is very important to follow the actions specified in the user manual. To not follow these rules could lead to damage the satellite or the subsystem/component. It is necessary to be aware what it can be done and what has to be avoided.

Assembly, Integration and Verification

Plan

1. Test planning: the plan of the test campaign shall be conducted before starting it. As a minimum, the requirements to be verified, the tests to be conducted with the step-by-step procedure as well as the expected results and pass/fail criteria shall be specified. This planning will help to conduct the tests in a systematic way and to have the specifications to be able to conduct the tests more than one time in the same configuration.
2. Personnel management: it is necessary to define a priori the exact role of each team member involved in the verification campaign. To not have a defined role for each one could lead to misunderstanding and human errors.
3. GSE testing: it is important to have high confidence on the values measured during the tests. In that case it is important to test the GSE before starting the test on the system/subsystem. In that case it will be possible to assess that the output given by the GSE are correct:
4. The electrical connection of the EGSE shall be controlled (correct welding, check wires continuity, etc.).

5. Satellite installation: the test set-up shall be correctly planned and conducted with sufficient margin of time before the test starts. The test duration shall be envisaged as well as safety measurements and regulations to protect operators.
6. Verification results reports: it is very important to fill as-run procedure during the tests to be also sure that all steps have been followed. After them test reports shall be produced.
7. Evaluate failures: during verifications failures/anomalies could be observed. Should it happen, NCRs shall be produced. In this case the root cause of the problem shall be founded and the possible solutions assessed before acting on the spacecraft. The intervention on the spacecraft is the last action after a failure is observed. If corrective actions are conducted to restore the satellite into its nominal condition after a failures has been observed, certain tests shall be conducted to verify the spacecraft meets the requirements after the intervention.
8. Programmatic: during the planning it is important to create a list of possible problems which can be encountered during the test and how to solve them. This will allow a rapid response if their take place. It is also recommended to take into account certain margin of time and budget. Some tests could not be run nominally and failures could take place. In that case it is advised, after fixing the possible failures, to repeat the test in which failures have been observed.

Subsystem level verifications

General

1. Real consumption: the real consumption of each subsystem specified in the datasheet (or after the subsystem manufacture) shall be verified by test. These values will then be used to define a more precise power budget.
2. Test against launch requirements: it is important to test all subsystems/components not only against the functional requirements, but also against the possible requirements required to be accepted for the launch. E.g. tests to verify outgassing and hazard materials requirements.

6.4 Recommendations and good practices

Electrical Power System

1. Test auto-discharge: storage and launch delay shall be considered. Hence, the verification of the batteries auto-discharge when connected to all loads (with DS pressed) should be assessed. This could be verified at subsystem level (connecting equivalent loads to the EPS) or at system level (if time is available).
2. Good knowledge of the batteries: the batteries are critical components. They shall be properly and detailed characterised. At least a test at component level is necessary to assess their functional behaviour. To test them in thermal chamber is highly envisage (and TV if never used in space environment).
3. Test power budget: the power budget shall be tested to verify and confirm the analysis conducted during the design phase.

Communications System

1. Low/no frequency drift: it is very important to assess that the radio of the communication system will not suffer frequency drift due to extreme temperatures, mainly if some CubeSats have similar frequencies in the same launch. A detailed FMECA on this point should be conducted
    a. Test: if it is possible and affordable, a thermal test it is recommended on the COMSYS. With the time the electrical characteristics can be changed. Worst case analysis should be done.

System level verifications

General

1. Test comparison: functional tests shall be conducted before and after environmental tests campaign. These tests shall demonstrate the correct functionality of the satellite and that it has not been affected by the exposure of the spacecraft to space environment during tests. The same test should be conducted before the shipment to test facilities to have a reference case to compare the future results.

6 LIFE-CYCLE GOOD PRACTICES

TV/TC tests

1. Mechanisms test: to conduct the test of the mechanisms during the TV/TC test is encourage to assess the correct capability of the mechanism to conduct its functionality in space environment. The test shall be planned before the starting of the TV/TC test and it is necessary to foresee if any limitation applies. In particular, limitations due to the dimensions of the facility and GSE.
2. Functional test: it is highly recommended to conduct functional testing during the thermal tests to verify the correct functionality the satellite at hot and low temperatures.

Functionality

1. Operative modes and transitions: it is important to test at ambient condition all the operative modes as well as transitions between them. It is worth to remark that the functionality test shall demonstrate the good functionality of the system (and each subsystem), not only check if switches-on. The correct functionality shall take into account that the correct outputs are achieved (e.g. correct values measured by sensors, etc.)
2. Polarity: once the satellite is completely assembled, the polarity of actuators (e.g. magnetorquers) and sensors (e.g. gyros) should be tested.

Tests optimisation

1. Classify requirements in groups according to the fact that all of them could be verified in the same test (or in a step of a test). This will reduce the duration of the tests.
2. Reduce the duration with a proper planning. A good combination will allow to eliminate some test preparation because the set-up is already conducted for a previous test, or the satellite status at the end of one test is the required status to begin the next one.
3. Combine thermal bake-out and thermal-vacuum tests in one test in order to reduce the time and cost. This recommendation applies when bake-out test is required. Usually this is the case when the properties in terms of possible contamination (i.e.

values of RML, CVCM and TML) are known for all parts. If it is not possible to know these values (mainly TML and CVCM), the necessity to conduct a bake-out test could arise.

4. Hybrid philosophy could help to reduce time and cost of test phase while keeping acceptable risk. Develop and test qualification and flight models for new/critical components/subsystems. Manufacture and test only flight models of components/subsystems which, from previous experience and/or analysis, the confidence level on the correct behaviour is guaranteed (e.g. structure, OBC used in previous missions and it had no failures, etc.)
5. Coordination: most of the times the verifications (mainly environmental tests) are conducted in different facilities of the developer, with personnel external of the team. It is important to have a very good coordination to exchange information about the facilities, required interfaces, etc. quite in advance to correctly plan the tests.
6. Foresee failures: during the verification preparation it is important to assess the possible failures which can occur during the tests and establish a recovery action. This could help to reduce the verification execution time.
7. Order of the tests: TVC test have a higher cost with respect to mechanical tests. Hence, it is recommended to conduct the mechanical tests before the TVC test. In the contrary, if a failure is identified during mechanical tests, thermal tests should be repeated with a cost and time increase. On the contrary, if the satellite fails during thermal tests it could be recovered and the possibility to not re-conduct the mechanical tests is envisaged.
8. Combine EM-autoCompatibility test during functional tests. The successful functional test leads also to a successful EM-autoCompatibility test.

Transport, storage and maintenance

1. Plan: establish a concrete plan to transport the CubeSat among the facilities (e.g. to test, integrate into the deployer, etc.). The test should include the procedures to

protect the satellite against shocks, contamination, humidity, ESD and other possible hazards.

2. A reduced functional test to be conducted before and after each transportation will allow to assess that the transport doesn't affect the correct functionality of the CubeSat.
3. Establish precise storage conditions: during the storage of the satellite before integration into the deployer shall be conducted taking into account precise storage conditions regarding temperature, humidity, protection against contamination and other agents that could damage the satellite.
4. Health check: a periodically health check should be conducted to verify the functionality of all subsystems.

Pre-launch activities

1. GCS test: it is important to check the correct functionality of the ground segment few days before the launch.

On-orbit operations

1. Failures envisage: to foresee possible failures which could take place in orbit is important. A recovery action/plan should be established before launch
2. Stabilise the satellite: satellite stabilisation is encourage before to start the nominal operations to assure a strong communication link with the satellite.

Other considerations

1. PA role: it is an important role in all space projects and it is highly advised to have this in CubeSat projects. Nevertheless, sometimes the reduced participants in the CubeSat tem leads to the fact that PA rose is not covered. To cope with this gape the PA role could be conducted among the different participants of the group (cross-check of documentation/design of the project).
2. Reduce of contamination and non-authorised personnel: the CubeSat project shall comply with clean room class 100000 as per CDS. Nevertheless, this type of facility is

not always available. It is recommended to conduct the development, A&I and test in a dedicated room with a minimum clean level is guaranteed. Moreover, the access to this room should be limited to the team members. This will reduce the risk to damage the satellite or its subsystems by non-authorised personnel.

3. Protection in the development room: a minimum protection shall be taken during the satellite (and/or its subsystems/components). Concretely protection against anti-static discharges and contamination (at least gloves) should be used. Avoid charge build-up.
4. Protection against other hazards: other hazards, apart from the space environment hazards, could be present after a CubeSat is deployed (e.g. the CubeSat could be affected by hydrazine from the last stage of the launcher or from the primary satellite, electrostatic discharge, etc.). One possibility could be to activate an active AOCS (if available) to move the CubeSat and point the most robust face to the hydrazine cloud.

6.5 Case study: e-st@r-I CubeSat FMECA

The first action conducted within the research was started from the need to evaluate the causes that conducted to the loss of e-st@r-I (Educational SatelliTe at politecnico di toRino) CubeSat. This CubeSat has been developed by the CubeSat Team at Politecnico di Torino within e-st@r program. The CubeSat Team is a student team born in 2009 for the development of the e-st@r program in the framework of the initiative “Educational Payload on the VEGA Maiden Flight” proposed by ESA Education Office in 2008. The Team is formed by students under coordination of the Team Leader, who is responsible for the whole program. The Team is organised according to a defined work breakdown structure, which takes into account both technical and non-technical aspects. The FMECA technique was preliminary conducted during satellite developing. However, an in-deep analysis is required to evaluate the possible causes of failure during in-orbit operations in order to improve the design for future follow-on projects (see section 7.3).

6.5.1 E-st@r program

E-st@r program is an educational program carried out at Politecnico di Torino within the CubeSat Team. It encompasses the design, development, manufacture, verification and operation of CubeSats conducted by students under the supervision of researchers and professors. This program, which is driven by educational and scientific purposes, is based on a hands-on-practice approach as a perfect means to achieve the University educational and technological objectives. I.e., to educate engineering students on systems development, management, and team work; and to achieve insight in the development of scenarios and enabling technologies for future space missions within a low-cost program. These program guidelines are summarised in Figure 32.

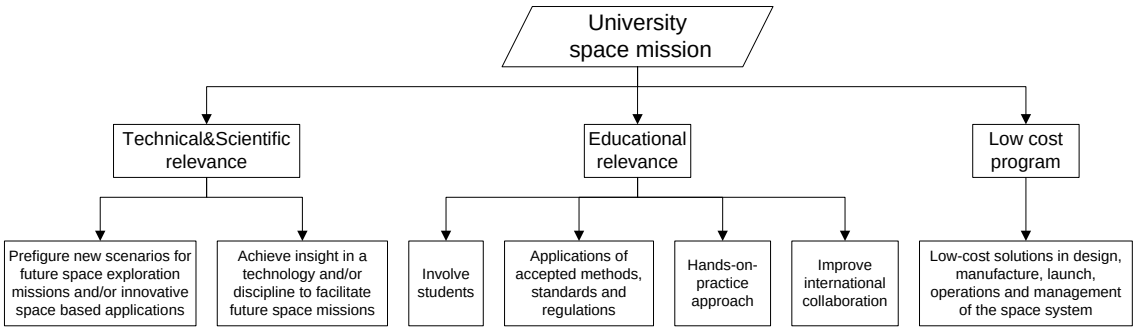


Figure 32: E-st@r program guidelines

The main program guidelines have been assumed as high-level objectives and constraints for the e-st@r program. They can be listed as follows:

- WHAT/1: To inspire and prepare future space-professionals: students are the end users of the mission
- WHAT/2: To improve knowledge in space science and engineering: real world shall take advantages of our missions
- WHY: To meet stakeholders' needs. Stakeholders are: students & civil society, scientific community and industry
- HOW: To carry out a space program from the design to in-orbit operations, completely managed by students

The educational purpose of the program is pursued at several levels: undergraduate, graduate and postgraduate. Students come mainly from the Aerospace Engineering area, but also from Mechanical, Electronics and Communication, and Energy Engineering.

6.5.1.1 Mission objectives

The mission objectives represent the broad goals that the system must achieve to be effective, productive, efficient and useful. The motivations that led us to define the mission objectives include “needs” of both scientific-technological importance as well as educational significance.

The relatively low cost from standardised components and piggy-back launch opportunities make CubeSats the perfect systems to achieve actual most significant challenges, i.e. to accomplish science goals while facing severe limitations on mass, volume and power. However, the CubeSats’ contribution to broad science goals shall be supported by the appropriate set of technologies.

One of the most enabling technologies for future CubeSat missions is the capability of autonomous attitude determination and control, specifically where requirements in terms of stabilisation and pointing accuracy are critical to the effectiveness of experiments, payload operations, communications, and in turn to the mission success. To address this need, the primary technology objective of e-st@r program is to demonstrate the capability of autonomous determination and control, through the development and test in-orbit an active attitude determination and control system entirely designed and manufactured by students. Moreover, a second objective has been defined: testing in orbit COTS technology and self-made hardware.

The motivations, needs and constraints that led to the definition of the mission objectives are shown schematically in Figure 33.

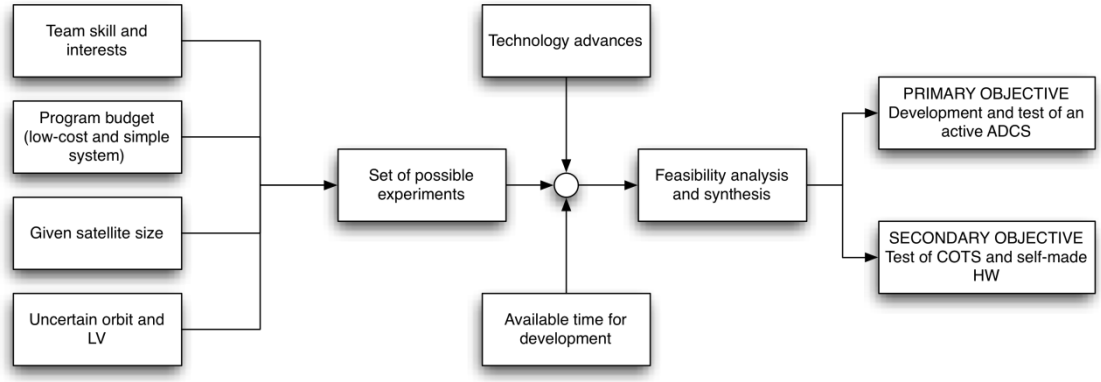


Figure 33: e-st@r mission objectives

6.5.2 E-st@r-I CubeSat description

In 2008 ESA Education Office released a call for proposals named "Educational Payload on the VEGA Maiden Flight". E-st@r-I project was presented and accepted as one of the 9 CubeSats to be launched on the VEGA Maiden Flight.

E-st@r-I is a 1U CubeSat developed for demonstrating autonomous attitude control capabilities based on magnetic actuation. A picture of e-st@r-I CubeSat is shown in Figure 34.

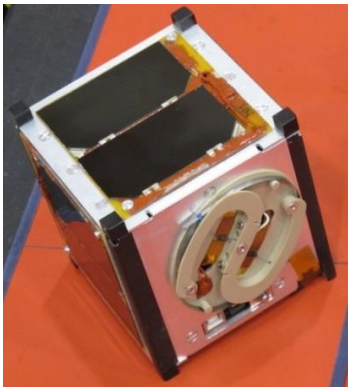


Figure 34: e-st@r-I flight unit

The nominal configuration in orbit provides for a free tumbling, without attitude stabilization. This task shall be accomplished upon the activation of the active attitude determination and control subsystem (A-ADCS), which actually represents the e-st@r-I payload. The stowed configuration of e-st@r-I is an aluminium-alloy cube-shaped box of 100mm per side, with 5 out of the 6 faces occupied by solar panels.

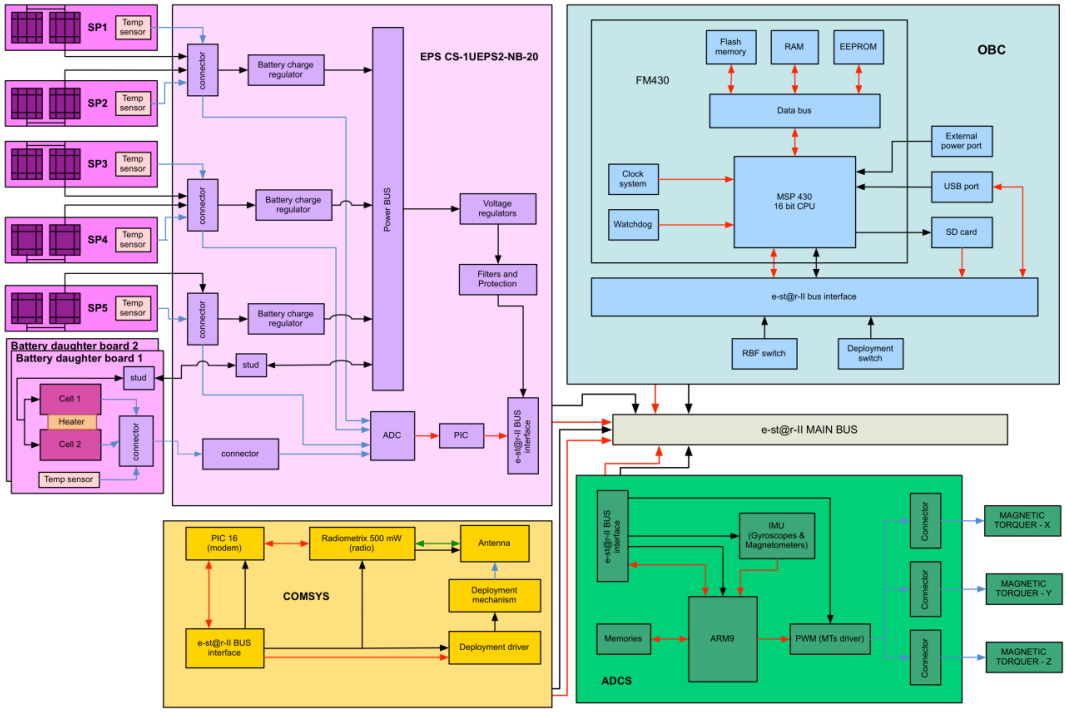


Figure 35: e-st@r-II system architecture blocks scheme

The sixth external surface hosts the antenna system and the access ports for ground operations. After the satellite activation, the antenna system deploys two arms of the dipole which remain attached to the CubeSat structure. The CubeSat has been designed, developed and assembled taking into account all the applicable requirements and constraints given in the CDS.

E-st@r-I system architecture blocks scheme is reported in Figure 35. The platform in support of the payload includes the Electrical Power Subsystem (EPS) devoted to provide, store, control and distribute the electrical power on-board, the Communication Subsystem (COMSYS) that provides the interface between the space and ground segments, and the On-Board Computer (OBC) which handles and executes commands, manages and stores data and performs autonomous on-board operations. The structure/mechanical system is devoted to carry the loads induced by the launch vehicle, to support and protect all other spacecraft subsystems, and to provide for spring plunger device. Passive thermal control has been designed for e-st@r-I.

6.5.3 E-st@r-I in-orbit experience

e-st@r-I was launched, after some delays on the scheduled date for the inaugural flight, on the VEGA Maiden Flight on February 13th 2012. Just after the release from the deployer the satellite was activated. However, first telemetry data were received only few days later. Moreover, the low quality of the signal with a low signal-to-noise (S/N) ratio made almost impossible to completely decode the signal and retrieve data.

A preliminary assessment of possible causes for the low S/N ratio was conducted by the Team. The most realistic rationale that justified the problem was a possible low batteries state-of-charge. Hence, the Team commanded the satellite to switch its operative mode to another one (called *safe energy*) at which the consumption is reduced at the minimum (i.e. communications are stopped in downlink and the payload is switched-off). Even if the cause of the low S/N ratio was individuated, a more detailed analysis was required to individuate the original cause of the failure.

6.5.4 E-st@r-I FMECA

To conduct the assessment of possible failure origin causes occurred during in-orbit operations of e-st@r-II, the FMECA technique has been applied. The outputs of the FMECA have been crucial to improve the design for the follow-on CubeSat, called e-st@r-II (see section 7.3).

An extraction of FMECA is shown in Figure 36 (complete FMECA is provided in Appendix C)

CubeSat: e-st@r-I
Date: 20.12.2013
Prepared by: Gerard Obiols Rabasa gerard.obiols@polito.it
Approved by: Fabrizio Stesina fabrizio.stesina@polito.it
Revision: 2
Issue: 0

System: e-st@r-I							Subsystem: Electrical Power Subsystem							
Ident. Number	Item/block	Function	Failure mode	Failure cause	Mission phase/ Op. Mode	Failure effects a. Local effects b. Next higher level b. End effects	Severity classification	Failure detection method/ observable symptoms	Compensating provisions	Severity Number SN	Probability and PN	Criticality Number CN	Recomendations	Remarks
19	D-PCDU	Doughter power control and distribution	Battery pack 1 does not work	Connection physically broken Physical disconnection of the connector Burnout Power requested from the ADCS too high	Basic mode Full mode Save energy Safe mission Temporary shut down	a. Less power available b. Partial EPS failure c. Not able to supply power to all subsystems	II - Critical			2			May be necessary to switch to Safe energy operational mode	
20			Battery pack 2 does not work	Connection physically broken Physical disconnection of the connector Burnout Power requested from the ADCS too high	Basic mode Full mode Save energy Safe mission Temporary shut down	a. Less power available b. Partial EPS failure c. Not able to supply power to all subsystems	II - Critical			2			May be necessary to switch to Safe energy operational mode	
21			Temperature sensor 1 does not work	Physical break Burnout	Basic mode Full mode Save energy Safe mission Temporary shut down	a. Temperature value of sensor 1 not available b. Battery pack 1 temperature not controlled c. Battery pack 1 temperature could be out of operative range,	IV - Minor			1			Check from telemetry if the battery 1 voltage is correct. If not, possible malfunction of battery 1	
22			Temperature sensor 2 does not work	Physical break Burnout	Basic mode Full mode Save energy Safe mission Temporary shut down	a. Temperature value of sensor 2 not available b. Battery pack 2 temperature not controlled c. Battery pack 2 temperature could be out of operative range,	IV - Minor			1			Check from telemetry if the battery 2 voltage is correct. If not, possible malfunction of battery 2	

Figure 36: e-st@r-II FMECA (extract)

The FMECA was conducted in a systematic approach: starting from system level, the subsystem and component decomposition have been followed to identify possible failures, causes and effects on the satellite. However, due to the fact that the satellite was entirely manufactured using COTS components, probability number and criticality number were not available. Anyhow, this drawback did not prevent to obtain high valuable outputs from which the failure causes of e-st@r-I were individuated.

High numbers of outputs have been obtained from the analysis. First, possible failures at system level refer to failures of each subsystem. Expect for the failure of the payload (which has been considered critical), all the other possible failures are considered catastrophic. This event is a direct consequence of the fact that no redundancies are present at subsystem level, and hence, any possible failure of one of the bus subsystems will lead to the loss of the mission.

Secondly, at subsystem level, most of the possible failures are classified as critical in the payload and EPS, while are catastrophic in the OBC and COMSYS. Failures that can occur in these last two subsystems lead to a complete loss of the mission, because the satellite would lose the ability to process data and/or communicated from/to ground segment.

Third, most of the possible failures of the EPS were stated as critical. One of them (i.e. the unavailability of one of the battery packs to supply power) would lead to not feed some

subsystems. Furthermore, one possible failure of the payload would be that the subsystem is not able to stabilise the CubeSat. The non-stabilisation would lead the impossibility to recharge batteries. Thus, the combination of these events would originate the failure on the reception of the signal and, at the end, the anticipation of the operations cessation with respect to schedule.

Important results have been obtained from this analysis. First of all, has been demonstrated the utility of applying this technique from the very beginning of a space project. Indeed, if a detailed analysis was conducted, the causes of the failures would be individuated during the design phase. Regarding the actions to avoid similar failures in the follow-on CubeSat, two main actions were envisaged: 1) to replace COTS battery packs by batteries from CubeSat EPS provider that already tested these components on-orbit, and 2) implement new operative modes in order to allow higher control on the payload activation and operations, giving more manual operability from ground, instead of automatic procedures. These two modifications along with others have been implemented in e-st@r-II. The e-st@r-II CubeSat has been used as test case for other part of the present research, detailed in next chapter.

7

RELIABILITY-ORIENTED VERIFICATIONS OF CUBESATS

Conventional satellites projects are, traditionally, oriented to give the same effort, in terms of cost, time and personnel, to design, development, integration and verification phases. On the contrary, CubeSats projects usually speed up design and development to conserve time, personnel, and financial resources for AIV phase.

Generally speaking, CubeSats reliability can be increased testing the system's functionality in all possible operational conditions that will face during its life-cycle. Normally, due to CubeSats components dimensions, they are not completely tested at equipment level, and are directly functionally tested at subsystem level. Environmental tests are generally conducted only at system level. Moreover, for classical projects standard procedures enforce the production of countless documents that could lead to an extremely bureaucratised project.

To conduct such verifications, CubeSat developers normally try to follow international standards (e.g., ECSS standards) that, however, have been stated for large-conventional satellites projects, with longer time schedules and higher budget. Hence, a tailoring of these standards is absolutely necessary to allow their application to CubeSat projects.

ECSS standards are studied and tailored to adapt them to CubeSat projects. A critical review of them is conducted in the present section, presenting an adaptation of the standards for AIV of CubeSats. The result is a standard methodology to conduct CubeSats verification that guarantees a sufficient confidence on satellite reliability and mission success maintaining a cost effective program.

7 RELIABILITY-ORIENTED VERIFICATIONS OF CUBESATS

7.1 European Cooperation on Space Standardization (ECSS) standards

The European Cooperation on Space Standardization (ECSS) is an organisation that works to develop a coherent, single set of user-friendly standards for use in all European space activities.

It has been developed as a cooperative effort between the European space agencies and space industries. The organisation is constantly reviewing the standards and publishing new updated versions. The ECSS standards are normative documents that encompass a comprehensive set of documents addressing all essential aspects of the three major space project branches for the successful implementation of space programmes and projects, i.e., engineering, project management and product assurance. Thus, ECSS standards are structured in three branches with the following contents:

- Management: this branch (i.e., M-branch) gives guidelines to achieve successful completion of the space project in terms of cost, schedule and technical performance. Project management is performed following a structured approach throughout all stages of its life-cycle and at all levels of the customer-supplier chain.
- Engineering: E-branch covers the engineering aspects of space systems and products, including the engineering process as applied to space systems and their elements or functions, and technical aspects of products used to accomplish, or associate with, space missions.
- Product Assurance: the Q-branch guides the engineers to assure that the space products accomplish their defined mission objectives and more specifically that they are Safe, Available and Reliable.

