POLITECNICO DI TORINO

DIPARTIMENTO di INGEGNERIA MECCANICA e AEROSPAZIALE
Corso di Laurea in Spazio
A.a 2020/2021
Sessione di Laurea Luglio 2021

TESI DI LAUREA

“Risk Assessment of an On Orbit Servicing mission based on space tug concept”

Relatore:
Nicole Viola

Correlatore:
Christopher Paissoni

Candidato:
Sergio Pansini

Matricola:
244090

Contents

List of Figures

List of Tables

Chapter 1

Introduzione

1.1 Historical background

Reliability analysis is a fundamental branch of any modern system design: it quantifies the probability of failure of the system and its protective barriers that prevent failure events to happen. Although reliability engineering has been acknowledged as a scientific discipline between 1960s and 1970s, some basic concepts were developed since the rise of mass production and during the World War II. In fact, after the war, several nations and US in particular funded studies to evaluate system failures and their relationship with component failures. These military efforts led to the rise and growth of this new discipline, formalized with the Advisory Group on Reliability of Electronic Equipment (AGREE) report in 1957. [1]
In the 1960s and 1970s, the discipline grew exponentially in different ways:

- development of new techniques (Bayesan approach, Markov chains..) and methods to identify possible failure causes;
- focus on software reliability, testing and maintenance;
- studies on system reliability and availability for complex space systems such as Mercury, Apollo and Gemini;
- evaluation of safety attributes and protective barriers of nuclear power plants. [1,2]

In early 1970s, reliability analysis were based on quantitative modeling of components, basically the probability that an item would not fail for a specified time or operation was estimated. Later, the focus shifted towards complex system analysis and the first steps in Probabilistic Risk Assessment (PRA) took place in the nuclear power industry with the WASH-1400 report in 1975. [1,3]
Meanwhile, NASA used quantitative risk analysis as a decision support tool for the Apollo program, but failure probabilities were overestimated because of conservative estimates so the Apollo program was more expensive than needed. Later on, NASA preferred qualitative analysis methods, such as Failure Mode and Effect Analysis (FMEA), Critical Item Lists (CIL) and risk matrices, to identify and mitigate potential risks. These methods collect information about likelihood and severity of consequences for each component to identify possible weak points and failure events that could lead to catastrophic effects.
In 1980s, NASA opposed resistance to PRA adoption for two reasons:

1. high cost of a complete PRA;

2. subjectivity of the Bayesan probability method.

However the Challenger disaster forced NASA to change risk approach and led to the review of all Space Shuttle FMEAs and CILs, because failuire risks were felt too optimistic. Since the Challenger accident, the use of PRA increased, there was an improvement of risk assessment methods and implementation of new models and software. Until then, FMEA had been seen as the main risk assessment tool at NASA, then it would have been seen as a step of the PRA. The next step was the evaluation of probabilities of component failures based on past failure data and experience and finally the estimation of the system failure probability per unit time or per operation. For this purpose, NASA commissioned two studies to determine PRA feasibility. These studies identified important failure scenarios never identified by previous FMEAs and showed that components with criticality higher than 1 (not taken in consideration for mitigation in FMEA or risk matrix approach) can contribute to 30% of overall failure risk. So it was clear that FMEA could underestimate the risk.
In 1995, NASA performed the first comprehensive Quantitative Risk Analysis (QRA) of all shuttle phases, using Master Logic Diagrams (MLDs), Event Trees (ETs) and Fault Trees (FTs) to evaluate the probability of a major accident as a function of component or subsystems failure probabilities. Since then, NASA included PRA as a decision making tool. [2]

1.2 Risk analysis nowadays

Risk analysis is performed to calculate the potential losses of a system and the components that contribute to such losses. Because space systems have to cope with hostile environment, they are designed as complex, autonomous and intelligent assets, but in this way the demand for risk analysis grew more and more in the last 20 years. In the past, the main way to assure safety was to design systems conservatively to avoid most of the risks occurrence. Although this philosophy assured safety, it also tended to design over-expensive systems. PRA development aided risk and program managers in making design, manufacturing and operation decisions. [4]
Risks can be categorized in several types (health, economic, environmental) but only safety-related risks are subjects of this work. Risk analysis consists of:

1. risk assessment;
2. risk management;
3. risk communication.

1.2.1 Risk assessment - PRA

Risk assessment can be viewed as a combination of:

- scenarios, what can go wrong;
- likelihoods, the probabilities of each scenario;
- consequences, the estimated effects of each scenario;
- relative importance of a single event compared to the other ones.