Verification process guidelines are reported in ECSS-E-ST-10-02C, and required tests in ECSS-E-ST-10-03C. Hence, these two documents are tailored to adapt them for a CubeSat project. In particular, their content is:

- ECSS-E-ST-10-02C: the standard established the requirements for the verification of a space system product. Fundamental concepts of the verification process and the

criteria for defining the verification strategy are defined as well as the requirements for the implementation of the verification programme are specified. Moreover, a list of expected documentation is provided.

- ECSS-E-ST-10-03C: this document addresses the requirements for performing verification by testing of space segment elements and space segment equipment on ground prior to launch.

7.2 ECSS standards tailoring for CubeSats verification

Verification main objective is to assess whether or not a system meets the requirements stated during design phase. In other words, verification activities answer the question *Does the system/subsystem/equipment meet its requirements?*. Thus, verification is a key-phase of a project life-cycle and the activities conducted are crucial to increase system's reliability and establish a good confidence of a successful mission. The verification process shall be conducted in a systematic approach at different levels (i.e., equipment, subsystem and system levels).

Generally, verifications process is made up of four main activities, i.e., planning, execution, reporting and control closeout, which are summarised, as detailed in ECSS-E-ST-10-02C, in Figure 27:

7 RELIABILITY-ORIENTED VERIFICATIONS OF CUBESATS

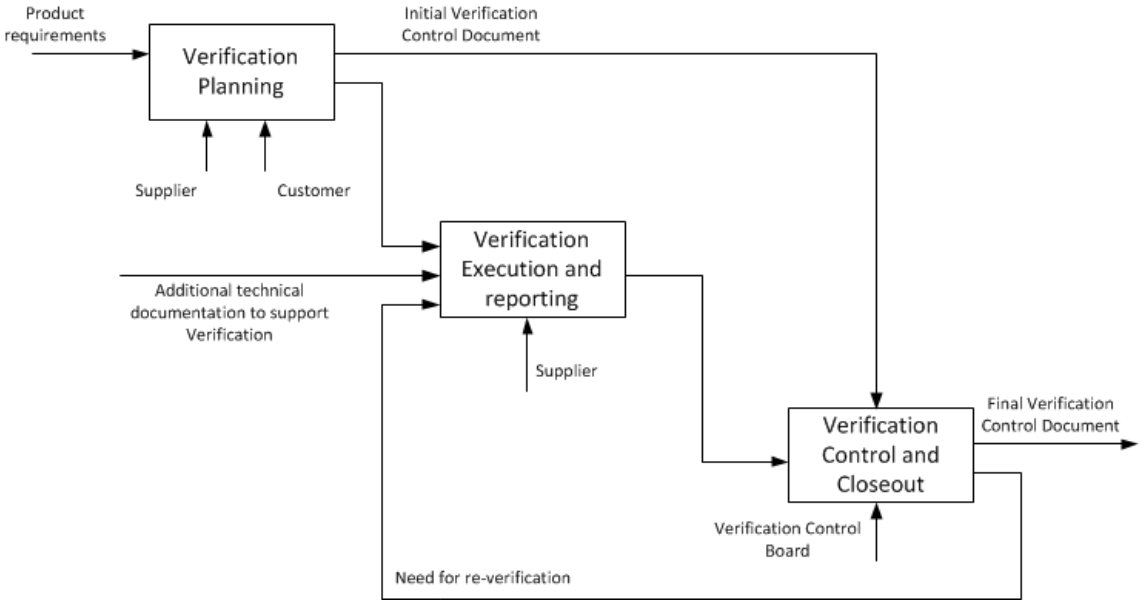


Figure 37: Verification process and activities

The first step in verification process is to conduct verification planning. Supplier and customer give their inputs that, together with product requirements defined during design phase, constitute the three inputs for the verification planning. As an output the initial verification control document is obtained. It contains the correlation between the requirements, the level and stage in which they shall be verified and the verification method to be used. Moreover, the required documents to conduct verification are written in this phase. The planning of verifications is used, together with any additional technical documentation useful for verifications, to precisely execute them and report the results. The results are cross-checked with requirements, and if the requirements are verified, they are closed-out and the final verification control document is released.

Among all verification methods, analysis and test are the most used. Conventionally, the role of tests is to verify analysis while the role of analyses is to support functionality. Classical space projects foresee to conduct high number of analyses and tests to verify the requirements. However, this approach cannot be followed in a CubeSat project because it will lead to a boost of reviews, overspecifications and paperwork production. Generally speaking, testing is the preferred verification method with the lowest risk, but, because it represents a

large expense, the tailoring of the test program, should also assure that a cost effective program is achieved.

The peculiarities of CubeSats (i.e., reduced mass and volume) allow to increase advantages of tests with respect to analyses. For example, testing CubeSat's thermal behaviour by means of thermal-balance test is worth in terms of time, instead of creating a complex model to conduct a very precise thermal analysis. Moreover, it is possible to verify the real functionality of the satellite under certain environmental conditions.

The proposed methodology is made up of two main activities, the first one is related to verification plan and the adaptation of ECSS-E-ST-10-02C, while the second is the tailoring of ECSS-E-ST-10-03C in a way to make CubeSat's verification phase cost-effective and time-saving. Obviously both activities are highly related because the tailoring of tests has a strong impact on verification planning and execution.

7.2.1 Verification planning

The verification planning, as it comes to light from Figure 37, it is detailed once the product requirements are already stated; i.e. at each design level a verification matrix, where product requirements, verification method and level are specified, is used as input for verification planning. The new methodology proposed in this section suggests a first updating of procedure, i.e. to use the verification planning not only for verification execution but also as an input for design (see Figure 38).

7 RELIABILITY-ORIENTED VERIFICATIONS OF CUBESATS

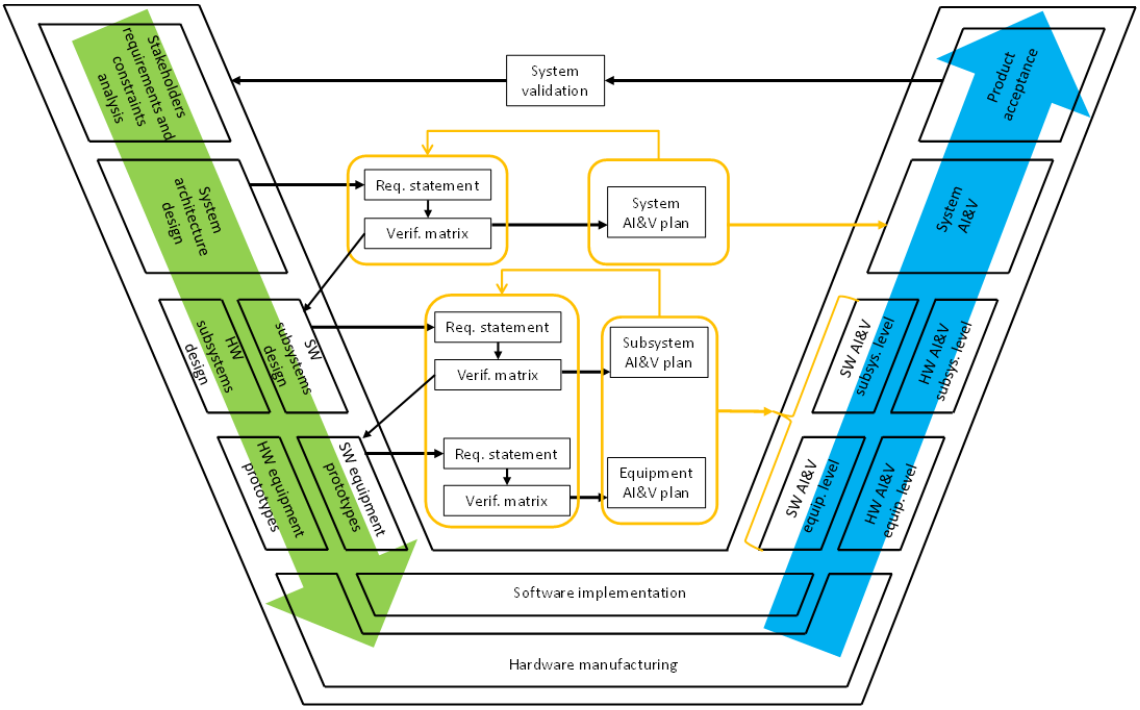


Figure 38: Verification activities within Vee-shaped model

Certain verification activities could require particular satellite functionalities that shall be taken into account during the design phases. For example, during thermal-vacuum cycling test normally satellite's functionality is tested. Hence, the CubeSat shall have the functionality to be activated/deactivated through ground support equipment. This capability shall be taken into account during design phase, however not always is conducted. Thus, it is clear that ignoring verification requirements during design phases could require future design modification/test adaptations with the consequence increase of cost and schedule delay.

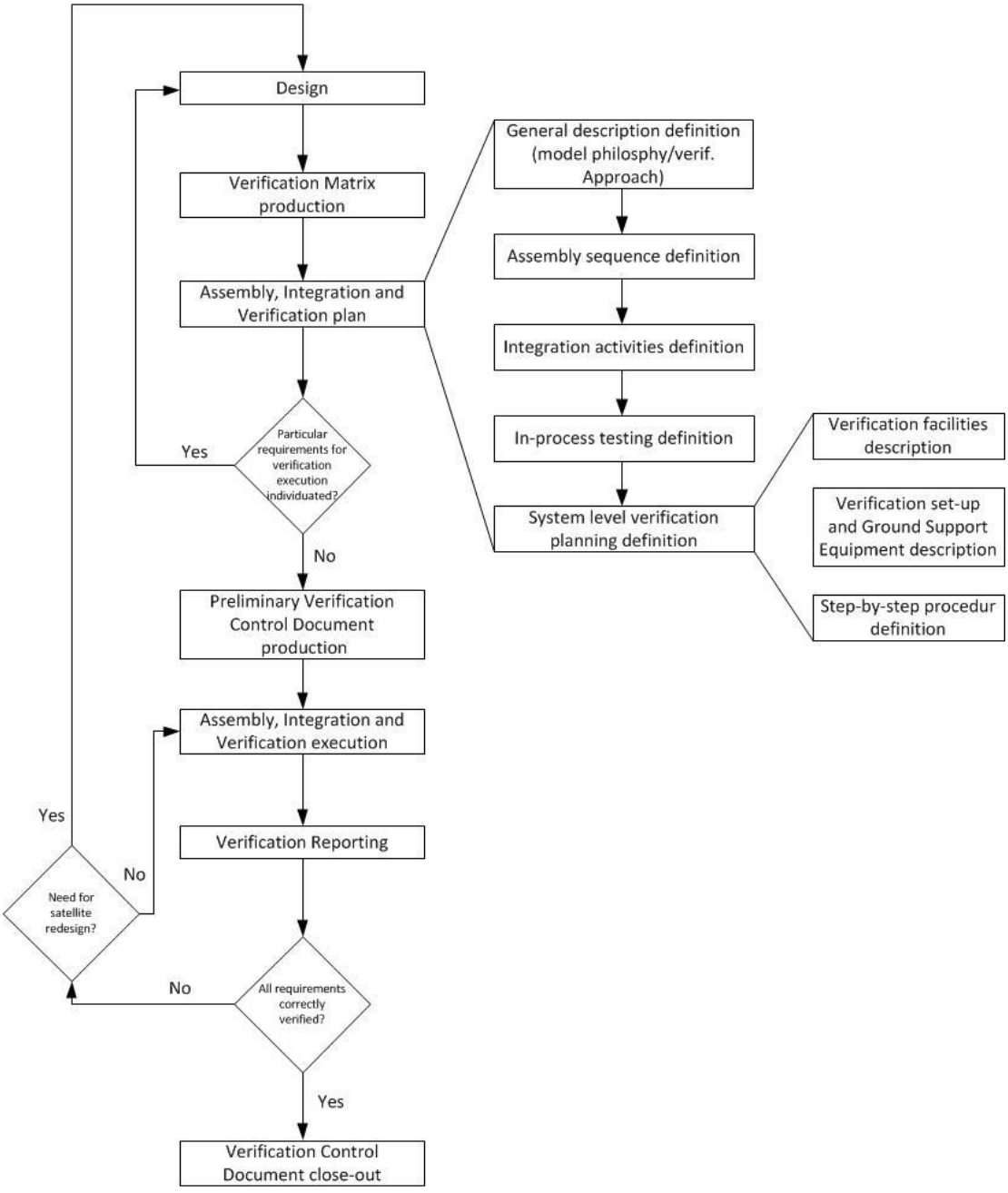


Figure 39: Verification activities flow-chart

A precise activities path to conduct verifications, from the design to the requirements close-out, is proposed in Figure 39. As stated before, it is necessary to take into account that, during verification planning, some requirements for verification execution can arise; and then shall be taken into account for a re-design of the satellite. Possible non-verified requirements

at the end of verification process can also lead to a need of re-design of the satellite. These two facts shall be represented in the verification activities flow, which are not stated in ECSS, as can see in Figure 37.

To conduct verification planning, it is necessary to define the levels and stages of the project at which the verifications will be conducted. Stages depend on the model philosophy adopted for the project (i.e., protoflight or prototype) while the levels depend upon the complexity of the project and on its characteristics. Taking into account CubeSat's intrinsic characteristics, equipment and subsystem levels are really close, and most of the times both of them are confused.

Finally, during verification planning the standard requires that certain number of documents shall be released. This list is extremely long for a CubeSat project, and to write all of them will probably bureaucratise too much this type of projects. Hence, it has been modified the requested documents regarding verification, mainly combining them, and stating their required content to minimise the paperwork. It is worth to remember, that the efforts shall be pointed to test the system, using it so much in so many situations that every possible way it could fail is found and fixed, using each failure to improve reliability. Paperwork shall be conducted to plan verifications and report them, but never to risk to death the program due to the high amount of documents to be produced.

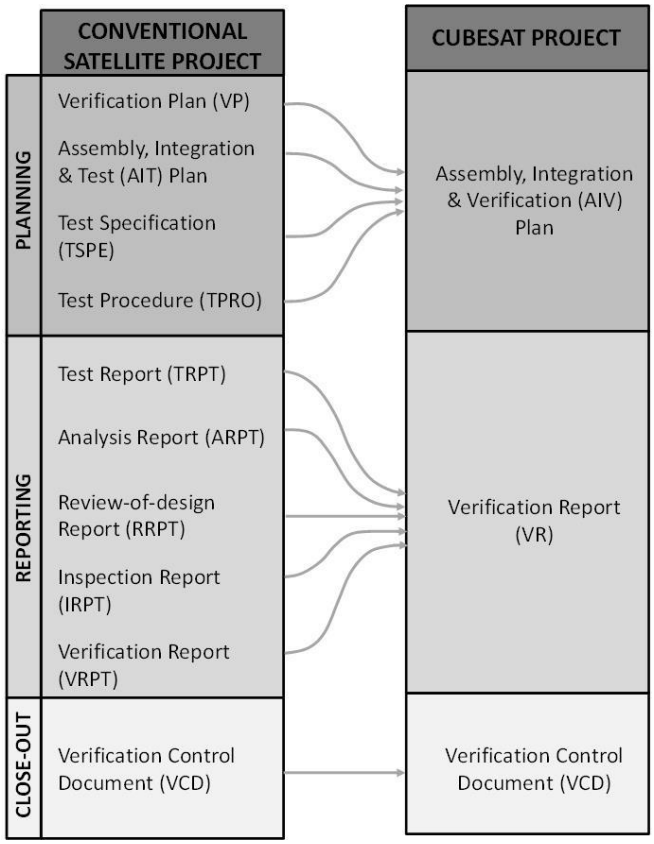


Figure 40: Adaptation of required documentation for verification process from standards for conventional space projects to CubeSats projects

Space project documentation for a space project required in the standards can be gathered in three groups: planning, reporting and close-out. The high amount of required documents is obviously overdemanding for a CubeSat project, and hence, a simplification of required paperwork is proposed, as presented in Figure 40.

In general terms, the proposed method for documentation simplification states to develop only three main documents, one for each activity of verification phase. It is important to not replicate information in the documents in order to avoid useless paperwork. A precise document structure and content has been defined to be applied to CubeSats projects. In particular, the contents of each of these documents should be:

- AIV Plan: As described in Figure 40, this document includes the contents of four different documents detailed in the standard, avoiding duplicity of information and

reducing its content to the minimum required to correctly conduct manufacturing and verification phase. The document should be divided in three parts. In the first one, general information about the satellite, including model philosophy adopted for its design and verification approach shall be specified. Second, the detailed procedure for mechanically assembly and integration of components to obtain subsystems from equipment level, and system from subsystems assembly and integration, shall be specified. Integration steps shall include possible intermediate test to be conducted during assembly and integration (e.g., electrical continuity, bonding, etc.). Finally, verifications at system level shall be planned. For each test it shall be specified: a description of the facilities in which the test will be conducted, the test set-up, required ground support equipment and a step-by-step procedure (i.e., required steps to conduct test, expected results and cross-correlation with requirements).

- Verification Report: this documents aims to gather the results of verification activities, to clearly state the requirements that have been verified, to specify verification close-out judgements and to describe any possible open issues remained after verification. For these reasons, the content can be tailored with respect to ECSS requirements, avoiding to repeat information already explained in the previous document (e.g. verification approach or model philosophy).
- Verification Control Document: this is the only document that shall contain the same information required for a conventional space project. Particularly, it shall contain the verification matrix, where all requirements are stated, specifying the verification method, the level and stage at which they shall be verified, the correlation with the document at which the verification is described, and the close-out judgement in binary terms (i.e., verified/non-verified).

7.2.2 CubeSat verifications at system level

Normally, standards shall be adapted to be applied to each project and, thus, each verification activity and product must be assessed as to its applicability to a specific project.

7.2 ECSS standards tailoring for CubeSats verification

However, the standardisation achieved with the CubeSat standard definition allows us to state a set of required verifications, regarding functionality as well as launch and space environment survival, which should be conducted for all CubeSats projects.

A study on the content of ECSS-E-ST-10-03C is conducted to assess the minimum required tests to be conducted in a CubeSat project at system level and especially to propose an optimised test schedule to obtain a time and cost effective verification phase. The abovementioned standard defines a system engineering approach with a description of required and optional tests, to be conducted at equipment and system level taking into account the model philosophy adopted for the project (i.e., protoflight or prototype approach). Moreover, different mandatory reviews to be conducted during testing process are specified.

It is evident that CubeSats can be different at subsystem level. Even so, at system level they are very similar. In particular, due to CubeSats standardisation the form-factor as well as mechanical interfaces with deployer adaptor are the same. Moreover, the standard CubeSat has been thought in a way that any possible debris due to a damage on the satellite remains inside the CubeSat structure and CubeSat's deployer, avoiding a damage to the primary payload and/or launcher. Hence, depending on different parameters like adopted model philosophy, launcher, orbit parameters, etc. different levels and durations of environmental tests can be applied. However, the same tests shall be conducted for all CubeSat projects in a certain step order.

7 RELIABILITY-ORIENTED VERIFICATIONS OF CUBESATS

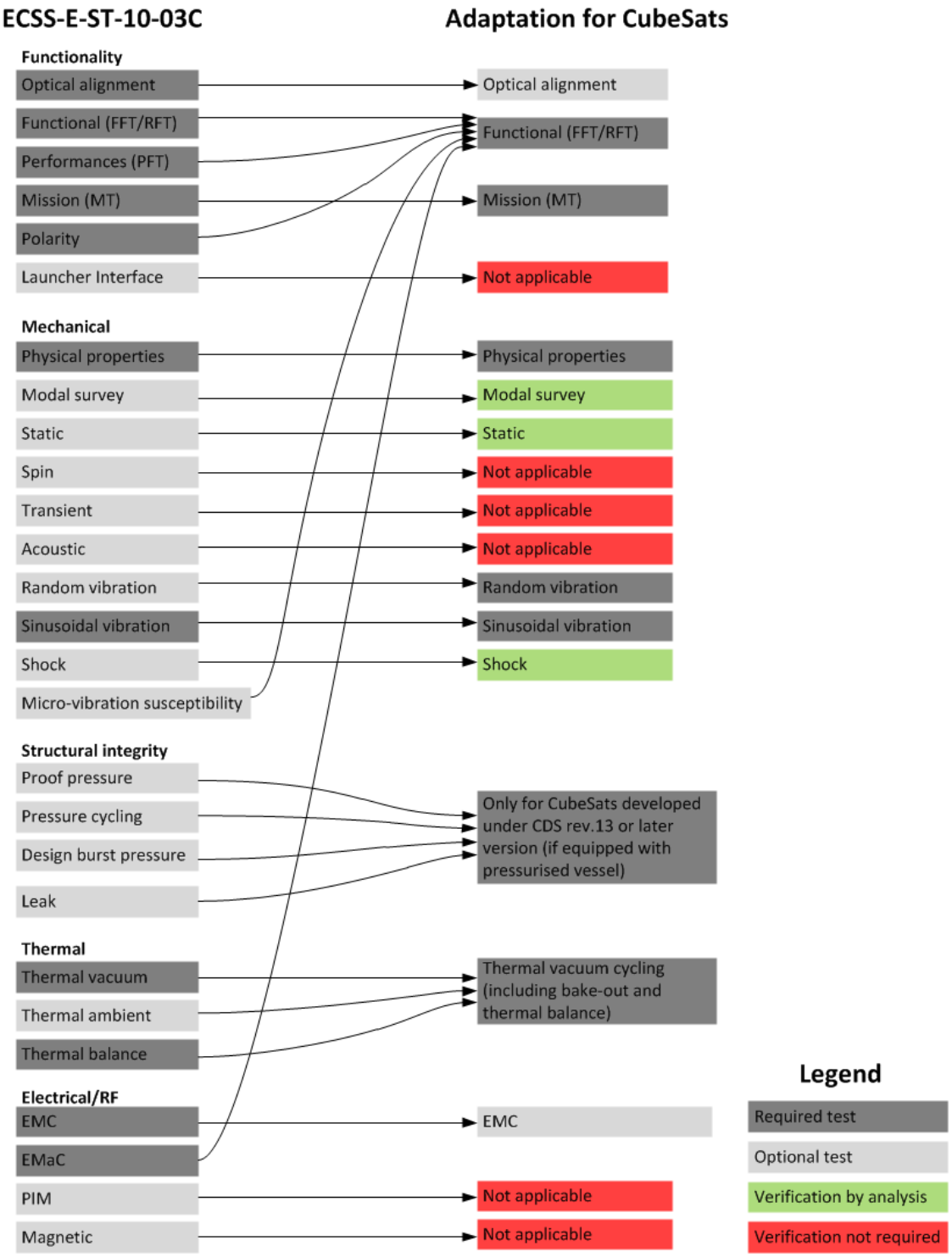


Figure 41: Standards required and optional tests, and proposed verifications for CubeSats

7.2 ECSS standards tailoring for CubeSats verification

Figure 41 shows the required (dark grey) and optional (light grey) tests for a space project designed following a protoflight approach at system level, and the proposed tests for CubeSats verification, considering also possible combinations for verification optimisation. Moreover, the verification methods for CubeSats verifications are detailed. It has been taken into account the protoflight approach because it is the one for which the standard envisages a wide number of tests. Note: the figure does not take into account required tests for space systems performing atmospheric entry nor for crewed missions.

Tests foreseen in standard have been gathered and classified in four groups for CubeSats projects: required tests, optional tests, not applicable tests or change test for analysis method. The verifications that have been individuated to be conducted in a CubeSat project at system level are:

Functional-oriented verification

Verification method: mandatory test

The functional verification shall be conducted by test. It aims at verifying functional requirements of the CubeSat. The test encompasses the functional, performance and polarity tests described in the standard. All of them can be conducted in one test for time and cost saving. In this test, all functionalities shall be tested, including all operative modes and transitions.

Additionally to the previous activities, the electromagnetic auto-compatibility test can be conducted during the functional test. I.e., it is checked that no electromagnetic disturbances created by the CubeSat itself are observed on the spacecraft functionality. Moreover, micro-vibration susceptibility tests, if applicable, can be conducted during the functional tests to evaluate the effect of potential sources to the component that is sensitive to micro-vibrations.

Mission-oriented verification

Verification method: mandatory test

Mission-oriented verification shall be conducted by means of test (i.e., mission test). It aims at verify the ability of the satellite to perform the mission and to identify anomalies not discernible in any other test before launch. In this kind of test the *test like you fly activities*

applies. This concept means *fly the mission on the ground*, i.e., perform the test following the entire mission profile (timeline and sequences). The mission test shall simulate, within the constraints of what can be simulated on ground, the real conditions that the satellite will meet on orbit, excluding environmental conditions (i.e., temperature and pressure), which are addressed during environmental verifications.

Optical alignment

Verification method: optional test

If CubeSat is equipped with optical components, a test shall be conducted to assess the correct alignment.

Physical properties

Verification method: mandatory test and analysis

Three main physical properties shall be verified: mass, centre of gravity (CoG) and moment of inertia (MoI). CubeSat's mass shall be verified by means of test using a precision scale. CoG and MoI shall be verified, at least, through analysis.

Modal survey

Verification method: mandatory analysis

The search of frequencies and mode shapes shall be conducted, at least, by analysis. A detailed CAD model shall be used to analyse the previous mentioned magnitudes. A highly simplified CAD model could lead to an increase of real modal frequencies.

Static

Verification method: mandatory analysis

In the same terms of modal survey, the verification that the satellite can cope with static loads can be conducted only by means of analysis. A correct analysis carried out with certified software is enough to verify the static loads requirement.

7.2 ECSS standards tailoring for CubeSats verification

Random vibration

Verification method: mandatory test

Random vibration test is primarily used to test and to qualify the CubeSat parts: electronic boards, instruments, etc. Random vibration tests are used to qualify flight hardware because they closely imitate the real launch environment by simultaneously exciting multiple frequencies. Random vibration levels and durations shall be agreed with launch provider.

Sinusoidal vibration

Verification method: mandatory test

Sinusoidal vibration test simulates the low-frequency sinusoidal dynamic loads. The sinusoidal tests are performed to verify the CubeSat structure dimensioning under the flight limit loads. Tests levels and durations shall be agreed with launch provider.

Shock

Verification method: mandatory analysis

Some launch providers could require a shock test. However, the characteristics of CubeSat projects allow avoiding this test and verifying shock response by means of analysis. In particular, the small dimension of the satellite, the closure of all components in the internal part of the structure and the installation of the CubeSat inside the deployer for the launch allow to conduct a shock sensitivity assessment instead of shock test.

Structural integrity

Verification method: mandatory test

Structural integrity tests include all verifications regarding pressurised vessels installed in the CubeSat. At the present, no CubeSats are equipped with this type of components because no pressurised vessels were allowed in accordance with CubeSat Design Specification (CDS) rev.12. However, the new revision of CDS (i.e., rev.13) allows the installation of this type of equipment. Hence, structural integrity tests shall be conducted if the pressurised vessel is installed in the satellite.

7 RELIABILITY-ORIENTED VERIFICATIONS OF CUBESATS

Thermal verifications

Verification method: mandatory test

Thermal verifications include four different activities: thermal-vacuum cycling test, thermal ambient cycling test, thermal balance test and bake-out test. In particular, thermal-vacuum cycling test aims at verify the correct functionality of the satellite when subjected to space environment in terms of temperature and pressure; thermal ambient cycling test is devoted to verify the correct operations of the spacecraft under space environment in terms of temperature (when the satellite will operate under a non-vacuum environment during its entire life); thermal balance test is conducted to verify the correctness of thermal analysis; bake-out test is conducted when some CubeSat materials are not compliant with respect to outgassing requirements. In this last case, the satellite is subjected to relatively high temperature under vacuum to allow outgassing of materials.

A combination of previous tests is proposed to reduce time and cost. First of all, thermal ambient test is not applicable due to the fact that the CubeSat will always operate under vacuum ambient. Hence, the thermal verification is a combination of the other three tests. In particular, during thermal-vacuum cycling tests, the maximum temperature reached during hot plateaux shall be maintained during certain duration to conduct a bake-out test. Furthermore, during the test, the characteristics on the temperature variation shall be correlated to the thermal model conducting, in this case, the thermal balance test during the first non-operational cycle.

ElectroMagnetic Compatibility (EMC)

Verification method: optional test

EMC test objective is to verify that the satellite is designed to achieve electromagnetic compatibility of the spacecraft in the presence of external electromagnetic environment.

7.2.3 Verification sequence

The verification process shall follow a precise sequence, as depicted in Figure 42.

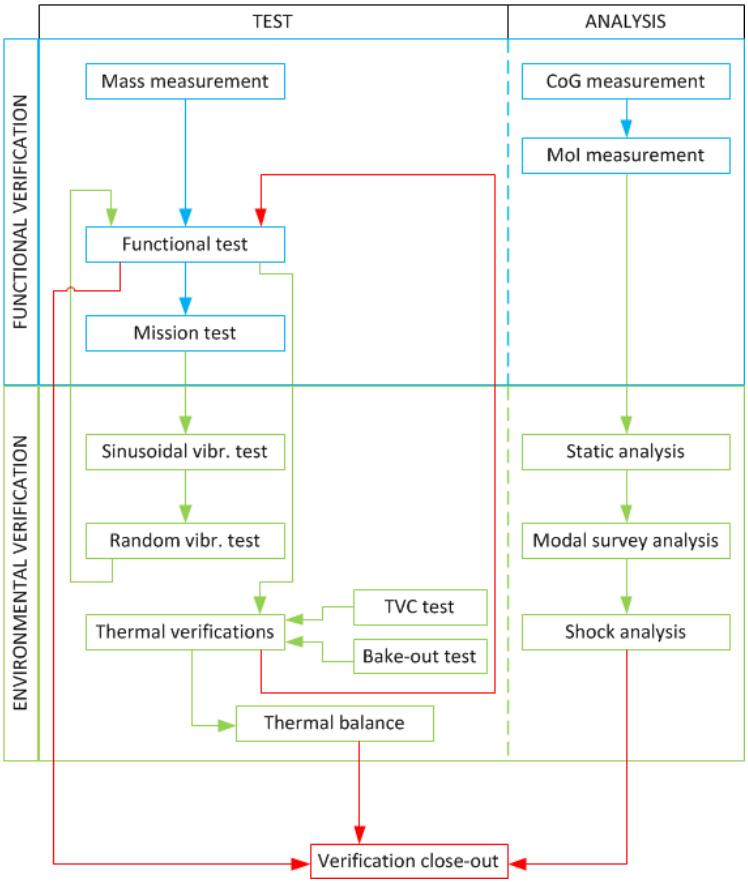


Figure 42: Sequence for CubeSats verification at system level

This sequence shall allow to verify the correct CubeSat functionality at ambient condition. Afterwards, environmental verification shall be conducted to assess that the CubeSat is able to survive launch and space environment. Moreover, the environmental tests shall be conducted in the precise sequence to be representative of life-cycle events. I.e., first of all launch takes place and then insertion into orbit. Hence, vibration tests shall be conducted before thermal-vacuum cycling test.

7.3 Case Study: e-st@r-II CubeSat

The previous proposed approach has been applied to e-st@r-II (Educational SaTellite at politecnico di toRino) CubeSat developed by the CubeSat Team at Politecnico di Torino within e-st@r program.

7.3.1.1 E-st@r-II CubeSat

E-st@r-II is a CubeSat developed as a follow-on of e-st@r-I, born with the same objective of testing on-orbit an active attitude determination and control subsystem. Generally speaking, the spacecraft architecture is identical to the first version of the satellite, represented in Figure 35. Due to the observed on-orbit failures of the first satellite, the post-mission FMECA analysis (see section 6.5) suggested making some minor modifications both in the hardware and in the software of the new satellite. Hereafter, the main differences between e-st@r-I and e-st@r-II, divided by subsystem, are highlighted (from the structure and thermal control system point of view, no modifications have been applied). These differences have obviously conditioned the application of the previous method. The differences are:

- Active ADCS: main changes with respect to e-st@r-I design are in the modes of operation of the payload rather than in the hardware configuration. In e-st@r-I the payload was activated autonomously on-board immediately after the CubeSat was released from the deployer, as also observed in the FMECA. This point was identified as one of the most critical once, because it could lead to a fast batteries depleting. In the new design, the payload is activated upon command from the ground control station, as detailed later on in section 7.3.1.4. To permit this new functionality, a circuit has been added in the printed circuit board (PCB), with respect to e-st@r-I ADCS PCB. Regarding the hardware, second minor modification regards the position of magnetorquers, which were placed internally on the structure in e-st@r-I. In the new satellite, to allow the reduction of internal complexity, they have been installed externally between structure and solar panels.
- EPS: this subsystem has been individuated as one of the most critical of e-st@r-I CubeSat in the FMECA analysis. Hence, the difference states in the storage,

regulation and distribution hardware. In particular, the batteries and regulation unit have been substituted by COTS hardware from a commercial company with recognised space engineering background.

- OBC: modifications and new operational modes have been applied, mainly related to new payload operations. These modifications applied to OBC software.
- COMSYS: in the case of this subsystem, the difference states in the software. In the new CubeSat, this subsystem is aimed to detect autonomously faults and recover communications using stored software sequence and hardware reset. In particular, a beacon signal (self-generated by the COMSYS and modulated in CW) has been implemented if no data are provided by the OBC for 5 minutes. Concretely, the string "estar2" is transmitted in Morse code. In case of a request for RF cessation, CW transmission can be stopped using a specific command from GCS. This command also works in case of OBC failure because it is executed directly from the COMSYS.

7.3.1.2 E-st@r-II mission architecture

E-st@r-II mission architecture is composed by classical space missions' elements, shown schematically in Figure 43. In particular:

- Space segment: e-st@r-II, a 1U CubeSats (payload and bus). The platform includes all subsystems in support of payload operations (i.e. bus), and the payload, which is an active attitude determination and control subsystem. A detailed description of the CubeSat is given in section 6.5.2.
- Ground segment: the ground segment of the e-st@r program (and hence, for the e-st@r-II project) consists of two ground stations: the main Ground Control Station (GCS) is the ARI – section of Bra (Ham Radio Club) and the second is the Mobile Ground Control Station (MGCS) located at Politecnico di Torino that is transportable and may be transferred everywhere. ARI-Bra station is an existing radio amateur station that supplies all the elements needed to communicate with e-st@r-II satellite: it is able to send commands to the satellite and to receive the telemetry packets. Other stations around the world (radio amateur network) may receive the CubeSat signal, but not command it.

- Launch segment: piggy-back launch is envisaged, but at the moment it is not yet defined.
- Subject: data measurement. Payload essentially senses the LEO environment, in terms of magnetic field. Data from magnetometer are used for his attitude determination task. Moreover, the satellite shall provide a large quantity of data about this orientation and angular velocities. These data will be subject of analysis on ground to verify the determination and control algorithms. Other telemetry data (i.e. temperatures, battery state of charge, on-board computer status, and communication system status) will be collected and analysed on ground to verify the proper functioning of COTS components, self-made hardware and software.
- Orbit: injection into LEO is foreseen, but at the moment the orbital elements are unknown.
- Operations: students at main and backup GCSs. Data processing at Systems and Technologies for Aerospace Research Laboratory (STARLab) for deeper investigation, or in case of emergency. Radio-amateur network and CubeSat Community will be involved in the data collection and will support the mission operations.
- Communications: telemetry data are sent by the CubeSat to the main GCS and to other stations all over the world. Data are coded in a defined protocol and transmitted to ground. The uplink commands are received on-board and relayed to other subsystems (mainly the OBC) according to a defined protocol. The downlink protocol is public in order to reach the largest quantity of ground stations and gather most data as possible. Uplink protocol instead, is not published and encrypted with secure code to avoid unauthorised commands from being transmitted and accepted by the satellite.

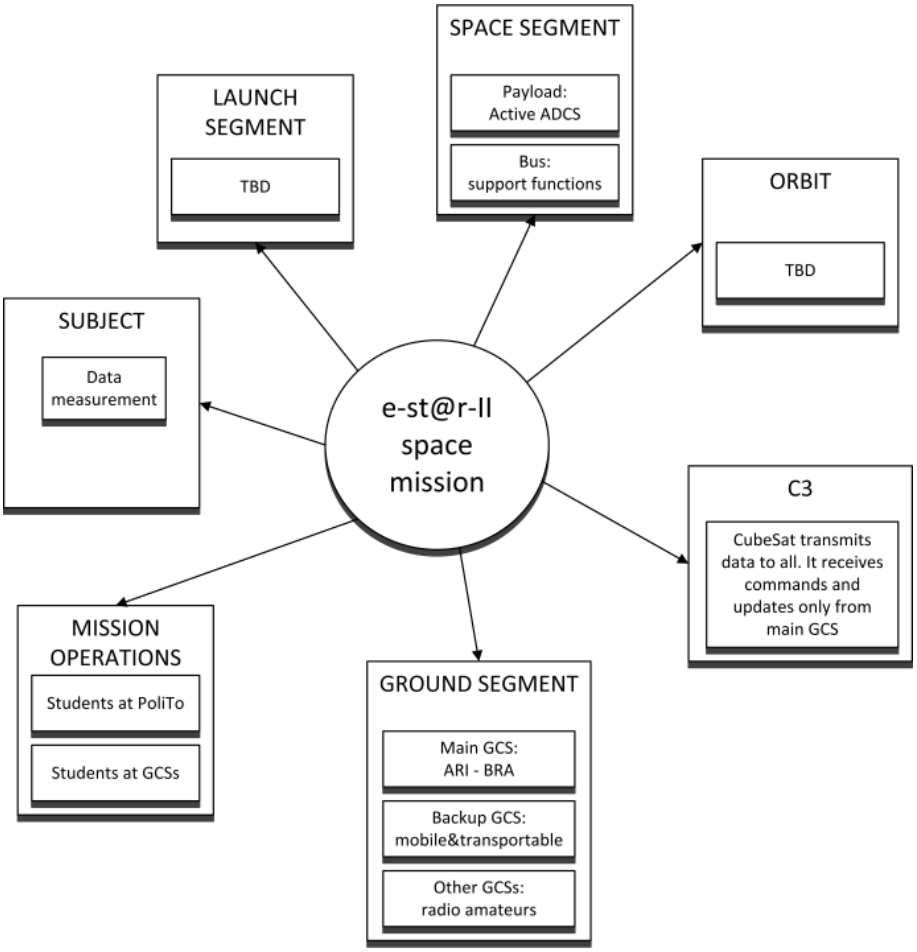


Figure 43: e-st@r-II mission architecture

7.3.1.3 E-st@r-II mission phases

A precise mission profile has been defined for the e-st@r-II mission. The mission phases are depicted in Table 9, which includes only orbit lifetime.

Table 9: e-st@r-II mission profile

Phase/Event	Duration	Description
Launch	T0	T0 is the actual lift-off time of the launch vehicle
CubeSat release and activation	T1	T1 is given by the burnout time necessary to reach the orbit plus the time needed to be ejected from the deployer. The CubeSat is instantaneously activated by the DS and enters the first mission phase in orbit
CubeSat appendages deployment	T2	T2 is given by the time delay imposed by CDS (30 min + margin) plus the time needed to deploy the antenna (approximately 1 minute)
Commissioning	T3	T3 is the time needed to prepare and check out the CubeSat for nominal operations. T3 ranges from a minimum of 10 minutes to several days, depending on commissioning activity result
Begin of mission	T4	T4 is the time at which the nominal mission begins officially
End of mission	T5	T5 = 1 (TBC)-to-12 (TBC) months after T4. Extended duration shall be considered.
Disposal of CubeSat	T6	T6 is the time needed for the orbit to decay after the mission has been declared finished (after which the CubeSat will burn in the upper layer of Earth's atmosphere).

7.3.1.4 E-st@r-II operational modes

Different operational modes have been implemented to allow the CubeSat to accomplish its mission. They depend upon the mission phase and operational needs. They have been derived from the applicable requirements and the mission phases. In particular, potential failures and malfunctions have been considered. Moreover, transitions between modes of operation have been implemented, and it can be either automatic or commanded from ground, as depicted in Figure 44.

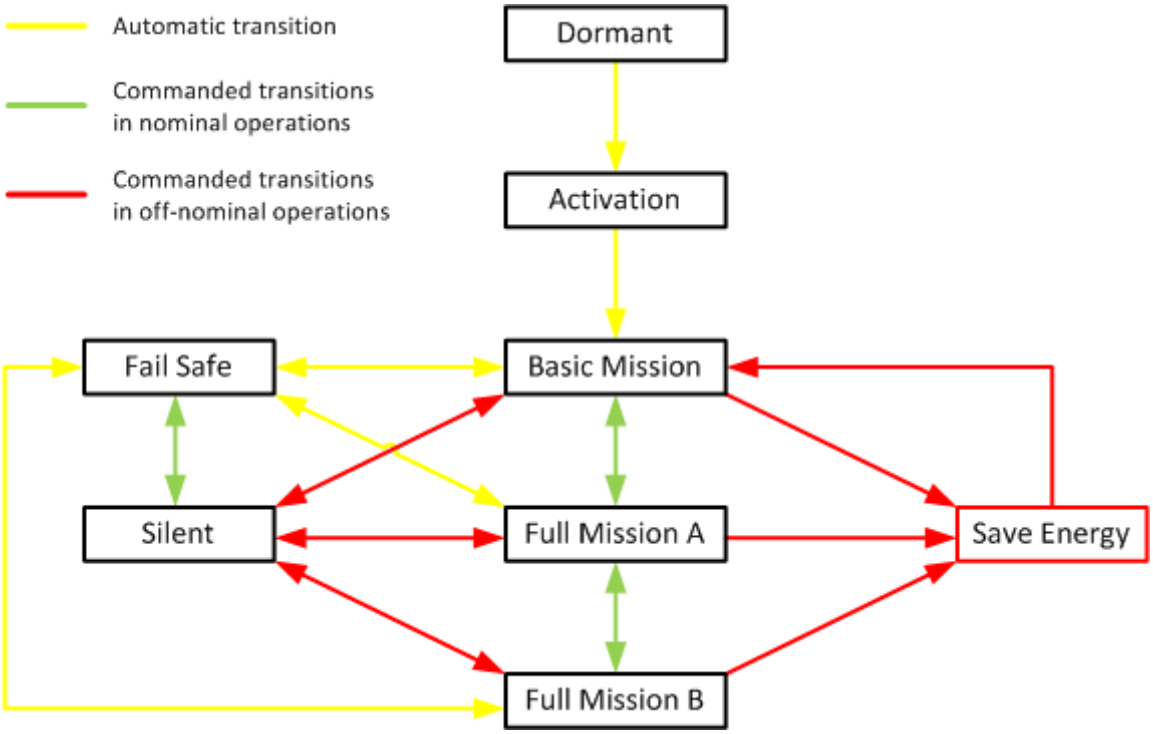


Figure 44: e-st@r-II modes of operations and transitions

The operative modes that have been designed and implemented are described in Table 10, which reports also the associated mission phases. In case some failures occur, the satellite can operate in degraded modes.

Table 10: e-st@r-II operational modes

Mode	Mission phase	Description
Dormant	Launch and CubeSat release	The CubeSat is "dormant", no RF emissions, no power consumption. All the subsystems are turned off
Activation	CubeSat appendage deployment	The CubeSat is activated by the DS. EPS is active. ADCS is in Mode 0: no component is active. The OBC starts booting and remains in a stand-by mode until all necessary checks are passed. Then the antenna is deployed. This mode is irreversible and cannot be repeated after the antenna deployment
Basic Mission	Commissioning Nominal mission	The CubeSat sends telemetry packets to ground every 120 seconds. It may receive commands from main GCS and execute them
Full Mission A	Nominal mission	The payload is activated. It performs the angular velocity damping using magnetometers and magnetic actuators (i.e. detumbling)

Full Mission B	Nominal mission	The payload is active and attitude determination is conducted. Gyroscopes measurements are used together with the magnetometer ones to estimate the attitude with an Multiplicative Extended Kalman Filter
Fail Safe	Commissioning Nominal mission	This is an off-nominal operative mode, and it is used in case communication between OBC and COMSYS fails. In this case, COMSYS autonomously sends Morse code (CW) every 5 minutes
Save Energy	Commissioning Nominal mission End-of-life	This is an off-nominal operative mode, and it is used in case low power is detected on-board. The CubeSat only carries out vital functions at minimum power consumption upon command from ground. Communication to Earth is stopped. Payload is deactivated
Silent	Commissioning Nominal mission End-of-life	In this mode communication to Earth is stopped. This mode is used in case a shutdown command is sent to the CubeSat upon request of ITU

Figure 45 shows the diagram of the mission phases and the relative modes of operation of the satellite during each phase.

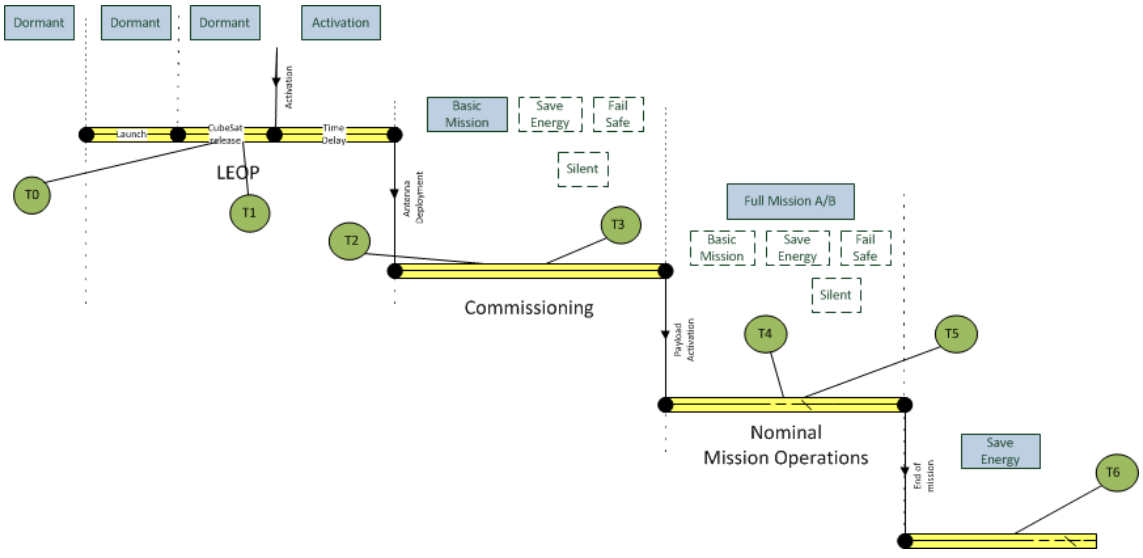


Figure 45: e-st@r-II mission phases and operational modes

7.3.1.5 Fly-Your-Satellite! Program

E-st@r-II project was selected as one of the six CubeSats to participate in the Phase 1 of the Fly Your Satellite! (FYS!) Programme launched by ESA Education Office at beginning 2013. The 'Fly Your Satellite!' programme is an exciting initiative from the Education and Knowledge Management Office of the European Space Agency focused on CubeSat projects run by university students. The programme is one of the several hands-on opportunities offered by ESA Education and provides experience of the full lifecycle of a space project. ESA provides the CubeSat teams with direct support from ESA technical specialists and access to state-of-the-art environmental test facilities. ESA will also procure a launch opportunity for selected CubeSats.

E-st@r-II successfully completed the first phase after the Technical Requirements Review in October 2013. At the date of the present thesis edition, the CubeSat is one of the three CubeSats that completed the development and functional testing in ambient conditions during the Phase 2, and it will be subjected to environmental test campaign scheduled for beginning 2015 at European Space Research and Technology Centre (ESTEC) facilities. Functional and environmental verifications has been and will be conducted following verification planning developed within the present PhD in accordance with methodology detailed above. The precise verification planning is detailed in the next section.

7.3.2 Assembly, Integration and Verification of e-st@r-II

E-st@r-II AI&V activities have been planned and executed following the studied method detailed in the previous section. The detailed information on how to conduct these three activities are gathered in the *e-st@r-II AIV document* composed by the information detailed in section 7.2.1. In particular, the document encompasses the assembly and integration plan of the satellite, divided in two main steps (i.e. preliminary integration and final assembly and integration) that includes the verifications to be conducted at component/subsystem level; followed by a specific section that includes verification plan for verifications at system level (i.e. functional and mission tests at ambient conditions, and environmental tests).

7.3.2.1 Assembly and Integration plan

As already introduced before, the A&I plan is organised in three sections, as shown in Figure 46. The first one includes the preliminary integration of the satellite in order to obtain the subsystems. In the second section the mechanical and electrical assembly and integration of subsystems is conducted. At the end, final assembly and integration of structure and solar panels is carried out. Moreover, two tests are foreseen (which will be explained in the verification plan section): in-process test and Integrated System Test (IST). The steps of second and third activities are detailed in Figure 47.

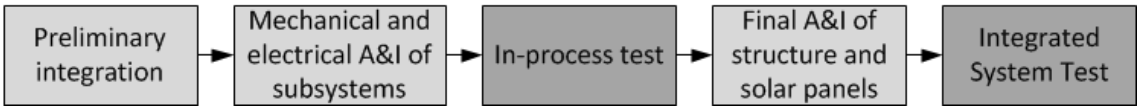


Figure 46: Assembly and Integration sequence of activities

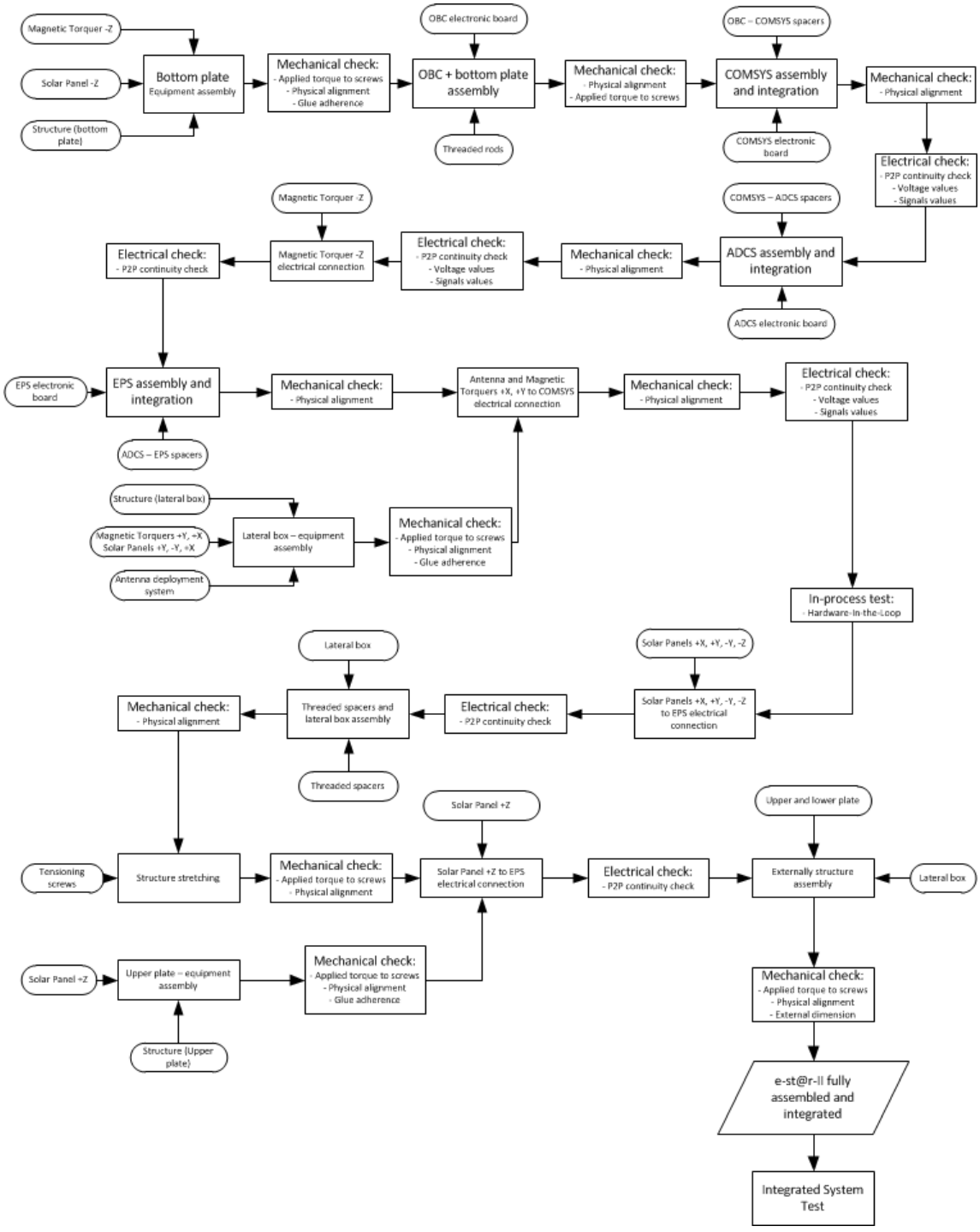


Figure 47: Assembly and Integration sequence

7 RELIABILITY-ORIENTED VERIFICATIONS OF CUBESATS

The preliminary integration consists on the mechanically and electrically integration of the three components: 1) SD card on the OBC board, 2) PIC-16 microcontroller on the COMSYS board, and 3) ARM-9 microcontroller on ADCS board. A functional test is conducted on each board after integrations to assess the correctness of the conducted activity.