Generally, PRA should evaluate a set of scenarios, likelihoods and related consequences. A scenario is composed of:

- an Initiating Event (IE), a perturbation out of nominal behaviour;
- pivotal events, successes or failures in response to the IE;
- end states, the possible effects of each scenario, with a different occurrence and severity for each one.

There are two types of risk assessment methodology:

1. qualitative, considers risks in a descriptive way and identify potential causes and effects of each failure, evaluating them with linguistic measures (low, moderate, high) or with fuzzy values;
2. quantitative, likelihoods and consequences are calculated with actual probability distributions and actual losses.

The main scope of PRA is to identify which components are the major contributors to overall risk and to evaluate effectiveness of mitigation actions. That means that PRA could point out design and operational deficiencies in order to improve them. [3,4,5]

1.2.2 Risk management

Risk management and risk assessment are interconnected, in fact the latter identifies risk contributors and the former uses these contributors to implement a control and mitigation strategy that should be monitored over time during design phases. The objective of risk management can be summarized as:

- prevent, control and minimize effects of a risk event;
- evaluate design or operation alternatives to minimize risk probability;
- take corrective actions.

To do so, it can be practical to split out the process into 3 steps:

1. identify which risk contributors influence more the overall system risk;
2. find the best strategy to avert or minimize risk effects (redundancy, testing, maintenance);
3. continuous monitoring over time of the strategy implemented and making adjustments to it when needed. [3,4]

1.2.3 Risk communication

Risk communication includes transfer and exchange of information about risk assessment and risk management between the analysts and the project stakeholders. This involves communicating main characteristics of risks, such as nature, probability and severity, and the benefits that would come with risk mitigation, in particular magnitude and importance of them and the balance between risks and benefits. [3,4]

1.3 PRA tools

There are several PRA techniques to identify risks and quantify their likelihood and severity, some of them are sequencial and others are deductive, the main methodologies are:

1. Master Logic Diagram (MLD) is a top-down scheme to identify IEs and group them according to the effects they cause on the system, at the top there are general system-level undesired events, more detailed ones going down and basic IEs at the bottom. It can show the logical representation of the causes of each failure and map each failure propagation to find causes and effects of it;

2. Event Sequence Diagram (ESD) is a flowchart with each scenario as a path that leads to several end states, it can reperesent well the sequence of operating procedures in case of failure;

3. Event Tree (ET) is the main technique used in PRA for modeling risk scenarios, it's an horizontal structure, that goes from left to right, and describes the sequence of subsystems or components that should fail to bring to a major failure of the system. At the far left there is an IE and for each IE several end states can be evaluated;

4. Fault Tree (FT) is a deductive top-down technique widely used in case of complex systems, It can model hardware and software failures as well as human errors. The Top Event(TE) is the failure event under observation and it can be split out in several lower level events until reached the desired level of detail, the bottom events are called Basic Events (BEs), which probability can be quantified using reliability models such as probability density functions. [3,4]

For some component-level BEs, reliability data could not be complete or applicable if obtained under different operating conditions or environment. So these data should be adopted only to produce a probability distribution of the component: the Bayes' Theorem could be used, it uses a prior distribution related to existing data and updates it with new evidence or information, obtaining a posterior distribution influenced greatly by the level of uncertainty in prior distribution. Sometimes failure rates are uncertain and a method for determining uncertainties should be used: a sampling process such as Monte Carlo simulation. During conceptual design of a new technologically advanced project, there could be an overall lack of detailed data about reliability of components. In that case, other techniques should be used, such as fuzzy theory described in chapter 3.

1.4 Scope of the work

Main objectives of this Master Thesis are:

- to analyze an OOS spacecraft design under a reliability point of view;
- to identify potential failure modes of functions/components in order to prioritize their mitigation;
- to calculate the mission reliability or failure probability;
- to evaluate which component or subsystem influence most mission failure probability and uncertainty.

At first, a functional analysis is required to lay the foundations of the whole work, from which basic functions will be extrapolated and they will be used in FFBD and functions/components matrix in order to establish a time sequence of all functions and to link each one of them to major components of the space tug design.
Once all components are listed in the matrix, a FMECA (Failure Mode, Effect and Criticality Analysis) and a FTA (Fault Tree Analysis) can be performed. The former identifies potential failure modes, causes and effects for each function/component considered and evaluates them with 3 scores based on their Occurrence, Severity and Mitigation (possibility). a RPN (Risk Priority Number) will result from the product of these 3 scores and it signifies that the respective function/component is critical and its mitigation should be prioritized. All functions/components with an high RPN or an high severity score will be listed as critical and inserted in a CFL (Critical Functions List) or CIL (Critical Items List).
Functions/components matrix is also useful to construct a Fault Tree, which is a PRA (Probabilistic Risk Assessment) technique to break down a system into its components. After identifying a Top Event and all Basic Events of the FT, they will be evaluated qualitatively and quantitatively as described in 3.4 and 3.4.2. The result of this analysis will be a failure probability of the Top Event (mission), which will be compared to Electric Propulsion GEO satellites failure probability.
At last, a sensitivity analysis will be performed in order to identify and classify which Basic Events influence the most Top Event failure probability. In this way critical to mission success components will be identified and compared to components listed in CIL in order optimize resource allocation during risk management.