The mechanical and electrical assembly and integration of subsystems is the main activity from which the CubeSat flight model is obtained. Starting from bottom plate, each subsystem is assembled and integrated following the established procedure (excluding structure and solar panels for further verifications to be conducted with in-process test). Between each step, different checks are conducted to assure that the assembly and integration has been conducted correctly. In particular:

- Mechanical checks: mainly three verifications are conducted. First, physical alignment measurement by means of calliper and ruler is carried out to verify the correctness of the mechanical assembly. Then, the mass of each assembled part is measured through precise scale to verify that the parameter is within the requirement. During structure assembly, applied torque to screws is measured and evaluated to assess that the correct torque has been applied.
- Electrical checks: these checks mainly consist in three tests. First, a point-to-point continuity test is conducted to verify that electrical paths are established between two identified points (i.e. the identified path conducts electricity as expected). Voltage and signals values are then measured. With these two tests it is intended to verify the correct voltage values in the identified points (e.g. regulated bus, microcontroller input voltage, etc.) and signal values (e.g. COMSYS PIC-16 microprocessor signals).

Before the final integration of solar panels and structure, an in-process test based on hardware-in-the-loop technique is performed to demonstrate the correct behaviour of the satellite focusing on the good functionality of the payload.

In the final assembly and integration the solar panels are connected to EPS board and the assembly of the structure is conducted. An Integrated System Test (IST) was envisaged to be

conducted after the assembly and integration to verify that the previous activities were correctly performed.

7.3.2.2 Verifications planning

The verification plan encompasses different functional tests and environmental tests, as observed in Figure 48, where steps in sequential way are represented and linked to required documentation to execute the verification activities.

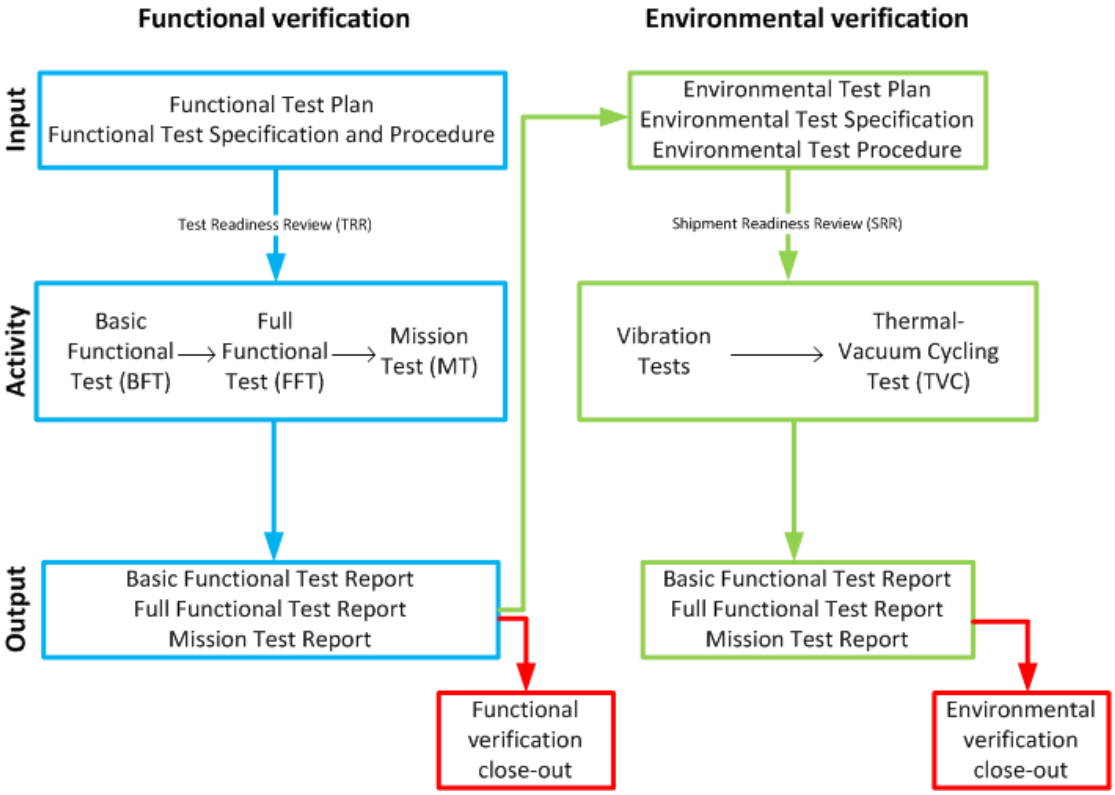


Figure 48: e-st@r-II verification activities and required documentation

The AIV plan is constituted by five different parts. In particular, two of them regard functional verification while three concern environmental verification. In test plans a general description of test activities (i.e., BFT, FFT and MT for functional verification, and TVC and vibration tests for environmental verification) are detailed. In Test specification and procedure technical information are explained. In particular, the requirements to be verified (around 300 for the e-st@r-II project), test facilities, set-up and tools, pass/fail criteria, step-by-step

procedure as well as documentation to be produced after the verification execution. The foreseen functional verifications are the following:

- Basic Functional Test: it aims at verifying the requirements against the basic functionalities needed to conduct the basic mission (i.e., no activation of the payload).
- Full Functional Test: it aims at verifying all the requirements, including those related to the payload. A tailored FFT is expected to be conducted during TVC test at hot and cold temperatures.
- Mission Test: it aims at verifying the ability of the satellite to perform the mission and to identify anomalies not discernible in any other test before launch. In this kind of test the *test like you fly activities* applies. In this case, the test execution shall last a minimum of one week. Due to this fact that it is intended to simulate the mission, the CubeSat shall be maintained active for the whole duration of the test. Hence, due to the lack of solar simulator at Politecnico di Torino, the solar panels are simulated by means of programmable power supplier.

An analysis of the requirements leads to the definition of two different environmental tests to be conducted at system level:

- Vibration Tests: sinusoidal and random vibration tests
- TVC Test: outgassing data was not available for some parts of the satellite. Hence, bake-out test were required to be conducted. ESA specialists accepted the proposal of conducting the bake-out during thermal-vacuum cycling test. The hot plateaux are held for a total of 140 hours to assure a good confidence that the materials will not outgas during launch.

Regarding verification management, during verification process two main reviews has been conducted with ESA specialists. In particular:

- Test Readiness Review: during this review, the Team demonstrated to ESA specialists the correctness of the functional verification planning and the readiness of the CubeSat flight model to be subjected to functional tests.

- Shipment Readiness Review: the SRRe has been conducted between the Team and ESA specialists, during which the correctness of environmental verification planning and the readiness of the CubeSat have been demonstrated. ESA representatives released the authorisation to proceed with environmental verification campaign at ESA/ESTEC facilities.

Functional Verifications

The objective of the test campaign is to verify, under ambient conditions, that the CubeSat performs the operations for which it has been designed. In particular, the functional verification campaign is aimed at demonstrating that the spacecraft accomplishes all the expected functions and is able to accomplish the designed mission.

The test planning begins with the identification of the functional requirements that the CubeSat shall satisfy and hence the functions to be executed. These requirements are stated in the verification matrix. The test activities consist, as previously introduced, of a Functional Tests (FTs) and Mission Test (MT). Moreover, during FTs some requirements are verified by means of direct measurement of the parameter by means of GSE (e.g. battery voltages). Specifically, functional tests verify the system versus the requirements, which specify the expected values to be obtained during the tests. In the other hand, mission test verifies the system against the mission, keeping in mind the mission profile. A diagram of the context for the functional tests and mission test is shown in Figure 49.

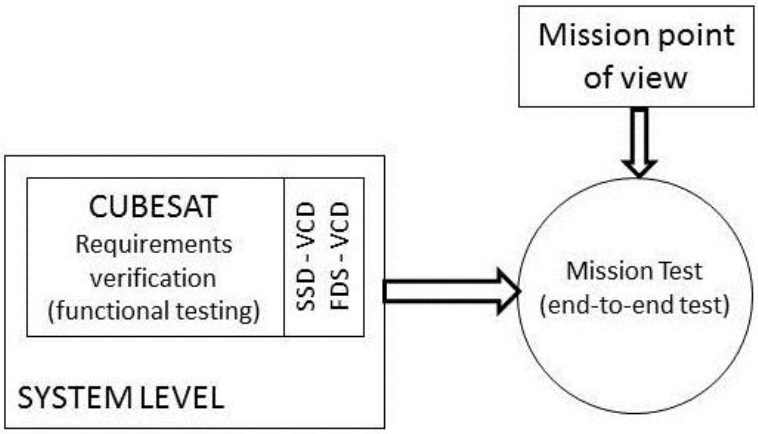


Figure 49: Context for the functional tests and mission test

Along with this information, the pass-fail criteria for each requirement has been stated together with the mapping matrix, where the correlations between each requirement and step of the procedure in which it is verified are stated. In Table 11 and Table 12 pass-fail criteria and mapping matrix for full functional test are reported as an example of the previous explained activities. These activities have been also conducted for all other verifications (Basic Functional Test and Mission Test). However, in order to allow a smooth read of the thesis, only full functional test has been stated as an example.

Table 11: Full Functional Test pass-fail criteria

Functions to be verified	Action	Pass/Fail Criteria (summary)	Requirements verified
Satellite dormant mode	Direct measurement	Power line, 3.3V, 5V and battery bus are deactivated by the DS.	SSR.05 OPS.07_02
Satellite activation	Direct measurement	The power line is activated by the DS release and Voltage on H2 36 is equal to battery state of charge (with margin) 3.3V, 5V and battery bus are activated by the DS.	SSR-EPS-INT.01 SSR-EPS-INT.02
Antenna deployment	Visual inspection	Antenna is deployed after 30 min	OPS.07_02 OPS.04
Basic Mode correct execution	Data analysis	The first telemetry is received after 30 min from DS release. Telemetry packets are received on GCS and data are consistent with basic mode of operation. Packets are received any 120 +/- 15 sec, and include the expected information in the correct format ADCS status = 0 Subsystems communicate via e-st@r-II bus Downlink is established in the correct frequency	OPS.05 SSR-F.05 SSR-F.10 SSR-F.10_03 SSR-OBC-F.01 SSR-OBC-F.01_04 SSR-OBC-F.05 SSR-COM-F.02 SSR-COM-D.06 OPS.07_03

Full Mission A mode correct execution	Data analysis	The command to switch to Full A is executed. Telemetry show that the IMU is active ADCS status = 1	OPS.07 SSR-OBC-F.01_10 OPS.07_04 SSR-F.03
Commands execution in Full Mission A The satellite is able to receive signal from ground, the OBC is able to manage commands, COMSYS is able to receive and demodulate commands on the designed frequency. GCS is able to send UHF signals and the GUI allows to send commands to the spacecraft	Data analysis	Commands are correctly sent to the spacecraft and the spacecraft returns the transponder. Telemetry data show the changes according to the commanded values OBC and ADCS dataflow show the changes according to the commanded values	SSR-F.05 SSR-F.10_03 SSR-OBC-F.01 SSR-COM-F.01 SSR-COM-F.07 SSR-COM-F.16 SSR-COM-D.06 GSR-HW-F.01 GSR-SW-GUI.05
Transition from Full Mission A to Full Mission B - Mode	Data analysis	The command to switch to Full B is executed. Telemetry shows that the IMU and magnetorquers are active. ADCS status = 2	OPS.07 SSR-OBC-F.01_10 OPS.07_04 SSR-F.04
Commands execution in Full Mission B The satellite is able to receive signal from ground, the OBC is able to manage commands, COMSYS is able to receive and demodulate commands on the designed frequency. GCS is able to send UHF signals and the GUI allows to send commands to the	Data analysis	Commands are correctly sent to the spacecraft and the spacecraft returns the transponder. Telemetry data show the changes according to the commanded values OBC and ADCS dataflow show the changes according to the commanded values	SSR-F.05 SSR-F.10_03 SSR-OBC-F.01 SSR-COM-F.01 SSR-COM-F.07 SSR-COM-F.16 SSR-COM-D.06 GSR-HW-F.01

spacecraft			GSR-SW-GUI.05
Transition from Full Mission A to Save Energy Mode Transition from Basic Mode to Save Energy Mode Transition from Full Mission B to Save Energy Mode	Data analysis	The command to switch to Save Energy is executed. No RF signal on GCS No ADCS task is executed on ADCS interface OBC task are suspended in the OBC interface PC	OPS.07 SSR-OBC-F.01_10 OPS.07_06
Transition from Full Mission A to Silent Mode Transition from Basic to Silent Mode Transition from Full Mission B to Silent Mode	Data analysis	The command to switch to Silent mode is executed. No RF signal on GCS	OPS.07 SSR-OBC-F.01_10 OPS.03 GSR-SW-GUI.05_07 GSR-SW-GUI.05_11

Table 12: Full Functional Test mapping matrix

ID	Requirement	Step
OPS.04	The CubeSat shall be designed to deploy booms, antennas, and solar panels at least after a minimum of 30 minutes after the CubeSat's	920
OPS.05	The CubeSat shall be designed to wait a minimum of 30 minutes after the CubeSat's deployment switch(es) are activated from CubeSat	1100
OPS.07_02	An activation mode shall be implemented: the CubeSat shall be activated immediately after the release from the P-POD	1100
OPS.07	Different operative modes shall be implemented to control different mission phases and conditions (both nominal and off-normal)	1400 2250 2500
GSR-SW-GUI.05_01	Command to switch to different operative modes shall be implemented: basic, full, silent and save energy	3890
SSR-OBC-F.01_10	The OBC shall allow for operative mode switching	3890
OPS.07_04	A full mission mode shall be implemented: the CubeSat shall be able to point Earth, communicate with GCSs, and accomplish slew manoeuvres, if commanded to	1380 2720
SSR-F.03	The CubeSat shall be able to determine its attitude	1400
SSR-F.04	The CubeSat shall be able to control its attitude	2750
GSR-SW-GUI.05_08	Command to manoeuvre the satellite shall be implemented	2750
OPS.07_06	A save energy mode shall be implemented: the CubeSat shall carry out only vital functions at minimum power consumption upon command from ground. Communication to Earth is limited to some extent and eventually it can be totally stopped. This mode can also be used in case a shutdown command is sent to the CubeSat upon request of FCC.	2250 2500 3500
OPS.03	CubeSat shall be designed to accept a shutdown command, as per Federal Communications Commission (FCC) regulation	2140 3380
OPS.07_07	A Silent Mode shall be implemented: CubeSat shall be able to stop any RF signal if commanded to	2140 2380 3380
GSR-SW-GUI.05_07	Command to shut down the satellite shall be implemented	2140 2380 3380

The full Functional Test sequence is depicted in Figure 50.

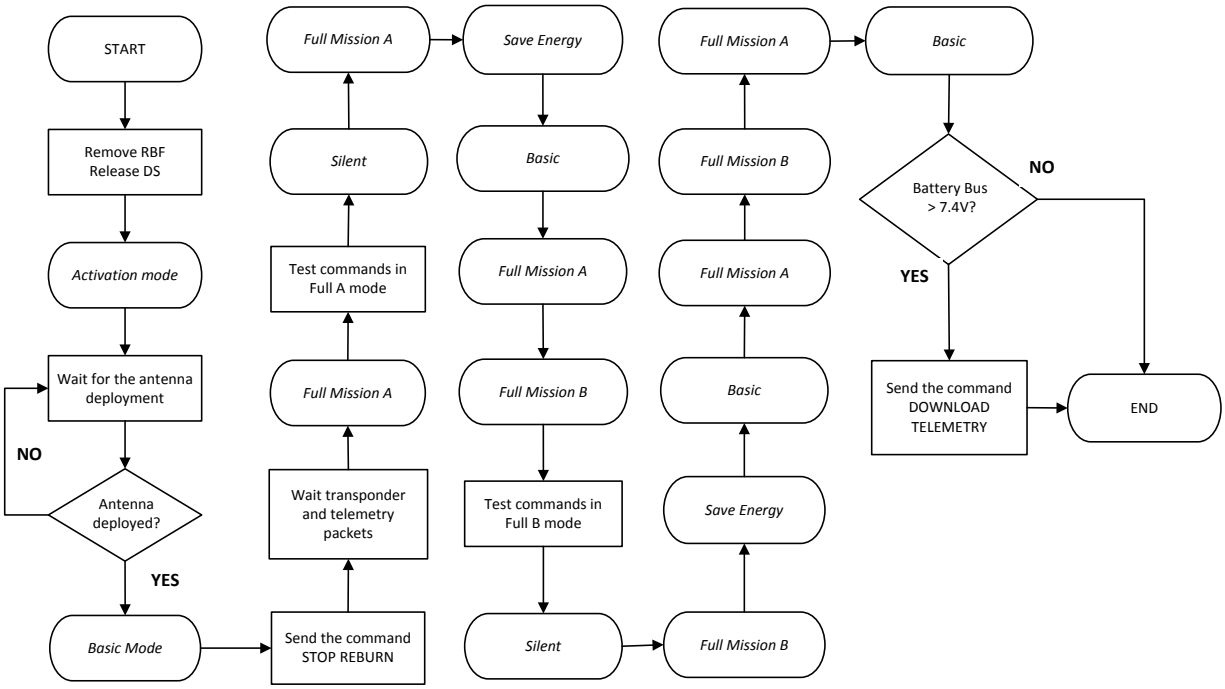


Figure 50: Full Functional Test sequence

The test set-up, sequence and step-by-step procedure are then stated. In particular, the test set-up for full functional test states as follows: The test will be performed during daytime, with the satellite fully integrated. The status of the satellite before the beginning of the test, and during the preparation, shall be *inactive*. GSE shall be set up in the designated area of the laboratory. MGCS software shall be initialized, and the MGCS shall be ready to receive the communication from the satellite with the radio frequency set to 437.485 MHz. TNC shall be set on 1200bps data rate. A backup of the GCS files from the previous communications shall be saved prior to the deletion of the files in the GCS log. The necessary connections with GSE shall be made with the satellite *inactive*.

A part of the step-by-step procedure for the Full Functional Test is shown in Table 13.

Table 13: Full Functional Test (partial) step-by-step procedure

Step n°	Action	Pass/Fail criteria	Expected Results	Actual result	Time	Anomalies	Remarks	Requirements verified
641	Insert the USB cable into the USB port of the OBC							
650	Read the dataflow on the OBC interface PC		Telemetry strings are present on the dataflow. OBC tasks are executed on the dataflow					
660	Confirm the correct data connection between OBC and EPS	Data analysis Dataflow and telemetry data show the status of the EPS. This criteria demonstrates that the EPS detects its status and communicates with the OBC	EPS task is executed on the dataflow. Telemetry strings are different from zero.					SSR-F.10_01 SSR-EPS-F.05 SSR-EPS-INT.01
670	Confirm the correct data connection between OBC and COMSYS	Data analysis The telemetry data is shown on the OBC dataflow and on the GCS interface. This demonstrates that • the OBC acquires data from subsystems • the OBC provide data to the COMSYS. • the COMSYS modulates telemetry from OBC	The first telemetry packet is received at the GCS					SSR-OBC-F.01_09 SSR-OBC-F.01_05 SSR-COM-F.16 SSR-F.10_02
680	Confirm the correct data connection between OBC and payload	Data analysis ADCS status is shown on the OBC dataflow in the OBC interface PC	ADCS task is executed on the dataflow					SSR-OBC-F.01_01 SSR-OBC-F.01_09
690	Confirm the first telemetry packet is sent	Data analysis The dataflow of the OBC shows COMSYS downlink string. This criteria demonstrates that COMSYS is able to transmit telemetry data signals,	COMSYS downlink string is executed on the dataflow.					SSR-COM-F.01 GSR-HW-F.01
700	Record time							

7 RELIABILITY-ORIENTED VERIFICATIONS OF CUBESATS

Environmental Verifications

The environmental verifications at system level consists on evaluating through test and analysis the capability of the CubeSat to withstand launch and space environment in terms of mechanical loads, temperature and pressure. The environmental verification plan foresees the verification of the static loads and natural frequencies by means of analysis conducted with Catia and Patran/Nastran tools. The verification plan envisage to verify the vibration and thermal-vacuum requirements by means of test. Following the defined method explained in the present chapter, the specifications and procedure for these tests have been stated. The tests will be conducted at ESA/ESTEC facilities under the supervision of ESA experts. The tests execution will follow the same order in which the satellite will encounter during the launch, i.e. first vibrations and then thermal-vacuum. The environmental verification plan has been detailed in the same way as the functional verification plan has been detailed. The verification matrix has been considered as the starting point from which all the requirements for environmental verification have been extracted. They have been classified based on the verification at which they have to be verified (analysis, vibration test, TVC test). The pass/fail criteria has been stated for each of them and the step-by-step procedure for each test have been established. Finally, the verification plan envisages the execution of functional tests before and after each environmental test (called Reduced Functional Tests – RFT) as well as different functional test during hot and cold plateaux of the TVC test (called TVC Functional Test – TFT). A flow-chart that depicts the environmental tests campaign activities is presented in Figure 51.

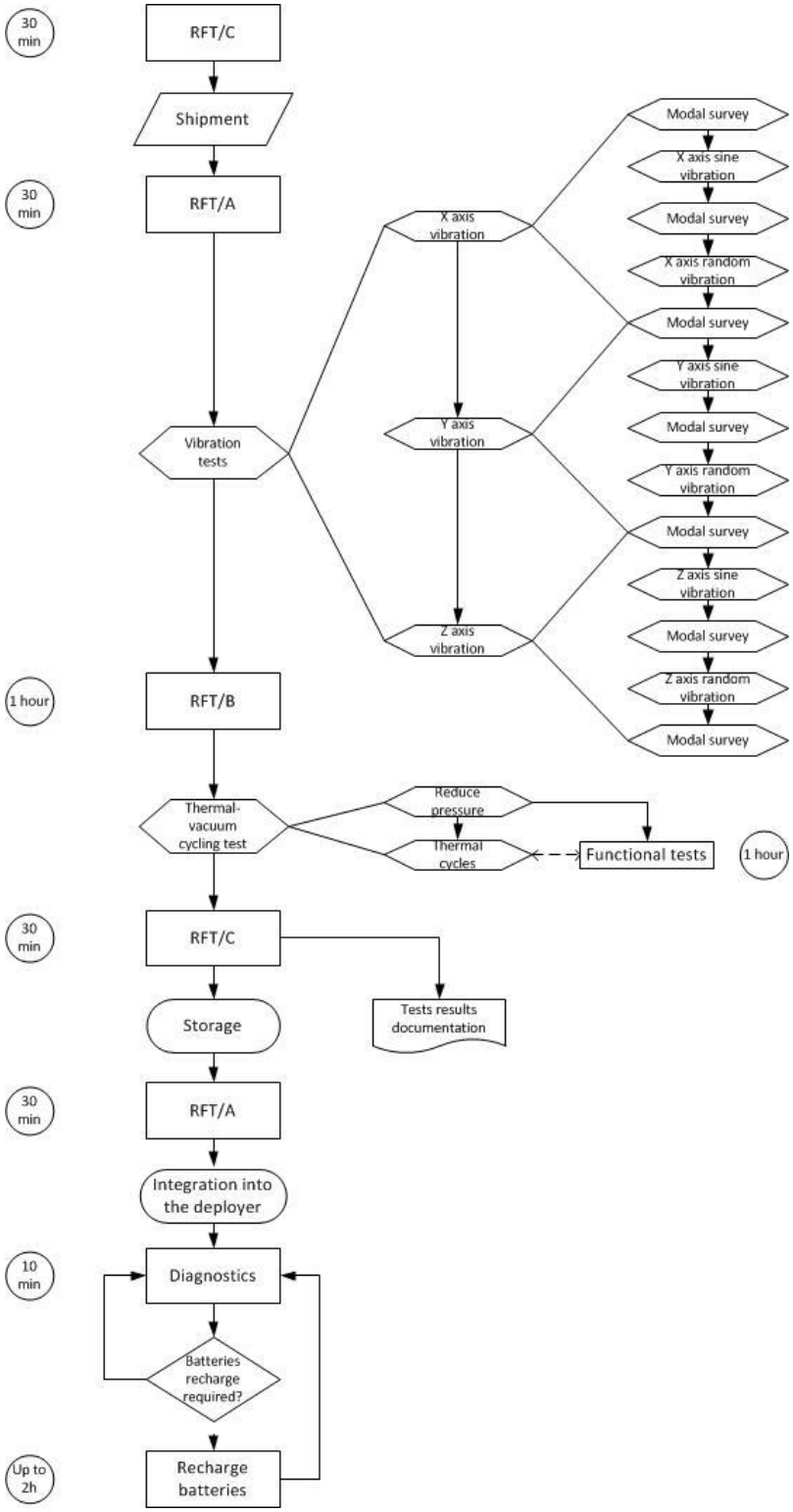


Figure 51: Environmental tests campaign activities flow-chart

The vibration tests encompass two type of vibrations: sinusoidal and random. The former is aimed at verifying the structure dimensioning under the flight limit loads while the latter, which substitutes acoustic vibrations test for spacecraft of reduced mass, is used to qualify flight hardware because it closely imitates the real launch environment by simultaneously exciting multiple frequencies. The step-by-step procedure foresees the insertion of the satellite in a test-deployer that will be installed on the electrodynamic shaker. In order to speed-up the test execution both vibration tests will be combined; i.e. instead of conduct first sinusoidal vibrations and then random vibrations, the excitation will be executed to X axis for both vibration types, then Y axis and then Z axis. The vibration levels have been established by ESA specialist based on previous experience on CubeSats launch and will be controlled on the satellite by means of accelerometers that will be installed on the satellite for this purpose and will be removed after the test.

As far as thermal-vacuum tests concerns, it has been envisaged to conduct, not only TVC test, but also bake-out test, as introduced above, due to the lack of information regarding some materials outgassing values. The need to conduct bake-out test represents a drawback for the Team, mainly because it implies a cost increase that the CubeSat Team cannot afford. Hence, it has been proposed, as already stated in the good practices for CubeSats development, to conduct the bake-out test during TVC test. This has been accepted by ESA specialists. Then, the TVC test will consist in four cycles of hot/cold temperatures under vacuum condition; and the hot temperature will be maintained for longer time to conduct bake-out test, as shown in Figure 52.

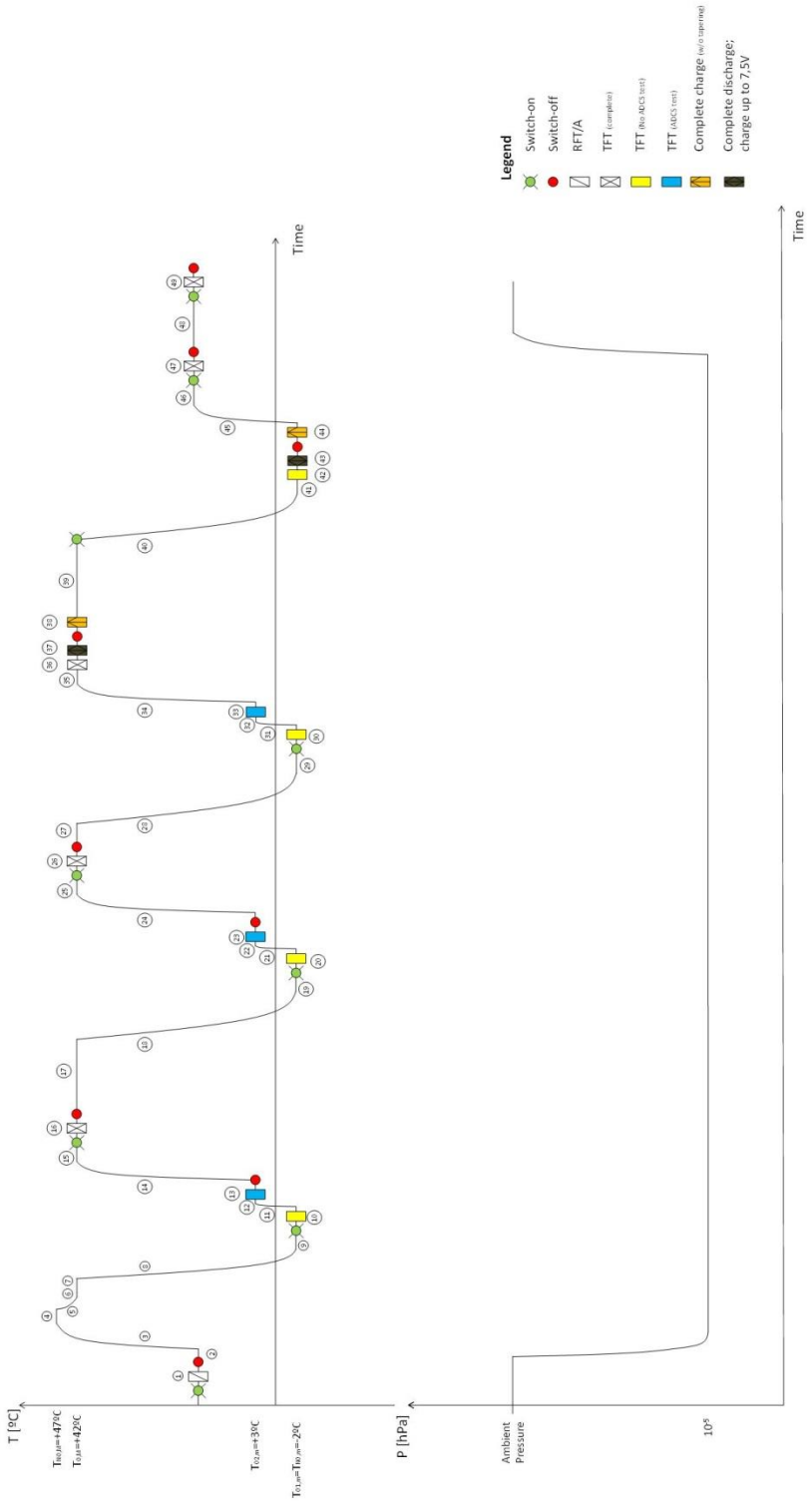


Figure 52: TVC test sequence

7 RELIABILITY-ORIENTED VERIFICATIONS OF CUBESATS

Going in-depth on the test description, during the first cycle the satellite will be non-operational, while the functionalities will be tested at hot and cold plateaux in the other three cycles. Moreover, a full discharge/charge cycle of the batteries at hot and cold plateaux will be conducted to assess the influence of temperature on undervoltage threshold protection. To conduct this test, four thermocouples have been installed on the satellite. The temperature limits have been established after a thermal analysis and also based on the components temperature ranges (operative and non-operative). Finally, a special ground support equipment (GSE) has been developed in order to control the activation of the satellite because the actual design does not allow to activate/deactivate the satellite by means of electrical connection. Hence, it has been installed a relay in parallel to the deployment switch from which the activation of the satellite is controlled. This equipment will be removed, after the verification execution. Moreover, the MGCS will be installed outside the TV chamber in order to communicate with the satellite. Finally, a set of voltmeters will be used to measure the batteries voltages. The connections will be conducted by means of one interface port (sub-D-25 connector) present on the facility. A schematics of the TVC test set-up is presented in Figure 53.

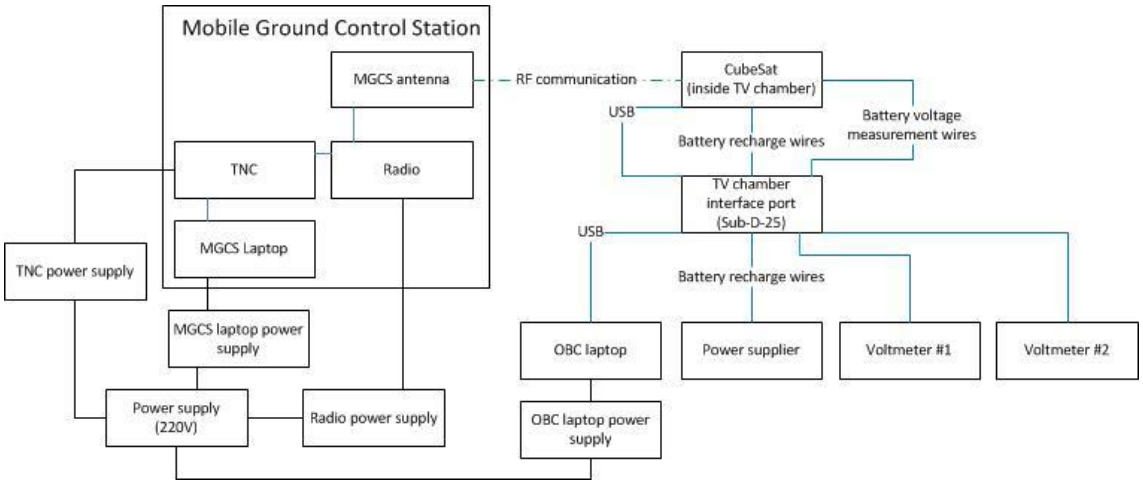


Figure 53: TVC test set-up schematics

As introduced above, a set of functional tests are foreseen to be conducted during the TVC test. Each RFT is identical with respect to tested command. The differences lay on the status of the SD card, where data is stored, before and after the test because could be needed

for future tests to leave the card full or empty. Iin particular, RFT/A and TFT will be performed during the TVC test. Concretely, the RFT/A will be conducted after insertion of the satellite in the TV chamber (and the TV chamber closure) at ambient temperature and pressure. This test is foreseen to assure the correct installation of the satellite inside the TV chamber. As already foreseen for the RFT/A, the SD card will be completely erased after the test in order to allow to test the antenna deployment system during the first TFT. Hence, the RFT/A will be conducted with the antenna folded. Then, the satellite will be switched-on again in the cold plateaux where TFT will be carried out. In this first test, the antenna deployment system will be tested. Then, TFT are envisaged in the other moments of the TVC test where the antenna deployment will not take place again. Finally, during the increase and decrease of temperature in the fourth cycle the satellite will remain switched-on and a TFT will be conducted.

7.3.2.3 Verification execution

Functional verifications have been conducted in the STARLab of the Politecnico di Torino. In Figure 54 a picture of e-st@r-II during Mission Test at STARLab is reported. The Laboratory constitutes the main facility where the CubeSat Team design and develop their projects.

Figure 54: e-st@r-II Mission Test at STARLab

The basic functional test has been carried out without errors, showing that the satellite is able to perform properly and contemporaneously basic functions and tasks as well as the on-orbit operations. Telemetry data contained in the packets are not corrupted as well as the commands are properly sent by the mobile ground control station (MGCS) and executed by the satellite.

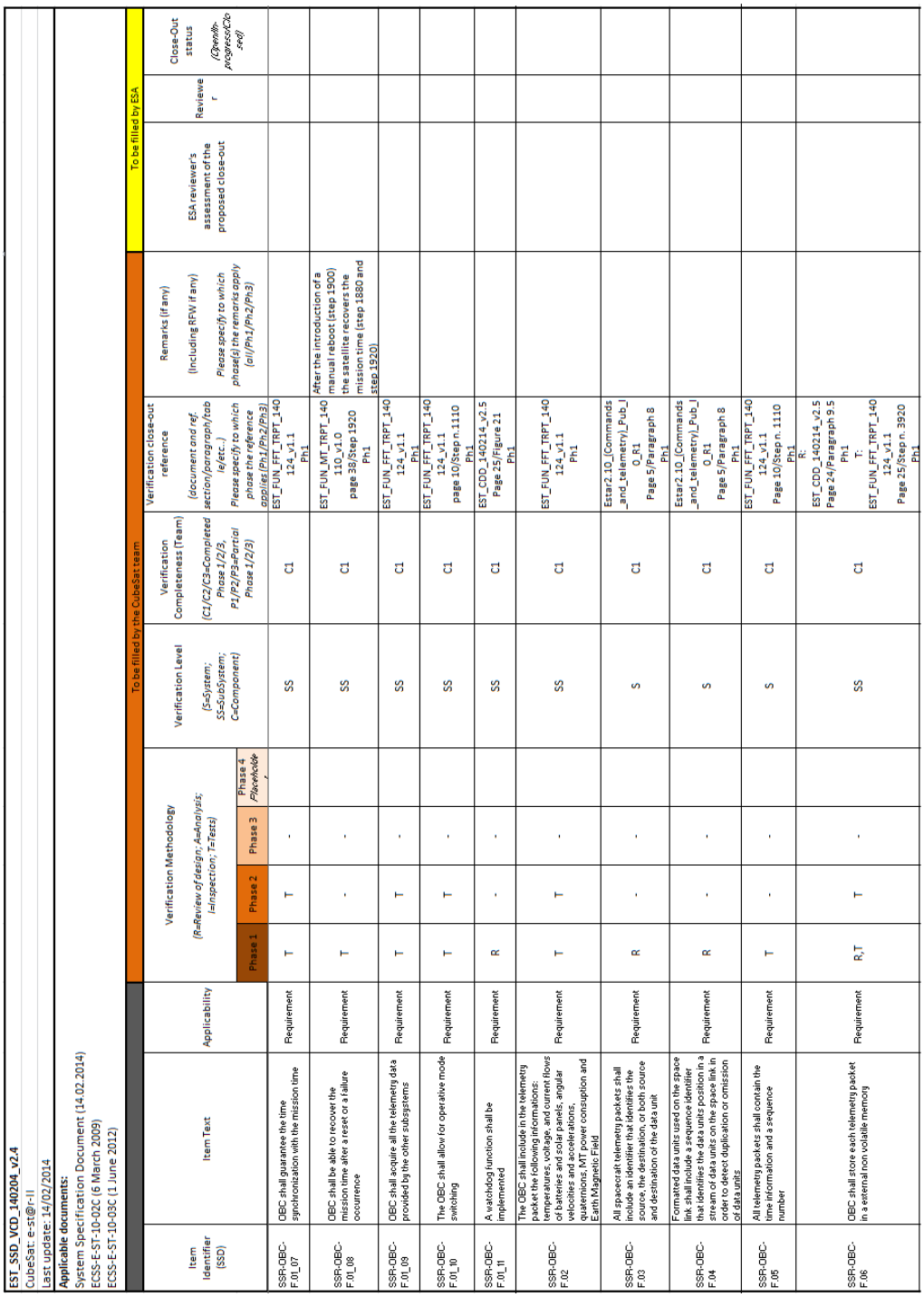
A large number of requirements have been verified within a single run demonstrating the capabilities both of the satellite (except for ADCS) and of the MGCS hardware and software involved in this test. The ADCS functions and related capabilities are not verified because only the basic mode of operations has been considered in this test. It also means that no transitions between modes of operations have been tested. Moreover, the commands that foresee the involvement of this subsystem have not been taken into account. In conclusion, the BFT has been a complete success because all the basic functionalities of the satellite are verified and no relevant failures occurred. No open issues remain at the end of the test.

The full functional test has been correctly conducted and all requirements were met. The verifications close-out were detailed in the verification reports and the verification matrix were filled with the reference of the documents were each requirement verification is reported. A partial verification matrix is shown in Table 14.

It has been shown that the satellite is able to perform properly and contemporaneously all functions and tasks as well as the on-orbit operations. Moreover it is able to transit from a mode of operation to another and to work properly in any mode of operation. During the test, the transition from and to Fail Safe Mode (i.e., mode in which communication between OBC and COMSYS fails) were not tested because it was not possible to perform a failure injection in the communication between both subsystems. A minor anomaly came up: the transponder signal (i.e., automatic transmission from the CubeSat that confirms the validation of the received telecommand) for the transition from Silent Mode (i.e., downlink communication is stopped) and Full Mission B Mode (i.e., all subsystems switched-on and ADCS performing attitude control) has not been received by the MGCS. Anyhow, the command was correctly validated and executed on board by the OBC even if the transponder were not sent. The

rationale that justifies this fault states in the contemporary occurrence of transponder and telemetry packet transmission where only the later were performed by the COMSYS.

Table 14: e-st@r-II verification matrix (partial)



EST_SSD_VCD_140204_v2.4
CubeSat: e-st@r-II
Last update: 14/02/2014
Applicable documents:
System Specification Document (14.02.2014)
ECSS-E-ST-10-02C (6 March 2009)
ECSS-E-ST-10-03C (1 June 2012)

			To be filled by the CubeSat team									To be filled by ESA		
Item Identifier (SSD)	Item Text	Applicability	Verification Methodology (R=Review of design; A=Analysis; I=Inspection; T=Tests) Phase 1	Phase 2	Phase 3	Phase 4 /Pack+Ade	Verification Level (S=System; SS=Subsystem; C=Component)	Verification Completeness (Team) (C1/C2/C3=Completed Phase 1/2/3, P1/P2/P3=Partial Phase 1/2/3)	Verification close-out reference (document and ref. section/paragraph/table/etc...) Please specify to which phase the reference applies (Ph1/Ph2/Ph3)	Remarks (if any) (Including RFW if any) Please specify to which phase(s) the remarks apply (all/Ph1/Ph2/Ph3)	ESA reviewer's assessment of the proposed close-out	Reviewer	Close-Out status (Open/In-progress/Closed)
SSR-OBC-F.01_07	OBC shall guarantee the time synchronization with the mission time	Requirement	T	T	-		SS	C1	EST_FUN_FFT_TRPT_140124_v1.1 Ph1				
SSR-OBC-F.01_08	OBC shall be able to recover the mission time after a reset or a failure occurrence	Requirement	T	-	-		SS	C1	EST_FUN_MT_TRPT_140110_v1.0 page 38/Step 1920 Ph1	After the introduction of a manual reboot (step 1900) the satellite recovers the mission time (step 1880 and step 1920)			
SSR-OBC-F.01_09	OBC shall acquire all the telemetry data provided by the other subsystems	Requirement	T	T	-		SS	C1	EST_FUN_FFT_TRPT_140124_v1.1 Ph1				
SSR-OBC-F.01_10	The OBC shall allow for operative mode switching	Requirement	T	T	-		SS	C1	EST_FUN_FFT_TRPT_140124_v1.1 page 10/Step n.1110 Ph1				
SSR-OBC-F.01_11	A watchdog function shall be implemented	Requirement	R	-	-		SS	C1	EST_CDD_140214_v2.5 Page 15/Figure 21 Ph1				
SSR-OBC-F.02	The OBC shall include in the telemetry packet the following information: temperature, voltage, and current flows of batteries and solar panels; angular velocities and accelerations; quaternions; MT power consuption and Earth Magnetic Field	Requirement	T	T	-		SS	C1	EST_FUN_FFT_TRPT_140124_v1.1 Ph1				
SSR-OBC-F.03	All spacecraft telemetry packets shall include an identifier that identifies the source, the destination, or both source and destination of the data unit	Requirement	R	-	-		S	C1	Estar2.10_[Commands_and_telemetry]_Pub_I0_R1 Page 5/Paragraph 8 Ph1				
SSR-OBC-F.04	Formatted data units used on the space link shall include a sequence identifier that identifies the data units position in a stream of data units on the space link in order to detect duplication or omission of data units	Requirement	R	-	-		S	C1	Estar2.10_[Commands_and_telemetry]_Pub_I0_R1 Page 5/Paragraph 8 Ph1				
SSR-OBC-F.05	All telemetry packets shall contain the time information and a sequence number	Requirement	T	-	-		S	C1	EST_FUN_FFT_TRPT_140124_v1.1 Page 10/Step n. 1110 Ph1				
SSR-OBC-F.06	OBC shall store each telemetry packet in a external non volatile memory	Requirement	R,T	T	-		SS	C1	EST_CDD_140214_v2.5 Page 24/Paragraph 9.5 Ph1 T: EST_FUN_FFT_TRPT_140124_v1.1 Page 25/Step n. 3920 Ph1				

As far as mission test regards, it has been carried out without relevant observed faults, showing that the satellite is able to perform properly the designed basic, full and off-nominal on-orbit operations. The foreseen mission profile has been conducted with success: telemetry packets did not report corrupted values, telemetry data always remained within the expected ranges for the proposed mission profile, and the required commands were executed by the satellite without misbehaviour. Two minor faults have been observed: first of all, two OBC software reboots occurred during the test; this is a non-nominal behaviour that actually is negligible and does not impact the on-orbit mission. Secondly, after the transmission of the command to activate the payload, the first received telemetry packet does not show the correct ADCS values: from previous tests it has been verified that usually ADCS telemetry updates on the second/third packet after command execution. This behaviour is typical of the nominal ADCS-OBC software communication and operation, and it does not represent and issue at the end.

The results of the functional tests clearly show the verification of all functional requirements and demonstrated the ability of the satellite to conduct the designed mission, increasing its reliability. Moreover, key-issues have been identified being highly useful for future real on-orbit operations. In particular, unexpected errors on received telemetry have been identified and they will be taken into account for the on-orbit operations planning and execution.

At the time where this PhD thesis has been written, only quasi-static loads and natural frequencies analysis has been conducted from the all envisaged environmental verifications due to some delays mainly on the availability of test facilities at ESA/ESTEC and delays on the first phase of the project (i.e. functional verifications at ambient condition). The environmental tests are envisaged to be conducted during the first quarter of 2015 but no exact date has been already established. The results of the mechanical analysis shows that the satellite is able to withstand the quasi-static loads, identifying a sufficient margin of safety (i.e. 2.15). Moreover, the modal analysis individuated the first natural mode of vibration at 210 Hz approx.. which is higher than the requirement of a minimum natural frequency of 120 Hz.

8

MISSION-ORIENTED RELIABILITY

One way to overcome the relative reduced CubeSats reliability is to focus the attention to mission objectives and mission reliability. The proposed approach is based on the fault tolerance techniques. In the origin of reliability, these techniques were applied to outdo the relative low reliability of systems components. Indeed, redundancies at subsystem level were applied to increase the reliability of the whole system without improving components.

Increasing reliability at system level by only means of applying fault prevention and removal techniques could lead to a boost on project cost. The design complexity and time-consuming (and hence costly) verification activities can be prohibitive for most of CubeSat projects. A good compromise between cost and reliability is to partially increase this dependability attributes at system level and partially at mission level, to achieve a good confidence that mission success will be reached. The former point has been addressed in the previous two sections. The latter is evaluated in this section. Different ways to achieve desired reliability at mission level that could assure the accomplishment of mission objectives are stated in the present chapter.

8 MISSION-ORIENTED RELIABILITY

8.1 Space segment architecture

The reliability of the mission depends on reliability of different mission architecture elements (mainly satellite but also launcher, ground segment, mission operations, etc.). Selection of appropriate launcher is driven, not only by technical requirements, but also political and economic aspects are taken into account. Anyway, it is not possible, from the mission point of view, to act on the reliability on the launch element and ground segment. Hence, it has been assumed that activities on ground segment are conducted perfectly and the launcher operates properly inserting satellite(s) in the desired orbit(s). Therefore, it has been only taken into account satellite(s) reliability as main parameter of mission reliability.

The idea proposed is to achieve acceptable mission reliability by implementing different mission architectures. Traditionally, most of unmanned space missions have been conducted by monolithic multi-objective conventional satellites, as detailed in chapter 2. New mission architectures are being developed as a complement of classical missions or to achieve mission objectives at lower cost. For example, a constellation of CubeSats for Earth observation could maximise coverage with respect to a monolithic architecture.

8.1.1 Swarm-like constellation

Swarm-like constellation is studied as a solution to increment reliability at mission level. The study foresees the deployment of a swarm-like constellation formed by different number of CubeSats. The reliability of the mission as dependable of each satellite is evaluated and compared with reliability of monolithic architecture composed by a conventional satellite. It is also considered the effect of losing some satellites in the constellation.

The like-swarm constellation can be modelled as a parallel system of identical CubeSats, as depicted in Figure 55.

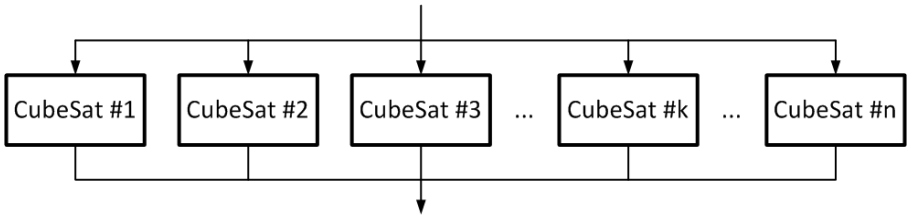


Figure 55: Swarm-like constellation block diagram as parallel system of identical CubeSats

All CubeSats in the constellation are assumed to be identical, as stated above, and have independent life distributions. Moreover, the state of the CubeSats are considered binary i.e., operational or non-operational. In this case, the reliability of the system (i.e. swarm-like constellation of CubeSats) is the probability that any one satellite is operational. In particular, the reliability of the system is:

$$R = 1 - (1 - p)^n \tag{8.1}$$

Where *p* is the probability that a satellite is operational.

However, for the present study it is not necessary true that only one operational CubeSat is enough to accomplish the mission. Then, it is necessary to evaluate the reliability of the system as the probability that *k* CubeSats are operational. Generally speaking, these types of systems are known as *k-out-of-n systems*. In this case, the system (i.e. the constellation) fails when *k+1* components (i.e. CubeSats) fail.

For these systems, taking into account again that all units have identical and independent life distributions and the probability that a unit is functioning is *p*, then the probability of having exactly *k* functioning units out of *n* is:

$$P_{(k;n,p)} = \binom{n}{k} p^k (1 - p)^{n-k} \qquad k = 0,1, \dots, n \tag{8.2}$$

The system is functioning properly if *k* or *k+1* or … or *n-1* or *n* units are functioning. Therefore, the reliability of the system is:

$$R_{(k;n,p)} = \sum_{r=k}^{n} \binom{n}{r} p^r (1 - p)^{n-r} \tag{8.3}$$

8.2 Swarm-like constellation vs. monolithic architectures

The comparison between these two architectures is conducted in terms of reliability and mean-time-to-failure. The observed reliability of conventional satellites is obtained from literature, as specified in section 4.5. The first step is to assess the reliability of the swarm-like constellation for different values of *k*. The first objective is to identify the value of *k* for which the reliability of the constellation after two years (as a reference mission time) is similar to the reliability of a mission conducted with a monolithic conventional satellite.

In chapter 4.4.2 it has been demonstrated that the observed CubeSats reliability follows Weibull distribution. The reliability expression as well as two Weibull parameters for CubeSats and all-satellites are:

Table 15: Reliability expression for Weibull distribution and parameters for CubeSats and all-satellites

Reliability expression for Weibull distribution		
$R = e^{-(t/\theta)^{\gamma}}$		
	Shape parameter γ [dimensionless]	**Characteristics life θ [years]**
CubeSats	0.2853	6619.4
All-satellites	0.3875	8316

Substituting the both shape parameter and characteristic life for all-satellites in the reliability expression for Weibull distribution, for *t=2 years*, the reliability of *R=0.9612*. To calculate the value of *k*, a constellation of 20 CubeSats is assumed (i.e., m=20). A MatLab® script has been developed to evaluate *k*. The comparison of reliability among a monolithic architecture (with a CubeSat and a conventional satellite) and a CubeSats constellation is shown in Figure 56.