Chapter 2

On orbit servicing

2.1 Historical background

The origin of on orbit servicing missions can be traced back to the Skylab, the first space station in history. In fact, the Skylab had two major failures right after launch in 1973: the thermal and micrometeoroid shield didn't work as planned and the solar arrays failed to deploy. These failures could compromise the mission success, so NASA sent a crew of astronauts to replace the shield and deploy completely the solar arrays ten days after Skylab launch. While this first servicing mission was performed with only Extravehicular Activities (EVAs), Space Shuttle and International Space Station (ISS) performed some robotic servicing tasks.
In 1990, the Hubble Space Telescope (HST) was launched into Low Earth Orbit (LEO) so that it could capture high-resolution images of the universe with lower background light than ground-based telescopes.
Unfortunately, within weeks of the launch, Hubble failed to achieve the high quality images expected in the design phase. The cause of this malfunction was a spherical aberration on the primary mirror, in addition HST experienced a thermally induced jitter from its solar arrays in particular during sunrise and sunset.

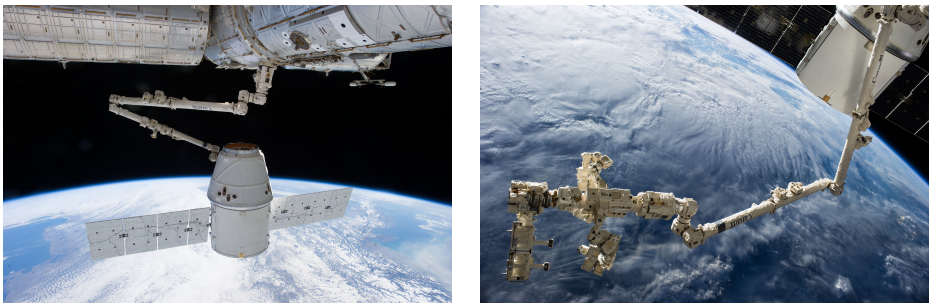
Figure 2.1: Hubble docked to the Shuttle

Nevertheless Hubble was designed specifically for on orbit servicing, in fact every instrument and equipment onboard were easily accessible for repair or replacement. So NASA managed to plan and carry out

a repairing program that would have restored the originally designed capability of HST. In 1993, the so called Service Mission 1 flew aboard the Endeavour with the aim of replace the malfunctioning optics with the Wide Field and Planetary Camera 2 (WFPC2) and the Corrective Optics Space Telescope Axial Replacement (COSTAR).
In this mission, there is a combination of robotic servicing and manned servicing, in fact the robotic arm mounted onboard the Shuttle was used to retrieve HST and dock it to the Shuttle itself. The astronauts worked five days to complete the replacement of Orbital Replacement Instruments (ORIs) and Orbital Replacement Units (ORUs), like the 2 optics, 4 gyroscopes, the solar arrays, 2 magnetometers and other electrical parts. [6]

Figure 2.2: Astronauts during Servicing Mission 1 on HST

Since its launch, Hubble underwent 4 servicing mission until 2009, all of them performed by Space Shuttle astronauts in EVAs and with the aim of improving the telescope and extend its lifetime.
A significant boost to robotic manipulators in space was given by the Space Station Remote Manipulator System (SSRMS or Canadarm 2) and the Special Purpose Dexterous Manipulator (SPDM or Dextre) onboard the ISS. The former can move around the station and is used to grapple and berth unpiloted vehicles visiting the ISS to resupply it, like SpaceX Dragon, Orbital Cygnus and Japanese HTV, and then undock and release them after completion of all tasks. The latter can attach to the Canadarm 2 or MBS or to specific locations of the ISS and is used for "dexterous" tasks, such as removal of damaged components or handling ORUs, that would have been performed by astronauts instead. [6,7]



(a) Canadarm2 berthing Dragon (b) Dextre mounted on Canadarm2

Figure 2.3: Robotic arms onboard the ISS

2.2 Technology demonstration missions

Robotic servicing has been studied theoretically since 1980s, but at that time OOS missions were demanding and some technological fields needed more research, in particular:

- kinematics of a robotic arm in space;
- communication between satellites, in order that a satellite can safely approach another one;
- knowledge of autonomous rendezvous and docking (AR&D) algorithms.