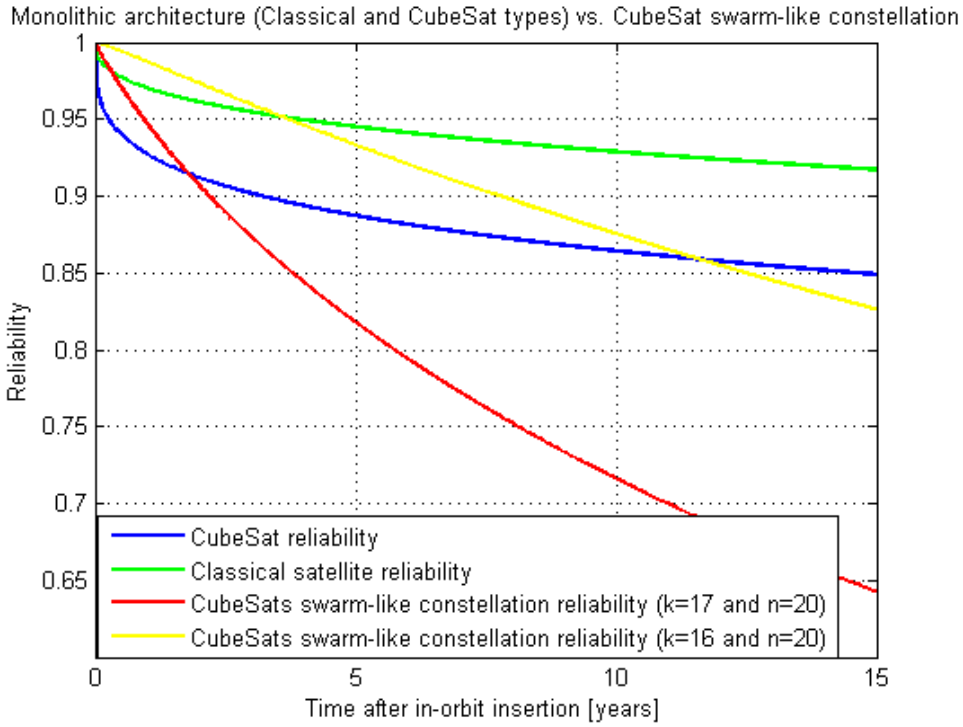


Figure 56: Reliability comparison between different mission architectures

Assuming a constellation of 20 identical CubeSats, with the requirement of a minimum of 16 operative spacecraft to accomplish the mission, the obtained reliability is higher than a monolithic architecture of a conventional satellite after 3.59 years after launch. Before this time, the constellation has a higher reliability with respect to monolithic architecture, while after 3.59 years, the latter is characterised by a higher reliability with respect to the former. Hence, it has been demonstrated, in a preliminary analysis, that it is possible to achieve higher mission reliability with a constellation of CubeSats than with a monolithic classical satellite.

Then, it is possible to evaluate the MTTF when *k* changes from 1 to 20. The obtained value indicates the time at which it is expected to lose the capabilities to completely achieve all mission objectives because minimum number of required satellites are not operational due to failures. Thus, on the basis of this value, it should be possible to establish a precise maintainability plan which can consist of a substitution of failed CubeSats inserting new once on orbit. Assuming, as previously, a constellation with initially 20 operative CubeSats (i.e., n=20), the variation of MTTF with respect to *k* is shown in Figure 57.

8 MISSION-ORIENTED RELIABILITY

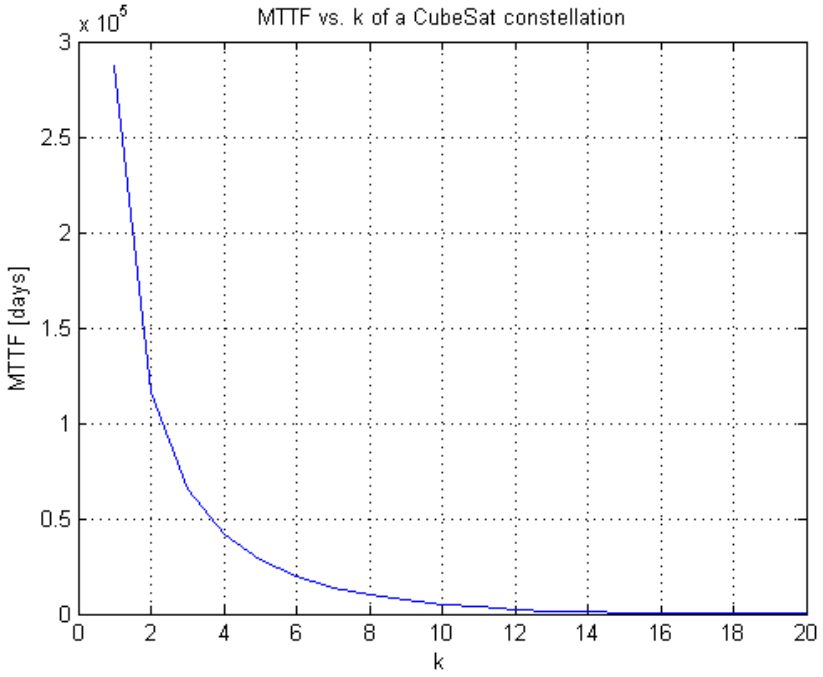


Figure 57: MTTF variation of a 20 CubeSats constellation with respect to *k*

The obtained result confirms the expected output, i.e., maintaining the number of CubeSats on the constellation constant, the higher is the number of required operational satellites to conduct the mission, the lower is the MTTF. It is clear that, for a constellation of 20 CubeSats, if only 1 is required to be operational in order to achieve the mission objectives, the MTTF is unrealistically high (precisely, 787 years). Obviously, a constellation of 20 CubeSats will not be deployed if only 1 satellite is required to accomplish the mission. Focusing the attention to a more realistic cases, for k=15, the expected MTTF is two years. Taking into account these results, different mission configurations shall be evaluated. For example, a mission of 4 years could be accomplished with a constellation of n=20 CubeSats with k=15, and replacing the failed after 2 years.

8.3 Case study: HumSat/GEOID constellation

A real project, called HumSat/GEOID constellation, has been adopted as case study to apply the previous identified method to increase reliability at mission level. As part of this project, the CubeSat Team is developing 3STAR, a 3U CubeSat to be inserted into orbit in order to be one of the space segment elements of the constellation.

8.3.1 3STAR

3STAR CubeSat is a project contained in the e-st@r program. It is the third CubeSat developed by the CubeSat Team, which also has educational and technological objectives. Besides the HumSat/GEOID payload, which is a communication subsystem to provide telecommunications services in support to humanitarian and emergency applications, 3STAR has a remote sensing payload. In particular, P-GRESSION multi-purpose payload under development at Politecnico di Torino will be installed in the satellite to perform different remote sensing techniques for Earth observation, atmosphere profiling for climate studies, and eventually warning services.

At the present, 3STAR project is under development at STARLab. In particular, the project is in the phase B of the life-cycle and the first prototypes of the subsystems will be developed in the next months.

8.3.2 HumSat project

HumSat (Humanitarian Satellite) Network project goal is the development of a nano-satellite constellation and its corresponding ground segments (shown in Figure 58) to provide support for humanitarian initiatives, especially in developing areas. Moreover, the project will provide educational hands-on practice to university students boosting cooperation between universities from different countries. HumSat project has been endorsed by European Space Agency, United Nations through the Office for Outer Space Affairs (UNOOSA), University of Vigo (Spain), California Polytechnic University (USA) and Autonomous National University of Mexico and CRECTEALC (Mexico).

8 MISSION-ORIENTED RELIABILITY

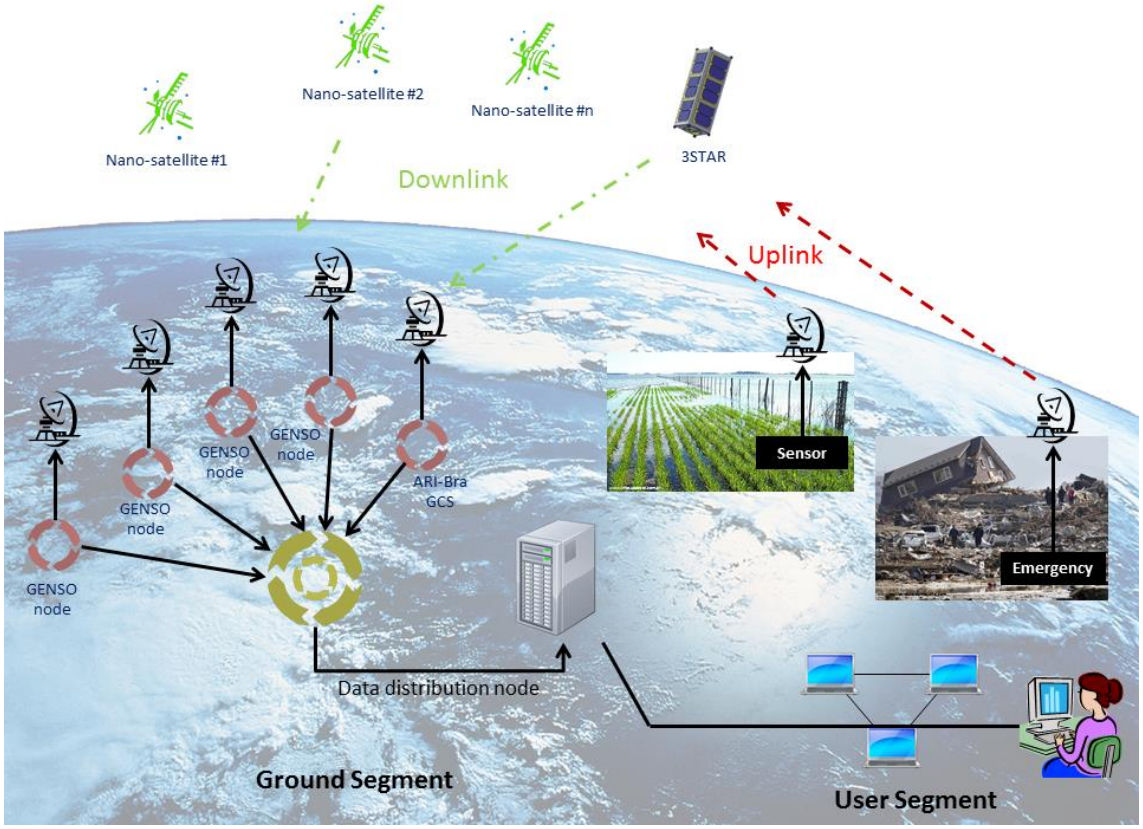


Figure 58: HumSat/GEOID network

Going in detail on the network architecture, the *space segment* is composed by different number of nano-satellites (including CubeSats) where 3STAR CubeSat will be inserted. The satellites will gather information from on-ground sensors placed all around the World. These sensors, freely deployed and developed by users of the network, are the *user segment*. All this information will be then transmitted and collected on the ground segment elements. The *ground segment* is formed by different nodes (i.e. ground control stations); each of one is part of the GENSO network. Each node will be also used to communicate and control the satellites. A Centralised HumSat Control Facilities collects the data from all nodes and stores them for retrieval by the users. It also implements the necessary mechanisms to provide confidentiality to users' data.

8.3.3 GEOID

GEOID, which stands for GENSO Experimental Orbital Initial Demonstration, is a project that will act as a primary tool for the large-scale validation of the GENSO network. The GENSO (Global Educational Network for Satellite Operations) network aims to increase the return from educational space missions by forming a worldwide network of ground stations and spacecraft which can interact via a software standard. GEOID initiative is considered as the ESA contribution to the HumSat project being the communications backbone and test-bed for the initial version of the HumSat system.

8.3.4 HumSat/GEOID constellation mission-oriented reliability

Ridolfi et al. utilised the HumSat/GEOID project as a key study to set up an optimisation process aimed at determining the best configurations of a swarm-like constellation of CubeSats. That study foresaw the deployment of a constellation formed by nano-satellites and ground stations to provide communication services between different locations on Earth with a store-and-forward architecture. Different number of CubeSats have been considered for the study. The authors established the optimum number of CubeSats to guarantee certain global coverage and constellation cost. The objective of the present key study is to add a figure-of-merit with respect to reliability, and validate the results obtained by Ridolfi et al. or propose different possible solutions to maximise mission reliability.

Different architectures have been considered the previous mentioned study. In particular, they are:

- 7 CubeSats in one orbital plane
- 8 CubeSats in one orbital plane
- 9 CubeSats in three orbital planes
- 12 CubeSats in three orbital planes

First approach takes into account the number of CubeSats. The target objective, as considered before, is to have a mission reliability equal or higher than those of a monolithic

architecture with conventional satellite after 2 years from the deployment of the satellites (i.e., R=0.9612). The script used in section 0 is used to determine the value of *k* for each architecture that assures an equal or higher mission reliability of 0.9612 after two years. The obtained results are the summarised in Table 16.

Table 16: *k*, n and $R_{(t=2\ years)}$ for different mission architectures

Nº of CubeSats (n)	k	$R_{(t=2\ years)}$
7	5	0.9818
8	6	0.9727
9	7	0.9618
12	9	0.9833

The results highlight that the higher is the number of CubeSats in the studied architecture (i.e., n), the higher is the difference between *n* and *k* to obtain a similar reliability of monolithic architecture with a classical satellite. A comparison of the previous architectures reliability is given in Figure 59.

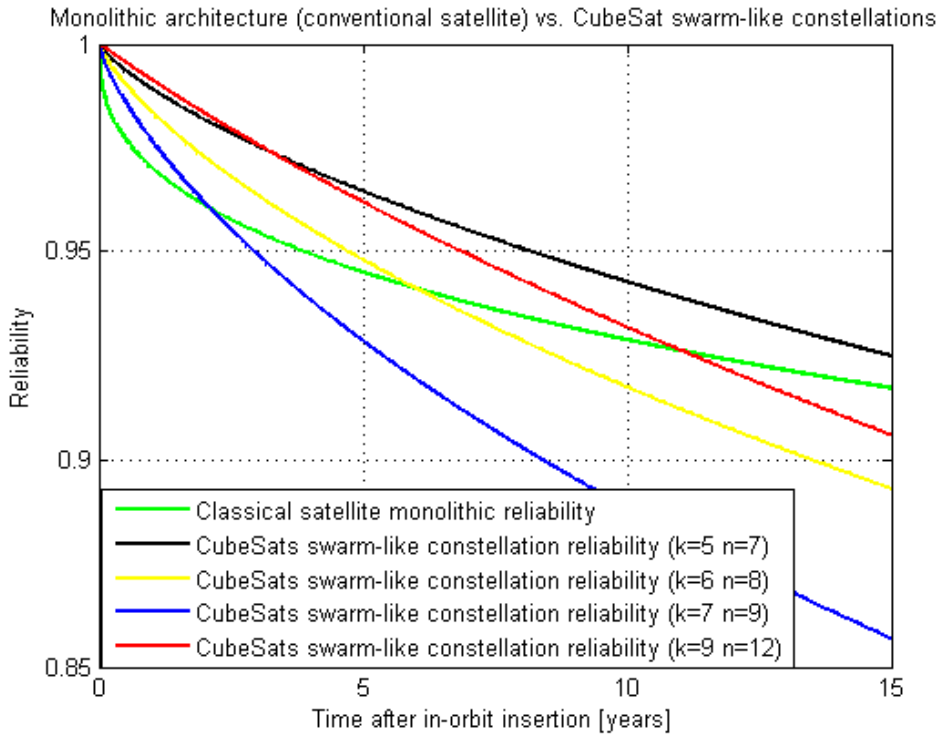


Figure 59: Reliability of CubeSats constellation for different n and k vs. monolithic architecture with conventional satellite

8.3 Case study: HumSat/GEOID constellation

Previous graphic stresses that the increase of CubeSats does not entail higher mission reliability during the whole mission. For the first two years after insertion into orbit, a constellation of 12 CubeSats guarantee the highest reliability of all architectures taken into account. However, after approximately three and a half years a constellation of 7 CubeSat with 5 operational spacecraft guarantees the highest reliability. Therefore, taking only into account the reliability, the best architecture for the first two years of mission is a 12 CubeSats with a requirement of minimum 9 operational. Nevertheless, the reliability difference during first two years of mission of the best two architectures is relatively low ($\Delta R=0.0022$). Thus, a different approach could be established: insert 12 CubeSats on-orbit but with the need of use 7 of them, and 5 as a back-up.

9

CONCLUSIONS

This PhD thesis explored the dependability of small-satellites and their missions, focusing the attention on CubeSats. The concrete research aims at filling the existent gap on literature about CubeSats failures and to explore possible methods to increase their dependability by means of improving their attributes.

The use of CubeSats, a satellite standard defined on its basic unit as a cube of 10cm side and maximum 1.33Kg, experienced a boost in the last decade. Mainly designed and developed in the university field, the use of this type of satellites for more-than-educational purposes is being increased in the last years. However, it is a common feeling in the CubeSat community that high number of this satellites failed once on-orbit. The research confirmed that more than 50% of the CubeSats failed after their insertion on-orbit, mainly due to lack of communications or problems with electrical power system. However, it could not be possible to identify the root cause of failures, mainly due to lack of information from CubeSats developers. Anyhow, the number of failures was available, and by means of non-parametric and parametric analysis has been demonstrated that CubeSats' failures follow a Weibull distribution, characterised by a high infant mortality.

A comparison between traditional space projects and CubeSats projects has been conducted. The former are characterised to accept low risk and consequently increase reliability through design and verifications complexity as well as mass and cost increase; the later usually accept high risk with low design and verifications complexity that lead to a mass and cost reduction. From this analysis it has been identified three key methods to increase CubeSats and CubeSats missions' reliability: 1) good practices to be conducted during all phases of satellites life-cycle, 2) reliability increase through verification, and 3) reliability increase at mission level.

9 CONCLUSIONS

The first method is based on applying good practices during all CubeSat life-cycle phases in order to increase the mission rate of success. An evaluation of activities conducted by CubeSat developers has been conducted through a questionnaire sent to all developers. The received answers have been used to state the good practices that will help future CubeSat developers to improve their projects.

Secondly, tailoring international standards has been a key-activity to establish a precise and systematic methodology for verification planning and execution of CubeSat. Following the proposed methodology gives to CubeSat developers the opportunity to conduct verification activities in an optimized way with respect to ECSS, allowing them to focus the attention on key-aspects like functional and concrete environmental verifications. The execution of these verifications leads to conduction of reduced cost and time-saving verification campaign.

This second method has been applied to e-st@r-II CubeSat. It has been demonstrated that the methodology perfectly fits a CubeSat project requirements in terms of cost, time and human-resources requirement. The execution of the planned verifications led to the verification of functional requirements of the satellite, increasing its reliability and the confidence of its ability to conduct the designed mission. Environmental verifications will allow to also increase both reliability and expected mission success. However, at the date these verifications could not be conducted due to management delays on ESA/ESTEC facilities side. It is expected that they will be carried out during first quarter 2015.

Finally, the characteristics of CubeSat projects allow the development of different mission architectures (e.g. swarm-like constellations) with respect to traditional monolithic architectures. This new concepts allow to define an alternative way to increase the reliability, at mission level instead of system level. Assuming that CubeSats reliability follows a Weibull distribution (as already verified), it has been demonstrated that it is possible to obtain a higher reliability at mission level for a CubeSats swarm-like constellation with respect to a classical monolithic satellite, even if single CubeSat reliability is lower than traditional satellite.

This study has been applied to 3STAR CubeSat, which is being developed at Politecnico di Torino within HumSat/GEOID program. The method demonstrated that a satellite constellation

of 12 CubeSats with a minimum of 9 operating is characterised by a higher reliability than a traditional satellite after 10 years of insertion into orbit.

In conclusion, it has been proven that the three proposed methods are effective to increase the CubeSats reliability and their mission rate of success. Moreover, with this research a useful guidelines for design, development, verify and operate a CubeSat has been supplied to all CubeSat community. Finally, as a main part of the research, it has been demonstrated that improving the verification activity is a key factor for the development of CubeSats, and leads to higher confidence in the success of CubeSats missions.

REFERENCES

Avižienis A., *The four-universe information system model for the study of fault—tolerance*, In: Proceedings of the 12th Annual International Symposium on Fault-Tolerant Computing, FTCS'82, IEEE Press, pp. 6-13 (1982)

Castet J-F., Saleh J.H., *Satellite Reliability: Statistical Data Analysis and Modeling*, Journal of Spacecraft and Rockets, Vol. 46, No.5, September-October 2009, DOI: 10.2514/1.42243

Castet J-F., Saleh J.H., *Satellite and satellite subsystems reliability: statistical data analysis and modelling*, In: Reliability Engineering and System Safety 2009; 94(11), 1718-1728

Chiesa S., *Affidabilità, sicurezza e manutenzione nel progetto dei sistemi – nuova edizione*, C.L.U.T. Editrice, 2010, ISBN: 978-88-7992-264-7

Dubos G. F., Castet J-F., Saleh J.H., *Statistical reliability analysis of satellites by mass category: Does spacecraft size matter?*, In: Acta Astronautica, Vol. 67, 2010, 584-595

Dubrova E., *Fault-Tolerant Design*, Springer Ed., 2013, ISBC: 978-1-4614-2112-27

ECSS-E-ST-10-02C (6 March 2009) – Space engineering – Verification

ECSS-E-ST-10-03C (1 June 2012) – Space engineering – Testing

ECSS-M-ST-40C_Rev.1(6 March 2009) – Space Project Management – Configuration and information management

ECSS-Q-ST-10C (15 November 2008) – Space Product Assurance – Product Assurance Management

ECSS-S-ST-00C (31 July 2008) – ECSS system – Description, implementation and general requirements

Elsayed E.A., *Reliability engineering*, 2nd ed., United States of America, A Willey publication, 2012, ISBN: 978-1-118-13719-2

REFERENCES

Ericson II, C.A., *Hazard Analysis Techniques for System Safety*, Wiley publication, 2005, ISBN: 978-0-471-72019-5

Fortescue P., Stark. J., Graham S., *Space Systems Engineering*, 3rd ed., Cornwall, United Kingdom, Willey publication, 2003, ISBN: 0-471-61951-5

Kaplan E.L., Meier P., *Nonparametric estimation from incomplete observation*, Journal of the American Statistical Association, Vol. 53, No. 282, June 1958, pp. 457-481

Laprie J.-C., *Dependability: Basic Concpets and Terminology*, Springer-Verlag, 1992

Laprie J.-C., *Dependable computing and fault tolerance: concepts and terminology*, In: 15th IEEE International Symposium on Fault-Tolerant Computing (FTCS-15), Ann Arbor, USA, June 1985, pp. 2-11

Lawless J.F., *Statistical Models and Methods for Lifetime Data*, 2nd ed., United States of America, A Willey-Interscience publication, 2003, ISBN: 0-471-37215-3

Meeker W.Q., Escobar L.A*., Statistical Methods for Reliability Data*, 1 ed., United States of America, A Wiley-Interscience publication, 1998, ISBN: 0-471-14328-6

National Aeronautics and Space Agency, *NASA Systems Engineering Handbook, NASA/SP-2007-6105, Rev.1*, December 2007

O'Connor P.D.T., *Practical Reliability Engineering*, 4th ed., Chippenham, Wiltshire, United Kingdom, Wiley publication, 2008, ISBN: 978-0-470-84462-5

Obiols-Rabasa G., Corpino S., Mozzillo R., Nichele F., *e-st@r-II experience: valuable knowledge for the e-st@r-I design*, In: 65th International Astronautical Congress, Toronto, Canada, 29 September – 03 October 2014

Obiols-Rabasa G., Corpino S., Nichele F., Ridolfi G., Stesina F., Viola N., *3-STAR Program at Politecnico di Torino*, In: Small Satellite, Services and Systems – the 4S Symposium, Portoroz, Slovenia, 4-8 June 2012

Rajan A., Whal Th., *Cost-efficient Methods and Processes for Safety-relevant Embedded Systems*, 1st ed., Wien, Wiley publication, 2013, USBN:978-3-7091-1386-8

REFERENCES

Ridolfi G., Corpino S., Stesina F., Notarpietro R., Cucca M., Nichele F., *Constellation of CubeSats: 3-STAR in the HumSat/GEOID mission*, 62nd International Astronautical Congress, Cape Town (South Africa), 2011

Saleh J.H., Castet J-F., *Spacecraft Reliability and Multi-State Failures*, 1st ed., Chichester, West Sussex, United Kingdom, Wiley publication, 2011, ISBC: 978-0-470-68791—8

Sandau R., *Status and trends of small satellite missions for Earth observation*, In: Acta Astronautica, Vol. 66, 2010, 1-12

Science and Engineering, Systems Analysis and Integration Laboratory, Systems Integration Division, Systems Verification Branch, George C. Marshal Space Flight Center, NASA, *Verification Handbook – Volume I: Verification Process, MFSC-HDBK-2221*, MSFC, Alabama, 1994

Tumer I.Y., *Design methods and practices for fault prevention and management in spacecraft*, Technical Report, 20060022566, NASA (2005)

USA Army, *Failure modes, effects and criticality analyses (FMECA) for command, control, communications, computer, intelligence, surveillance, and reconnaissance (C4ISR) facilities*, Technical Manual No. 5-698-4, Washington DC., 29 September 2006

Yu W.D., *A software fault prevention approach in coding and root cause analysis*, Bell Labs Tech. J. 3(2),3-21 (1998)

APPENDIX A

Newton-Raphson Method

The Newton-Raphson Method is used for solving nonlinear equations iteratively based on the idea of linear approximation. Let $f_{(r)}$ be a well-behaved function, let *r* be a root of the equation $f_{(r)} = 0$, and x_0 be a good estimate of *r*. The function $f_{(x)}$ is then expanded using Taylor series:

$$f_{(r)} = f_{(x_0)} + (r - x_0)f'_{(x_0)} + \frac{(r - x_0)^2}{2!}f''_{(x_0)} + \cdots \tag{B.1}$$

Being x_0 a good estimate of *r*, then $r = x_0 + h$. Hence, $h = r - x_0$, being h relatively small due to the fact that x_0 is a good estimate of *r*. Thus, the previous polynomial of degree infinity equation (B.1) can be solved taking only the first two terms of the right-hand side:

$$0 = f_{(r)} = f_{(x_o+h)} \approx f_{(x_0)} + hf'_{(x_0)} \tag{B.2}$$

Hence, *h* and *r* expressions are:

$$h \approx -\frac{f_{(x_0)}}{f'_{(x_0)}} \tag{B.3}$$

$$r = x_0 + h \approx x_0 - \frac{f_{(x_0)}}{f'_{(x_0)}} \tag{B.4}$$

Hence, placing x_1 as the improved estimate of the root *r*, the following expression is obtained:

$$x_1 = x_0 - \frac{f_{(x_0)}}{f'_{(x_0)}} \tag{B.5}$$

x_1 is then used in lieu of x_0 in eq. (B.5) to obtain a better estimate of the root. The process is then iteratively repeated until the difference between two consecutive estimates of the root is acceptable (i.e., under a certain threshold). The general expression for the Newton-Raphson Method is the following:

$$x_{n+1} = x_n - \frac{f_{(x_n)}}{f'_{(x_n)}} \tag{B.6}$$

The steps are summarised as follow:

1. Determine an initial estimate $\hat{x}_0$of *r*, such as $f_{(\hat{x}_0)} \cong 0$
2. Calculate the second estimate $\hat{x}_{k+1} = \hat{x}_k - \frac{f_{(\hat{x}_k)}}{f'_{(\hat{x}_k)}}$ (i.e. k=0, k+1=1 for the first iteration)
3. If $|d| = \hat{x}_k - \hat{x}_{k+1} \geq \varepsilon$, being ε a chosen threshold, increase k (i.e. k=k+1) and proceed from point 2 again. If $|d| = \hat{x}_k - \hat{x}_{k+1} \leq \varepsilon$, a root value is obtained

APPENDIX B

CubeSats Questionnaire

GENERAL INFORMATION

1. Institution

2. Satellite name

3. CubeSat type (Select one option)
○ 1U ○ 1.5U ○ 2U ○ 3U

4. Objectives of the project
Objective #1
Objective #2
Objective #3

5. Participants to the project (%)
(a) Undergraduate students
(b) Graduate students

APPENDIX B – Cubesat Questionnaire

(c) PhD students
(d) Professors
(e) Industry professionals
(f) Others

6. Total funding level of the project (please specify currency)

7. Launch and orbit specifications
(a) Date of launch [dd/mm/yyyy]
(b) Launch site
(c) Launcher
(d) Orbit inclination [deg]
(e) Perigee [Km]
(g) Apogee [Km]

8. Actual status of the satellite (Select one option)
○ Active ○ Non active ○ Deorbited ○ CubeSat launched to the ISS but not yet deployed

9. Please, provide a brief description of the mission

CUBESAT DESIGN

10. Model philosophy adopted (Select one option)
○ Prototype ○ Protoflight ○ Hybrid

11. Has some standard been followed? (Select one option)
○ Yes ○ No

12. If in the previous question you answered yes, please specify what standard you followed

13. Have you performed some reliability analysis from the very early development phases to improve robustness of the CubeSat? (e.g. FMECA, etc.) (Select one option)
○ Yes ○ No

14. If in the previous question you answered yes, please specify the methods used to evaluate the CubeSat reliability

APPENDIX B – Cubesat Questionnaire

What of the following models have you build? Please, specify also if they are mathematical/virtual model(s) and/or hardware model(s)

15. Type of model

	Mathematical/Virtual	Hardware
(a) CAD model (only Mathematical/Virtual selection is possible for this model)	☐	☐
(b) Electrical model	☐	☐
(c) Structural model	☐	☐
(d) Thermal model	☐	☐
(e) Engineering model	☐	☐
(f) Engineering Qualification model	☐	☐
(g) Qualification model	☐	☐
(h) Flight model	☐	☐
(i) Protoflight model	☐	☐

16. Has any software model of the subsystems been established in order to analyse by simulation the behaviour of each of them? (Select one option)

○ Yes ○ No

17. If in the previous question you answered yes, please specify which subsystem(s) has(ve) been modelled

☐ EPS
☐ ADCS
☐ COM
☐ OBDH
☐ Thermal
☐ Mechanisms
☐ Payload
☐ Other (please specify)

18. Has a software simulation of the entire system functionality been performed to improve the CubeSat design before starting the hardware manufacturing? (Select one option)
○ Yes ○ No

19. Have HiRel components been used? (Select one option)
○ Yes ○ No

20. If you answered yes in the previous question, please specify what components are HiRel

21. Have tests been performed at equipment level? (either on self-developed or acquired equipment) (Select one option)
○ Yes ○ No

22. If in the previous question you answered yes, please specify on what components/equipment you conducted the following tests
(a) Functional tests
(b) Mechanical tests
(c) Thermal test
(d) Radiation test

23. Has any type of redundancy been foreseen in the design of the satellite? If yes, please specify (Select one option)
○ Yes ○ No
CUBESAT HANDLING

APPENDIX B – Cubesat Questionnaire

24. Has it been necessary to transport the CubeSat among different facilities? (e.g. to perform the tests, to integrate it into the CubeSat deployer, etc.) (Select one option)
○ Yes ○ No

25. If in the previous question you answered yes, what of the following considerations have been taken into account?
☐ Protection against shocks
☐ Control of humidity
☐ Control of contamination
☐ Other (please specify):

CUBESAT VERIFICATION PREPARATION

26. Has an AIV plan been established for the project? (Select one option)

○ Yes ○ No

27. Were test specifications and written step-by-step procedures prepared for each test? (Select one option)

○ Yes ○ No

28. If step-by-step test procedures were prepared, did they include the nominally expected system response to each test step? (Select one option)

○ Yes ○ No

Please, specify the position and the number of sensors which have been placed for the following tests (if performed). If no sensors have been utilised in some position, leave the space empty

	29. External part of the CubeSat	30. Internal part of the CubeSat	31. On the shaker plate (only for mechanical tests)	32. On the CubeSat deployer (only for mechanical tests)
(a) Mechanical tests				
(b) TV/TC tests				

33. Please, describe briefly the criteria adopted to decide the position of the sensors.

(a) Mechanical tests

(b) TV/TC tests

APPENDIX B – Cubesat Questionnaire

34. Did you perform a calibration of GSE, and in particular measurement systems (such scale, voltmeter, amperometer, callipers, ...) before performing the tests? (If their calibration was performed by a certified authority and was still within the expiry date you may answer yes) (Select one option)
○ Yes ○ No

35. Has any kind of dry-test been conducted on the GSE before performing the tests? (e.g. to verify the correct functionality of the GSE and/or the sensors) (Select one option)
○ Yes ○ No

36. If in the previous question you answered yes, please explain briefly what kind of dry-tests you have conducted

APPENDIX B – Cubesat Questionnaire

CUBESAT VERIFICATION EXECUTION

What verification have you performed at system level and what method have you used?

	37. Select if the verification has been conducted		38. If yes, please select the verification method(s)	
	Yes	**No**	**Analysis**	**Test**
(a) Mass measurement	○	○	○	○
(b) Geometry measurement	○	○	○	○
(c) Centre of Gravity measurement	○	○	○	○
(d) Moments of Inertia measurement	○	○	○	○
(e) Static loads	○	○	○	○
(f) Shock	○	○	○	○
(g) Random vibrations	○	○	○	○
(h) Sinusoidal vibrations	○	○	○	○
(i) Thermal Vacuum/Thermal Cycling	○	○	○	○
(j) EMC/EMauto-Compatibility	○	○	○	○
(k) Radiations	○	○	○	○
(l) Functional test	○	○	○	○
(m) Performance test	○	○	○	○
(n) Mission test	○	○	○	○

Please, specify the following parameters established for the TV/TC test (if performed)

	39. Value of the parameters for the TV/TC tests
(a) Maximum temperature [ºC]	
(b) Duration of the hot plateaux [min]	
(c) Minimum temperature [ºC]	
(d) Duration of the cold plateaux [min]	
(e) Number of cycles	
(f) Temperature rate of change [ºC/min]	
(g) Dwell time until functional test starts [min]	
(h) Were the maximum and minimum temperatures applied evenly to the whole satellite or to selected parts?	

APPENDIX B – Cubesat Questionnaire

40. How did you establish the temperatures limits for the TV/TC tests? (e.g. based on previous experience, from a thermal analysis, from components/materials datasheet, etc.)

41. How did you establish the number of cycles of the TV/TC tests?

Please, specify the levels of the static loads test (if performed)

	42. Longitudinal QSL [g]	43. Lateral QSL [g]
(a) Maximum		
(b) Minimum		

44. How did you establish the static loads levels?

Please, specify the levels of the shock test (if performed)

	45. Frequency [Hz]	46. SRS Input level [g] with Q-factor of 10
(a) First values		
(b) Second values		
(c) Third values		
(d) Fourth values		
(e) Fifth values		

47. How did you establish the shock level?

48. In what direction(s) and how many times has the shock been applied?

Please, specify the levels of the random vibrations test (if performed)

	49. Frequency [Hz]	50. Level [g^2/Hz]
(a) First values		
(b) Second values		
(c) Third values		
(d) Fourth values		
(e) Fifth values		
(f) Sixth values		
(g) Seventh values		
(h) Eighth values		
(i) Ninth values		
(j) Tenth values		

51. Duration of the random vibrations test [min]

52. How did you establish the random vibrations levels?

APPENDIX B – Cubesat Questionnaire

Please, specify the levels of the sinusoidal vibrations test (if performed)

	53. Frequency [Hz]	54. Level [g]
(a) First values		
(b) Second values		
(c) Third values		
(d) Fourth values		
(e) Fifth values		
(f) Sixth values		
(g) Seventh values		
(h) Eighth values		
(i) Ninth values		
(j) Tenth values		

55. Sweep rate of sinusoidal vibrations test[oct/min]

56. How did you establish the sinusoidal vibrations levels?

57. How did you establish the levels for the EMC/EMauto-Compatibility tests?

58. How did you establish the radiation levels (if performed)?

APPENDIX B – Cubesat Questionnaire

CUBESAT VERIFICATION RESULTS

59. Has(ve) any anomaly(ies)/failure(s) been individuated during the tests?

○ Yes ○ No

60. Has(ve) the anomaly(ies)/failure(s) been fixed before the launch? (Select one option)

○ Yes ○ No

61. Please, specify which test/s has/ve been repeated after the failure(s) has(ve) been fixed

☐ Physical properties ☐ Static loads ☐ Shock ☐ Random vibrations ☐ Sinusoidal vibrations

☐ TV/TC ☐ EMC/EMAuto-Compatibility ☐ Radiations ☐ Functional test

☐ Performance test ☐ Mission test ☐ Other (please specify):

Please, specify in which test(s)the anomaly(ies)/failure(s) has(ve) been individuated. For each one, please describe briefly the observed failure

	62. Anomaly(ies)/Failure(s) observed			63. Brief description of the anomaly(ies)/Failure(s)
	Yes	**No**	**Verification not conducted**	
(a) Physical properties measurement	○	○	○	
(b) Static loads test	○	○	○	
(c) Shock	○	○	○	
(d) Random vibrations test	○	○	○	
(e) Sinusoidal vibrations test	○	○	○	
(f) Thermal Vacuum/Thermal cycling test	○	○	○	
(g) EMC/EMauto-Compatibility tests	○	○	○	
(h) Radiation test	○	○	○	
(i) Functional test	○	○	○	
(j) Performance test	○	○	○	
(k) Mission test	○	○	○	

For the observed anomaly(ies)/failure(s) (for each test) select the consequence on the project in terms of cost (assuming a project budget of 100k€) and schedule (assuming 2 years design life

cycle)

	64. Cost increasing wrt a project budget of 100k€				65. Schedule delay wrt 2 years design life cycle			
	More than 15 %	**Up to 15%**	**Up to 5%**	**Up to 1%**	**Delay > 6 months**	**Delay up to 6 months**	**Delay up to 3 months**	**Delay up to 1 months**
(a) Anomalies during physical properties measurement	○	○	○	○	○	○	○	○
(b) Failures during static loads test	○	○	○	○	○	○	○	○
(c) Failures during shock tests	○	○	○	○	○	○	○	○
(d) Failures during random vibrations test	○	○	○	○	○	○	○	○
(e) Failures during sinusoidal vibrations test	○	○	○	○	○	○	○	○
(f) Failures during thermal Vacuum/Thermal cycling test	○	○	○	○	○	○	○	○
(g) Failures during EMC/EMauto-Compatibility tests	○	○	○	○	○	○	○	○
(h) Failures during radiation test	○	○	○	○	○	○	○	○
(i) Failures during functional test	○	○	○	○	○	○	○	○
(j) Failures during performance test	○	○	○	○	○	○	○	○
(k) Failures during mission test	○	○	○	○	○	○	○	○

CUBESAT INTEGRATION INTO THE DEPLOYER

66. How long the CubeSat has remained installed inside the deployer until the launch? [days]

67. Has been possible to recharge the batteries after its integration into the deployer? (Select one option)

○ Yes ○ No

68. If in the previous question you answered yes, when was the last time the batteries were recharged? [days before launch date]

CUBESAT INTEGRATION INTO THE DEPLOYER

69. How did you verify the correct ejection of the CubeSat from the deployer?

☐ Ejection confirmed by launch authority/launch provider

☐ Ejection confirmed by CubeSat deployer provider

☐ Ejection confirmed when first signal of the CubeSat was received

☐ Other (please specify):

70. How did you know that the antenna has been deployed?

71. Has a communication link with the satellite been established within the first hours after its deployment? (Select one option)

○ Yes ○ No

APPENDIX B – Cubesat Questionnaire

72. If in the previous question you answered no, please briefly explain the reason why, in your opinion, the communication link has not been established

73. Has the intensity level of the signal been high enough to correctly decode the signal? (Select one option)
○ Yes ○ No

74. If in the previous question you answered no, please briefly explain why, in your opinion, the received signal power was not high enough to be decoded?

75. Have the telemetry values been comprised in the nominal/expected ranges? (Select one option)
○ Yes ○ No

76. If in the previous question you answered no, please briefly explain why the telemetry values were not in the nominal/expected ranges?

CUBESAT INTEGRATION INTO THE DEPLOYER

77. Has(ve) failure(s)/malfunction(s) been observed on the CubeSat during the nominal mission? (Select one option)

○ Yes ○ No

78. Please, explain briefly which is, in your opinion, the origin of the failure(s) you observed and the consequences on the system and mission.

79. If any failure(s) has(ve) been observed, on which subsystem(s) occurred?

☐ EPS ☐ ADCS ☐ Mechanisms ☐ Payload

☐ COM ☐ OBDH ☐ Thermal

80. Have you performed corrective actions to restore the satellite into its nominal conditions? (Select one option)

○ Yes

○ No

81. What was the nominal mission duration and the real mission duration? (if the mission has not been finished leave the real mission duration field empty)

(a) Nominal duration [months]

(b) Real duration [months]

82. What is the rate of success of your mission (%) wrt your success criteria? (Enter a value greater than 0)

83. How long you took to complete the questionnaire? [minutes]

APPENDIX B – Cubesat Questionnaire

If you would like to recommend other people to fill this questionnaire, please provide their names and e-mail addresses

	84. Name and Surname	85. e-mail
(a) Person #1		
(b) Person #2		
(c) Person #3		
(d) Person #4		
(e) Person #5		
(f) Person #6		
(g) Person #7		
(h) Person #8		
(i) Person #9		
(j) Person #10		

86. Please provide any comment or suggestion you have

APPENDIX C

E-st@r-I FMECA

FMECA

CubeSat:	e-st@r-I
Date:	20.12.2013
Prepared by:	Gerard Obiols Rabasa gerard.obiols@polito.it
Approved by:	Fabrizio Stesina fabrizio.stesina@polito.it
Revision:	2
Issue:	0

System: e-st@r-I							Subsystem: All			
Ident. Number	Item/block	Function	Failure mode	Failure cause	Mission phase/ Op. Mode	Failure effects a. Local effects b. Next higher level b. End effects	Severity classification	Severity Number SN	Probability and PN	Criticality Number CN
1	e-st@r-I	Mission object	PCDU does not correctly work	Voltage regulator does not work PIC does not work ADC does not work Filter and protection lost BCR-SP1/SP2 does not work BCR-SP3/SP4 does not work BCR-SP5 does not work Connector SP1-SP2 does not work Connector SP5 does not work MPPT SP1-SP2 does not work MPPT SP3-SP4 does not work MPPT SP5 does not work	Basic mode Full mode Save energy Safe mission Temporary shut down	a. No power to satellite subsystems b. Loss of all subsystems c. Mission failed	I - Catastrophic	4		
2			D-PCDU does not correctly work	Battery pack 1 does not work Battery pack 2 does not work Temperature sensor 1 does not work Temperature sensor 2 does not work Connector PCDU/D-PCDU does not work Studs do not work	Basic mode Full mode Save energy Safe mission Temporary shut down	a. No power to satellite subsystems b. Loss of all subsystems c. Mission failed	I - Catastrophic	4		
3			ADCS does not correctly work	ARM9 fails IMU fails Connector MT -X fails Connector MT +Y fails Connector MT -Z fails MT -X fails MT +Y fails MT -Z fails 104 pin connector fails	Basic mode Full mode Save energy Safe mission Temporary shut down	a. Not possible to determine and control attitude b. N/A c. Loss of the payload	II - Critical	3		
4			COMSYS does not correctly work	Dipole antenna does not work Radio module fails PIC fails 104 pin connector fails	Basic mode Full mode Save energy Safe mission Temporary shut down	a. COMSYS does not process commands b. Not possible to establish a communication link c. Mission failed	I - Catastrophic	4		
5			OBC does not correctly work	MSP430 fails Watchdog fails Clock fails Flash memory fails EEPROM memory fails RAM memory fails SD card fails Deployment switch fails 104 pin connector fails	Basic mode Full mode Save energy Safe mission Temporary shut down	a. OBC does not work b. Satellite lost c. Mission Failed	I - Catastrophic	4		

APPENDIX C – E-st@r-l FMECA

System: e-st@r-l							Subsystem: EPS			
Ident. Number	Item/block	Function	Failure mode	Failure cause	Mission phase/ Op. Mode	Failure effects a. Local effects b. Next higher level b. End effects	Severity classification	Severity Number SN	Probability and PN	Criticality Number CN
6	PCDU	Power Control and Distribution	Voltage regulator does not work	Physical break Burnout	Basic mode Full mode Save energy Safe mission Temporary shut	a. PCDU does not work b. Possible overcharge on other subsystems c. Possible loss of EPS or other subsystem(s)	II - Critical	3		
7			PIC does not work	Physical break Burnout Degraded operation Shorted Opened Parametric failure Mechanical failure Functional failure Bond failure	Basic mode Full mode Save energy Safe mission Temporary shut down	a. Lost of data about EPS b. PCDU does not work correctly c. EPS may not work	II - Critical	3		
8			ADC does not work	Physical break Burnout	Basic mode Full mode Save energy Safe mission Temporary shut	a. Lost of data about EPS b. PCDU does not work correctly c. EPS may not work	II - Critical	3		
9			Filter and Protection lost	Physical break Burnout	Basic mode Full mode Save energy Safe mission Temporary shut down	a. PCDU does not work correctly b. Possible overcharge on other subsystem(s) c. Possible loss of EPS or other subsystem(s)	II - Critical	3		
10			BCR-SP1/SP2 does not work	Physical break Burnout	Basic mode Full mode Save energy Safe mission Temporary shut	a. Loss of SP1 and SP2 b. Less power to PCDU c. Less power available on board	II - Critical	3		
11			BCR-SP3/SP4 does not work	Physical break Burnout	Basic mode Full mode Save energy Safe mission Temporary shut	a. Loss of SP3 and SP4 b. Less power to PCDU c. Less power available on board	II - Critical	3		
12			BCR-SP5 does not work	Physical break Burnout	Basic mode Full mode Save energy Safe mission Temporary shut	a. Loss of SP5 b. Less power to PCDU c. Less power available on board	III - Marginal	2		
13			Connector SP1-SP2 does not work	Physical break Mechanical connection failure Intermittant contact	Basic mode Full mode Save energy Safe mission Temporary shut	a. Loss of SP1 and SP2 b. Less power to PCDU c. Less power available on board	II - Critical	3		
14			Connector SP3-SP4 does not work	Physical break Mechanical connection failure Intermittant contact	Basic mode Full mode Save energy Safe mission Temporary shut	a. Loss of SP3 and SP4 b. Less power to PCDU c. Less power available on board	II - Critical	3		
15			Connector SP5 does not work	Physical break Mechanical connection failure Intermittant contact	Basic mode Full mode Save energy Safe mission Temporary shut	a. Loss of SP5 b. Less power to PCDU c. Less power available on board	III - Marginal	2		
16			MPPT SP1-SP2 does not work	Physical break Burnout	Basic mode Full mode Save energy Safe mission Temporary shut	a. Loss of energy from SP1-SP2 b. Less power to PCDU c. Less power available on board	II - Critical	3		
17			MPPT SP3-SP4 does not work	Physical break Burnout	Basic mode Full mode Save energy Safe mission Temporary shut	a. Loss of energy from SP3-SP4 b. Less power to PCDU c. Less power available on board	II - Critical	3		
18			MPPT SP5 does not work	Physical break Burnout	Basic mode Full mode Save energy Safe mission Temporary shut	a. Loss of energy from SP5 b. Less power to PCDU c. Less power available on board	III - Marginal	2		

19	D-PCDU	Doughter power control and distribution	Battery pack 1 does not work	Connection physically broken Physical disconnection of the connector Burnout Power requested from the ADCS too high	Basic mode Full mode Save energy Safe mission Temporary shut down	a. Less power available b. Partial EPS failure c. Not able to supply power to all subsystems	II - Critical	2		
20			Battery pack 2 does not work	Connection physically broken Physical disconnection of the connector Burnout Power requested from the ADCS too high	Basic mode Full mode Save energy Safe mission Temporary shut down	a. Less power available b. Partial EPS failure c. Not able to supply power to all subsystems	II - Critical	2		
21			Temperature sensor 1 does not work	Physical break Burnout	Basic mode Full mode Save energy Safe mission Temporary shut down	a. Temperature value of sensor 1 not available b. Battery pack 1 temperature not controlled c. Battery pack 1 temperature could be out of operative range, or the battery may not	IV - Minor	1		
22			Temperature sensor 2 does not work	Physical break Burnout	Basic mode Full mode Save energy Safe mission Temporary shut down	a. Temperature value of sensor 2 not available b. Battery pack 2 temperature not controlled c. Battery pack 2 temperature could be out of operative range, or the battery may not	IV - Minor	1		
23			Connector PCDU/D-PCDU does not work	Mechanical connection failure Intermittant contact	Basic mode Full mode Save energy Safe mission Temporary shut	a. Loss of data from d-PCDU b. Possible loss of D-PCDU c.	II - Critical	3		
24			Studs do not work	Physical break Burnout	Basic mode Full mode Save energy Safe mission Temporary shut	a. Loss of D-PCDU b. EPS does not work c. No power to satellite subsystems	I - Catastrophic	4		

APPENDIX C – E-st@r-l FMECA

System: e-st@r-l							Subsystem/Component: EPS/All			
Ident. Number	Item/block	Function	Failure mode	Failure cause	Mission phase/ Op. Mode	Failure effects a. Local effects b. Next higher level b. End effects	Severity classification	Severity Number SN	Probability and PN	Criticality Number CN
25	PIC	EPS microcontroller	Physical break	High mechanical loads during the launch	Launch	a. PIC does not work b. Lost of data about EPS c. PCDU does not work	II - Critical	3		
26			Burnout	Affected by radiation Overcurrent Temperature out of the operative temperature range of the component	Basic mode Full mode Save energy Safe mission Temporary shut	a. PIC does not work b. Lost of data about EPS c. PCDU does not work correctly	II - Critical	3		
27	Solar panel 1	To obtain electrical power from sun radiation	Physical break		Launch	a. Solar panel 1 does not produce electrical power b. Less power to PCDU c. Less power to subsystems and	II - Critical	3		
28			Temperature SP1 does not work		Basic mode Full mode Save energy Safe mission Temporary shut down	a. Temperature value of SP1 temperature sensor not available b. SP1 temperature not controlled c. SP1 temperature could be out of operative range: less	III - Marginal	2		
29	Solar panel 2	To obtain electrical power from sun radiation	Physical break		Launch	a. Solar panel 2 does not produce electrical power b. Less power to PCDU	II - Critical	3		
30			Temperature SP2 does not work		Basic mode Full mode Save energy Safe mission Temporary shut down	a. Temperature value of SP2 temperature sensor not available b. SP2 temperature not controlled c. SP2 temperature could be out of operative range: less	III - Marginal	2		
31	Solar panel 3	To obtain electrical power from sun radiation	Physical break		Launch	a. Solar panel 3 does not produce electrical power b. Less power to PCDU c. Less power to subsystems and	II - Critical	3		
32			Temperature SP3 does not work		Basic mode Full mode Save energy Safe mission Temporary shut down	a. Temperature value of SP3 temperature sensor not available b. SP3 temperature not controlled c. SP3 temperature could be out of operative range: less	III - Marginal	2		
33	Solar panel 4	To obtain electrical power from sun radiation	Physical break		Launch	a. Solar panel 4 does not produce electrical power b. Less power to PCDU c. Less power to subsystems and	II - Critical	3		
34			Temperature SP4 does not work		Basic mode Full mode Save energy Safe mission Temporary shut down	a. Temperature value of SP4 temperature sensor not available b. SP4 temperature not controlled c. SP4 temperature could be out of operative range: less	III - Marginal	2		
35	Solar panel 5	To obtain electrical power from sun radiation	Physical break		Launch	a. Solar panel 5 does not produce electrical power b. Less power to PCDU c. Less power to subsystems and	II - Critical	3		
36			Temperature SP5 does not work		Basic mode Full mode Save energy Safe mission Temporary shut down	a. Temperature value of SP5 temperature sensor not available b. SP5 temperature not controlled c. SP5 temperature could be out of operative range: less	III - Marginal	2		
37	Voltage Regulator	Regulate voltage from EPS to subsystems	Physical break	High mechanical loads during the launch	Launch	a. Voltage regulator does not work b. PCDU does not work correctly c. Possible overcharge on other subsystem(s)	II - Critical	3		
38			Burnout	Affected by radiation Overcurrent Temperature out of the operative temperature range of the component	Basic mode Full mode Save energy Safe mission Temporary shut down	a. Voltage regulator does not work b. PCDU does not work correctly c. Possible overcharge on other subsystem(s)	II - Critical	3		

39	Filter and protection	Power filter and protection from singular events	Physical break	High mechanical loads during the launch	Launch	a. F&P lost b. PCDU does not work correctly c. Possible overcharge on other subsystem(s)	II - Critical	3		
40			Burnout	Affected by radiation Overcurrent Temperature out of the operative temperature range of the component	Basic mode Full mode Save energy Safe mission Temporary shut	a. F&P lost b. PCDU does not work correctly c. Possible overcharge on other subsystem(s)	II - Critical	3		
41	Connector SP1-SP2	Connect solar panels 1 and 2 to battery charge regulator	Physical break	High mechanical loads during the launch	Launch	a. Connector SP1/SP2 does not work b. Loss of energy produced by SP1 and SP2	II - Critical	3		
42			Mechanical connection failure	Disconnection of the SP1-SP2 connector during the launch due to vibrations Crimped wires not correctly inserted into the connector	Basic mode Full mode Save energy Safe mission Temporary shut down	a. Connector SP1/SP2 does not work b. Loss of energy produced by SP1 and SP2	II - Critical	3		
43			Intermittant contact	Crimped wires not correctly inserted into the connector SP1-SP2 connector not correctly inserted into the ADCS board receptacle		a. Connector SP1/SP2 may not work b. SP1 and SP2 energy may not be availabe c. Possible less power to PCDU	II - Critical	3		
44	Connector SP3-SP4	Connect solar panels 3 and 4 to battery charge regulator	Physical break	High mechanical loads during the launch	Launch	a. Connector SP3/SP4 does not work b. Loss of energy produced by SP3 and SP4	II - Critical	3		
45			Mechanical connection failure	Disconnection of the SP3-SP4 connector during the launch due to vibrations Crimped wires not correctly inserted into the connector	Basic mode Full mode Save energy Safe mission Temporary shut down	a. Connector SP3/SP4 does not work b. Loss of energy produced by SP3 and SP4	II - Critical	3		
46			Intermittant contact	Crimped wires not correctly inserted into the connector SP3-SP4 connector not correctly inserted into the ADCS board receptacle		a. Connector SP3/SP4 may not work b. SP3 and SP4 energy may not be availabe c. Possible less power to PCDU	II - Critical	3		
47	Connector SP5	Connect solar panel 5 to battery charge regulator	Physical break	High mechanical loads during the launch	Launch	a. Connector SP5 does not work b. Loss of energy produced by SP5 c. Less power to PCDU	III - Marginal	2		
48			Mechanical connection failure	Disconnection of the SP5 connector during the launch due to vibrations Crimped wires not correctly inserted into the connector	Basic mode Full mode Save energy Safe mission Temporary shut down	a. Connector SP5 does not work b. Loss of energy produced by SP5 c. Less power to PCDU	III - Marginal	2		
49			Intermittant contact	Crimped wires not correctly inserted into the connector SP5 connector not correctly inserted into the ADCS board receptacle		a. Connector SP5 may not work b. SP5 energy may not be availabe c. Possible less power to PCDU	III - Marginal	2		
50	Battery charge regulator SP1-SP2	Regulate battery charging, protection from power overloads and overcharges	Physical break	High mechanical loads during the launch	Launch	a. BCR-SP1/SP2 does not work b. SP1 and SP2 power not regulated c. Less power to PCDU	II - Critical	3		
51			Burnout	Affected by radiation Overcurrent Temperature out of the operative temperature range of the component	Basic mode Full mode Save energy Safe mission Temporary shut	a. BCR-SP1/SP2 does not work b. SP1 and SP2 power not regulated c. Less power to PCDU	II - Critical	3		
52	Battery charge regulator SP3-SP4	Regulate battery charging, protection from power overloads and overcharges	Physical break	High mechanical loads during the launch	Launch	a. BCR-SP3/SP4 does not work b. SP3 and SP4 power not regulated c. Less power to PCDU	II - Critical	3		
53			Burnout	Affected by radiation Overcurrent Temperature out of the operative temperature range of the component	Basic mode Full mode Save energy Safe mission Temporary shut	a. BCR-SP3/SP4 does not work b. SP3 and SP4 power not regulated c. Less power to PCDU	II - Critical	3		
54	Battery charge regulator SP5	Regulate battery charging, protection from power overloads and overcharges	Physical break	High mechanical loads during the launch	Launch	a. BCR-SP5 does not work b. SP5 power not regulated c. Less power to PCDU	II - Critical	3		
55			Burnout	Affected by radiation Overcurrent Temperature out of the operative temperature range of the component	Basic mode Full mode Save energy Safe mission Temporary shut	a. BCR-SP5 does not work b. SP5 power not regulated c. Less power to PCDU	II - Critical	3		
56	ADC	Convert analogic data from PCDU to digital data to communicate to PIC	Physical break	High mechanical loads during the launch	Launch	a. ADC does not work b. Lost of data about EPS c. PCDU does not work	II - Critical	3		
57			Burnout	Affected by radiation Overcurrent Temperature out of the operative temperature range of the component	Basic mode Full mode Save energy Safe mission Temporary shut	a. ADC does not work b. Lost of data about EPS c. PCDU does not work correctly	II - Critical	3		

APPENDIX C – E-st@r-l FMECA

58	MPPT SP1 - SP2		Physical break	High mechanical loads during the launch	Launch	a. MPPT SP1 - SP2 does not work	II - Critical	3		
59			Burnout	Affected by radiation Overcurrent Temperature out of the operative temperature range of the component	Basic mode Full mode Save energy Safe mission Temporary shut	a. MPPT SP1 - SP2 does not work	II - Critical	3		
60	MPPT SP3 - SP4		Physical break	High mechanical loads during the launch	Launch	a. MPPT SP3 - SP4 does not work	II - Critical	3		
61			Burnout	Affected by radiation Overcurrent Temperature out of the operative temperature range of the component	Basic mode Full mode Save energy Safe mission Temporary shut	a. MPPT SP3 - SP4 does not work	II - Critical	3		
62	MPPT SP5		Physical break	High mechanical loads during the launch	Launch	a. MPPT SP5 does not work	III - Marginal	2		
63			Burnout	Affected by radiation Overcurrent Temperature out of the operative temperature range of the component	Basic mode Full mode Save energy Safe mission Temporary shut	a. MPPT SP5 does not work	III - Marginal	2		
64	Battery pack 1	Store electrical power	Connection physically broken	High mechanical loads during the launch	Basic mode Full mode Save energy Safe mission Temporary shut down	a. Battery pack 1 does not supply electrical power to PCDU b. Partial EPS failure c. Less power to satellite subsystems	II - Critical	3		
65			Physical disconnection of the connector	Vibrations during launch Crimped wires not correctly inserted to the connectors		a. Battery pack 1 does not supply electrical power to PCDU b. Partial EPS failure c. Less power to satellite subsystems	II - Critical	3		
66			Burnout	Temperature out of the operative temperature range of the component Battery is not a space qualified component: could not execute expected functions		a. Battery pack 1 does not supply electrical power to PCDU b. Partial EPS failure c. Less power to satellite subsystems	II - Critical	3		
67	Battery pack 2	Store electrical power	Connection physically broken	High mechanical loads during the launch	Basic mode Full mode Save energy Safe mission Temporary shut down	a. Battery pack 2 does not supply electrical power to PCDU b. Partial EPS failure c. Less power to satellite subsystems	II - Critical	3		
68			Physical disconnection of the connector	Vibrations during launch Crimped wires not correctly inserted to the connectors		a. Battery pack 2 does not supply electrical power to PCDU b. Partial EPS failure c. Less power to satellite subsystems	II - Critical	3		
69			Burnout	Temperature out of the operative temperature range of the component Battery is not a space qualified component: could not execute expected functions		a. Battery pack 2 does not supply electrical power to PCDU b. Partial EPS failure c. Less power to satellite subsystems	II - Critical	3		
70	Temperature sensor SP1	Measure operational temperature of solar panel 1	Physical break	High mechanical loads during the launch	Launch	a. Temperature value of SP1 temperature sensor not available b. Solar panel 1 temperature not controlled c. Only SP1 temperature sensore	IV - Minor	1		
71						a. Temperature value of SP1 temperature sensor not available b. Solar panel 1 temperature not controlled c. Solar panel 1 temperature could be out of temperature operative range, it could be broken: less power to EPS	III - Marginal	2		
72			Burnout	Affected by radiation Overcurrent Crimped wires not correctly welded	Basic mode Full mode Save energy Safe mission Temporary shut down	a. Temperature value of SP1 temperature sensor not available b. Solar panel 1 temperature not controlled c. Only SP1 temperature sensore	IV - Minor	1		
73						a. Temperature value of SP1 temperature sensor not available b. Solar panel 1 temperature not controlled c. Solar panel 1 temperature could be out of operative range: less power to EPS	III - Marginal	2		

74	Temperature sensor SP2	Measure operational temperature of solar panel 2	Physical break	High mechanical loads during the launch	Launch	a. Temperature value of SP2 temperature sensor not available b. SP2 temperature not controlled c. Only SP2 temperature sensore	IV - Minor	1		
75						a. Temperature value of SP2 temperature sensor not available b. SP2 temperature not controlled c. Solar panel 2 temperature could be out of temperature operative range, it could be broken: less power to EPS	III - Marginal	2		
76			Burnout		Basic mode Full mode Save energy Safe mission Temporary shut down	a. Temperature value of SP2 temperature sensor not available b. SP2 temperature not controlled c. Only SP2 temperature sensore	IV - Minor	1		
77						a. Temperature value of SP2 temperature sensor not available b. SP2 temperature not controlled c. SP2 temperature could be out of operative range: less	III - Marginal	2		
78	Temperature sensor SP3	Measure operational temperature of solar panel 3	Physical break	High mechanical loads during the launch	Launch	a. Temperature value of SP3 temperature sensor not available b. SP3 temperature not controlled c. Only SP3 temperature sensore	IV - Minor	1		
79						a. Temperature value of SP3 temperature sensor not available b. SP3 temperature not controlled c. Solar panel 3 temperature could be out of temperature operative range, it could be broken: less power to EPS	III - Marginal	2		
80			Burnout	Affected by radiation Overcurrent Crimped wires not correctly welded	Basic mode Full mode Save energy Safe mission Temporary shut down	a. Temperature value of SP3 temperature sensor not available b. SP3 temperature not controlled c. Only SP3 temperature sensore	IV - Minor	1		
81						a. Temperature value of SP3 temperature sensor not available b. SP3 temperature not controlled c. SP3 temperature could be out of operative range: less	III - Marginal	2		
82	Temperature sensor SP4	Measure operational temperature of solar panel 4	Physical break	High mechanical loads during the launch	Launch	a. Temperature value of SP4 temperature sensor not available b. SP4 temperature not controlled c. Only SP4 temperature sensore	IV - Minor	1		
83						a. Temperature value of SP4 temperature sensor not available b. SP4 temperature not controlled c. Solar panel 4 temperature could be out of temperature operative range, it could be broken: less power to EPS	III - Marginal	2		
84			Burnout	Affected by radiation Overcurrent Crimped wires not correctly welded	Basic mode Full mode Save energy Safe mission Temporary shut down	a. Temperature value of SP4 temperature sensor not available b. SP4 temperature not controlled c. Only SP4 temperature sensore	IV - Minor	1		
85						a. Temperature value of SP4 temperature sensor not available b. SP4 temperature not controlled c. SP4 temperature could be out of operative range: less	III - Marginal	2		

86	Temperature sensor SP5	Measure operational temperature of solar panel 5	Physical break	High mechanical loads during the launch	Launch	a. Temperature value of SP5 temperature sensor not available b. SP5 temperature not controlled c. Only SP5 temperature sensore	IV - Minor	1		
87						a. Temperature value of SP5 temperature sensor not available b. SP5 temperature not controlled c. Solar panel 5 temperature could be out of temperature operative range, it could be broken: less power to EPS	III - Marginal	2		
88			Burnout	Affected by radiation Overcurrent Crimped wires not correctly welded	Basic mode Full mode Save energy Safe mission Temporary shut down	a. Temperature value of SP5 temperature sensor not available b. SP5 temperature not controlled c. Only SP5 temperature sensore	IV - Minor	1		
89						a. Temperature value of SP5 temperature sensor not available b. SP5 temperature not controlled c. SP5 temperature could be out of operative range: less	III - Marginal	2		
90	Connector PCDU/D-PCDU	Connect PCDU to D-PCDU in data transmission	Mechanical connection failure	High mechanical loads during the launch	Basic mode Full mode Save energy Safe mission Temporary shut down	a. Connector PCDU/D-PCDU does not work b. No data transmisison between PCDU and D-PCDU c. Loss of data from D-PCDU	II - Critical	3		
91			Intermittant contact	Non correct connection due to vibration during the launch	Basic mode Full mode Save energy Safe mission Temporary shut down	a. Connector PCDU/D-PCDU does not work correctly b. Data from D-PCDU not always available c. Intermittant loss of data from D-PCDU	II - Critical	3		
92	Studs	Electrical power connection	Physical break	High mechanical loads during the launch	Launch	a. Studs do not work b. Loss of D-PCDU c. EPS does not work	I - Catastrophic	4		
93			Burnout		Basic mode Full mode Save energy Safe mission Temporary shut	a. Studs do not work b. Loss of D-PCDU c. EPS does not work	I - Catastrophic	4		
94	104 pin connector	Interface among subsystems. Transfer data and power	Mechanical connection failure	High mechanical loads which produce the break of the pins	Basic mode Full mode Save energy Safe mission Temporary shut down	a. Connector not able to interface among subsystems b. Data and power not transfered from the EPS to the subsystems c. Loss of satellite	I - Catastrophic	4		

System: e-st@r-l							Subsystem: ADCS			
Ident. Number	Item/block	Function	Failure mode	Failure cause	Mission phase/ Op. Mode	Failure effects a. Local effects b. Next higher level b. End effects	Severity classification	Severity Number SN	Probability and PN	Criticality Number CN
95	ARM9	Process ADCS data	Physical break	High mechanical loads	Launch	a. ARM9 lost b. ADCS not able to determine and control the satellite attitude c. Payload lost	II - Critical	3		
96			Burnout	Affected by radiation Overcurrent Temperature out of the operative temperatur range of the component	Basic mode Full mode Save energy Safe mission Temporary shut	a. ARM9 lost b. ADCS not able to determine and control the satellite attitude c. Payload lost	II - Critical	3		
97			ARM9 unplugged	Vibrations during launch unplugged the ARM9	Basic mode Full mode Save energy Safe mission Temporary shut	a. ARM9 lost b. ADCS not able to determine and control the satellite's attitude c. Payload lost	II - Critical	3		
98	IMU	Measure satellite accelerations and the magnetic field	Physical break	High mechanical loads which produce the break of the screws with which the IMU is screwed to the ADCS board	Launch	a. IMU lost b. ADCS not able to determine the satellite's attitude c. Payload lost	II - Critical	3		
99			Burnout	Affected by radiation Overcurrent Temperature out of the operative temperatur range of the component	Basic mode Full mode Save energy Safe mission Temporary shut	a. IMU lost b. ADCS not able to determine the satellite's attitude c. Payload lost	II - Critical	3		
100	Connector MT +X	To connect MT +X to ADCS board	Mechanical connection failure	Disconnection of the MT connector during the launch due to vibrations Crimped wires not correctly inserted into the connectors	Basic mode Full mode Save energy Safe mission Temporary shut down	a. MT +X does not work b. Satellite not able to control its attitude around relative axis c. Attitude control ability reduced	III - Marginal	2		
101			Physical break	High mechanical loads	Launch	a. MT +X does not work b. Satellite not able to control its attitude around relative axis c. Attitude control ability reduced	III - Marginal	2		
102			Intermittant contact	Crimped wires not correctly inserted into the connector MT connector not correctly inserted into the ADCS board receptacle	Basic mode Full mode Save energy Safe mission Temporary shut down	a. MT +X works intermittantly b. Satellite not always able to control its attitude around relative axis c. Attitude control ability intermittantly	IV - Minor	1		
103	Connector MT -Y	To connect MT -Y to ADCS board	Mechanical connection failure	Disconnection of the MT connector during the launch due to vibrations Crimped wires not correctly inserted into the connectors	Basic mode Full mode Save energy Safe mission Temporary shut down	a. MT -Y does not work b. Satellite not able to control its attitude around relative axis c. Attitude control ability reduced	III - Marginal	2		
104			Physical break	High mechanical loads	Launch	a. MT -Y does not work b. Satellite not able to control its attitude around relative axis c. Attitude control ability reduced	III - Marginal	2		
105			Intermittant contact	Crimped wires not correctly inserted into the connector MT connector not correctly inserted into the ADCS board receptacle	Basic mode Full mode Save energy Safe mission Temporary shut down	a. MT -Y works intermittantly b. Satellite not always able to control its attitude around relative axis c. Attitude control ability intermittantly	IV - Minor	1		
106	Connector MT -Z	To connect MT -Z to ADCS board	Mechanical connection failure	Disconnection of the MT connector during the launch due to vibrations Crimped wires not correctly inserted into the connectors	Basic mode Full mode Save energy Safe mission Temporary shut down	a. MT -Z does not work b. Satellite not able to control its attitude around relative axis c. Attitude control ability reduced	III - Marginal	2		
107			Physical break	High mechanical loads	Launch	a. MT -Z does not work b. Satellite not able to control its attitude around relative axis c. Attitude control ability reduced	III - Marginal	2		
108			Intermittant contact	Crimped wires not correctly inserted into the connector MT connector not correctly inserted into the ADCS board receptacle	Basic mode Full mode Save energy Safe mission Temporary shut down	a. MT -Z works intermittantly b. Satellite not always able to control its attitude around relative axis c. Attitude control ability intermittantly	IV - Minor	1		

109	Magnetic torquer +X	Modify satellite attitude	Physical break	High mechanical loads during the launch	Launch	a. MT +X does not work b. Satellite not able to control its attitude around relative axis c. Attitude control ability reduced	IV - Minor	1		
110			Burnout	Overcurrent Shortcircuit of MT wires	Basic mode Full mode Save energy Safe mission Temporary shut down	a. MT +X does not work b. Satellite not able to control its attitude around relative axis c. Attitude control ability reduced	IV - Minor	1		
111	Magnetic torquer -Y	Modify satellite attitude	Physical break	High mechanical loads during the launch	Launch	a. MT -Y does not work b. Satellite not able to control its attitude around relative axis c. Attitude control ability reduced	IV - Minor	1		
112			Burnout	Overcurrent Shortcircuit of MT wires	Basic mode Full mode Save energy Safe mission Temporary shut down	a. MT -Y does not work b. Satellite not able to control its attitude around relative axis c. Attitude control ability reduced	IV - Minor	1		
113	Magnetic torquer -Z	Modify satellite attitude	Physical break	High mechanical loads during the launch	Launch	a. MT -Z does not work b. Satellite not able to control its attitude around relative axis c. Attitude control ability reduced	IV - Minor	1		
114			Burnout	Overcurrent Shortcircuit of MT wires	Basic mode Full mode Save energy Safe mission Temporary shut down	a. MT -Z does not work b. Satellite not able to control its attitude around relative axis c. Attitude control ability reduced	IV - Minor	1		
115	104 pin connector	Interface among subsystems. Transfer data and power	Mechanical connection failure	High mechanical loads which produce the break of the pins	Basic mode Full mode Save energy Safe mission Temporary shut down	a. Connector not able to interface among subsystems b. Data and power not transfered from the EPS to the subsystems c. Loss of satellite	I - Catastrophic	4		

System: e-st@r-I							Subsystem: COMSYS			
Ident. Number	Item/block	Function	Failure mode	Failure cause	Mission phase/ Op. Mode	Failure effects a. Local effects b. Next higher level b. End effects	Severity classification	Severity Number SN	Probability and PN	Criticality Number CN
116	Dipole antenna	Transmit and receive data to and from ground control station	Physical break	High mechanical loads	Launch Activation	a. Antenna does not work b. COMSYS not able to transmit nor receive data c. Communication link not established. Loss of communication	I - Catastrophic	4		
117			Antenna in contact with the structure	After the deployment, the antenna does not remains in its designed shape, it bends and touches the structure	Basic mode Full mode Save energy Safe mission Temporary shut down	a. Change of antenna characteristics b. Change of signal characteristics c. Degradation of communication link	II - Critical	3		
118	Radio module	Compose signal to transmit	Physical break	High mechanical loads	Launch	a. Radio module does not work b. COMSYS not able to transmit nor receive data c. Communication link not established. Loss of communication	I - Catastrophic	4		
119			Burnout	Affected by radiation Overcurrent Temperature out of the operative temperature range of the component	Basic mode Full mode Save energy Safe mission Temporary shut down	a. Radio module does not work b. COMSYS not able to transmit nor receive data c. Communication link not established. Loss of communication	I - Catastrophic	4		
120	PIC	TNC/modem tasks	Physical break	High mechanical loads	Launch	a. PIC does not work b. COMSYS not able to transmit nor receive data c. Communication link not established. Loss of communication	I - Catastrophic	4		
121			Burnout	Affected by radiation Overcurrent Temperature out of the operative temperature range of the component	Basic mode Full mode Save energy Safe mission Temporary shut down	a. PIC does not work b. COMSYS not able to transmit nor receive data c. Communication link not established. Loss of communication	I - Catastrophic	4		
122	104 pin connector	Interface among subsystems. Transfer data and power	Mechanical connection failure	High mechanical loads which produce the break of the pins	Basic mode Full mode Save energy Safe mission Temporary shut down	a. Connector not able to interface among subsystems b. Data and power not transfered from the EPS to the subsystems c. Loss of satellite	I - Catastrophic	4		

APPENDIX C – E-st@r-I FMECA

System: e-st@r-I							Subsystem: OBC			
Ident. Number	Item/block	Function	Failure mode	Failure cause	Mission phase/ Op. Mode	Failure effects a. Local effects b. Next higher level b. End effects	Severity classification	Severity Number SN	Probability and PN	Criticality Number CN
123	MSP430	Execute OBC code (microprocessor)	Physical break	High mechanical loads	Launch	a. CPU does not work b. OBC does not work c. Satellite lost	I - Catastrophic	4		
			Burnout	Affected by radiation Overcharge Temperature out of the operative temperature range of the component	Basic mode Full mode Save energy Safe mission Temporary shut	a. CPU does not work b. OBC does not work c. Satellite lost	I - Catastrophic	4		
124	Watchdog	To supervise CPU operations, avoiding deadlock	Physical break	High mechanical loads	Launch	a. Loss of watchdog b. CPU not supervised c. Possible OBC	I - Catastrophic	4		
			Burnout	Affected by radiation Overcharge Temperature out of the component nominal range of temperatures	Basic mode Full mode Save energy Safe mission Temporary shut	a. Loss of watchdog b. CPU not supervised c. Possible OBC deadlock	I - Catastrophic	4		
125	Clock	To give operation time to CPU	Physical break	High mechanical loads	Launch	a. Clock does not work b. CPU does not work c. OBC does not work	I - Catastrophic	4		
			Burnout	Affected by radiation Overcharge Temperature out of the component nominal range of temperatures	Basic mode Full mode Save energy Safe mission Temporary shut	a. Clock does not work b. CPU does not work c. OBC does not work	I - Catastrophic	4		
126	Flash memory		Physical break	High mechanical loads	Launch	a. Flash memory does not work b. CPU cannot communicate with flash memory c. OBC may not work	I - Catastrophic	4		
			Burnout	Affected by radiation Overcharge Temperature out of the component nominal range of temperatures	Basic mode Full mode Save energy Safe mission Temporary shut down	a. Flash memory does not work b. CPU cannot communicate with flash memory c. OBC may not work	I - Catastrophic	4		
127	EEPROM memory		Physical break	High mechanical loads	Launch	a. EEPROM memory does not work b. CPU may not work c. OBC may not work	I - Catastrophic	4		
			Burnout	Affected by radiation Overcharge Temperature out of the component nominal range of temperatures	Basic mode Full mode Save energy Safe mission Temporary shut	a. EEPROM memory does not work b. CPU may not work c. OBC may not work	I - Catastrophic	4		
128	RAM memory		Physical break	High mechanical loads	Launch	a. RAM memory does not work b. CPU may not work c. OBC may not work	I - Catastrophic	4		
			Burnout	Affected by radiation Overcharge Temperature out of the component nominal range of temperatures	Basic mode Full mode Save energy Safe mission Temporary shut	a. RAM memory does not work b. CPU may not work c. OBC may not work	I - Catastrophic	4		
129	SD card	To store data, operational files	Physical break	High mechanical loads	Launch	a. SD card does not work b. Loss of memorized data c. OBC may not work	I - Catastrophic	4		
			Burnout	Affected by radiation Overcharge Temperature out of the component nominal range of temperatures	Basic mode Full mode Save energy Safe mission Temporary shut down	a. SD card does not work b. Loss of memorized data and store of new data not possible c. OBC may not work	I - Catastrophic	4		
130	Deployment switch	Inhibit all satellite when pressed	DS not pressed during the launch	Tab boken Internal mechanisms broken Wires (which connect the DS to the OBC board) broken	Launch	a. Satellite electrically switch on b. Activation sequence understands that the satellite is inside the deployer and does not start c. Satellites remains "dormant"	IV - Minor	1		
			Vibrational open-close motion during the launch	Vibrations during launch produce enough separation between e-st@r-I and the satellite or the base plate with which is in contact to press and depress the DS	Launch	a. Fast cycling opening and closing activation circuit b. Activation sequence understands that the satellite is inside the deployer and does not start c. Satellites remains "dormant"	IV - Minor	1		
			Does not depress after release	Tab broken Internal mechanisms broken Wires (which connect the DS to the OBC board) broken	Activation	a. DS does not close the activation circuit b. All subsystems are switched off c. Satellite remains switched off	I - Catastrophic	4		
131	104 pin connector	Interface among subsystems. Transfer data and power	Mechanical connection failure	High mechanical loads which produce the break of the pins	Basic mode Full mode Save energy Safe mission Temporary shut down	a. Connector not able to interface among subsystems b. Data and power not transfered from the EPS to the subsystems c. Loss of satellite	I - Catastrophic	4		