These obstacles were overcome by Space Shuttle missions, completion of GPS constellation, ground tests with robotic arms and ISS teleoperated rendezvous and docking operations.
Starting in the late 1990s, the National Space Development Agency of Japan (NASDA) and the United States Air Force Research Laboratory worked independently at experimental robotic servicing missions. NASDA launched the Engineering Test Satellite-7 (ETS-VII) in 1997, it was composed of a chaser, equipped with a $2m$ robotic arm, and a target satellite. This was the first satellite with a robotic arm and the first successful AR&D experiment. In 2 years of operations, it demonstrated basic technologies for AR&D in all its component parts and also other secondary objectives, such as experiments related to teleoperation, latency and dynamic coordination of the robotic arm mounted on the chaser satellite.
The United States Air Force Research Laboratory built a series of micro-satellites, called eXperimental Small Satellites (XSS), and launched XSS-10 in 2003 and XSS-11 in 2005. The former acquired and tracked its own second stage and navigated around it at from $100m$ to $20m$ of distance to inspect it. The latter demonstrated autonomous proximity maneuvers near well-known US objects and it took several images to inspect them.
These 2 experimental programs demonstrated several technologies, such as autonomous navigation system, teleoperated robotic arms on satellites or R&D mechanism and software , that opened the way to autonomous robotic servicing on orbit. [6]

2.2.1 Orbital Express

Thanks to these technological demonstration, an end-to-end autonomous robotic servicing mission was finally possible: the Orbital Express flight demonstration was envisioned and funded by the Defense Advanced Research Projects Agency (DARPA) and Boeing.
The goal of this program was to test and validate several technologies, such as:

- autonomous operations and servicing software;
- autonomous Guidance Navigation & Control system;
- autonomous capture and docking mechanism;
- zero gravity fluid transfer;
- ORU transfer;
- advanced robotics.

(a) ASTRO's robotic arm capturing NextSat

(b) ASTRO assembled

Figure 2.4: Orbital Express

Orbital Express was launched in 2007 and it was composed of a chaser (ASTRO) and a target (NextSat) in a mated configuration. The mission was divided in several scenarios, to test all its technologies at different levels of autonomy. In fact, during the scenario 0 ASTRO simply transferred hydrazine to NextSat at the lowest level of autonomy, so that ground approvals were necessary to perform every single step of the fluid transfer.

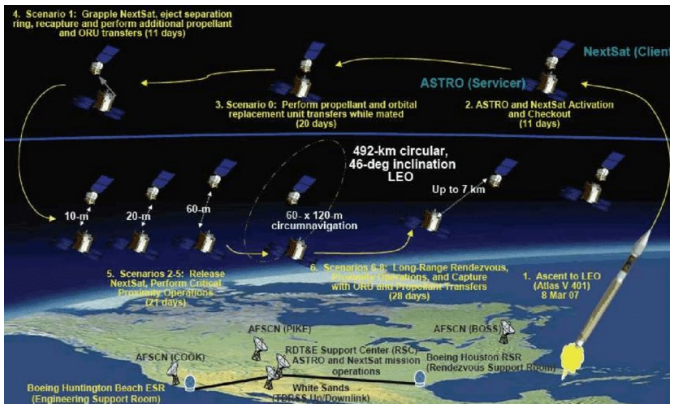


Figure 2.5: Schematic representation of all mission scenarios

The following scenarios increased the level of autonomy and complexity of servicing operations. In fact, scenario 1 started with the ejection of the separation ring that connected ASTRO with NextSat, while the robotic arm mounted on the chaser was grappling the target in a pre-berth position. After separation, ASTRO captured and docked NextSat, thanks to a capture mechanism, and they returned to the mated configuration. At this point, another fluid transfer was performed, with an autonomy level 2 instead. The scenarios that followed were with an higher autonomy level, in particular guidance, navigation, control, fluid transfer, rendezvous maneuvers and capture operations were fully autonomous while ORUs replacements needed ground orders to begin (autonomy level 3). [8]

ASTRO performed several rendezvous with NextSat at different distances, using the Autonomous Rendezvous and Capture Sensor System (ARCSS), that is composed of:

1. narrow FOV acquisition and visible track sensor (VS1), designed to track the target beyond $200Km$ and to provide bearing data of it beginning at range of $5\ Km$ with favorable lightning conditions;
2. mid to short range wide FOV visible track sensor (VS2), used in the final approach to the client in order to keep the entire satellite in the field of view;
3. long wave infrared sensor (IRS), designed to take the place of VS1 and VS2 during nighttime operations or bad lightning conditions;
4. precision laser rangefinder, designed to track NextSat from $7\ Km$.

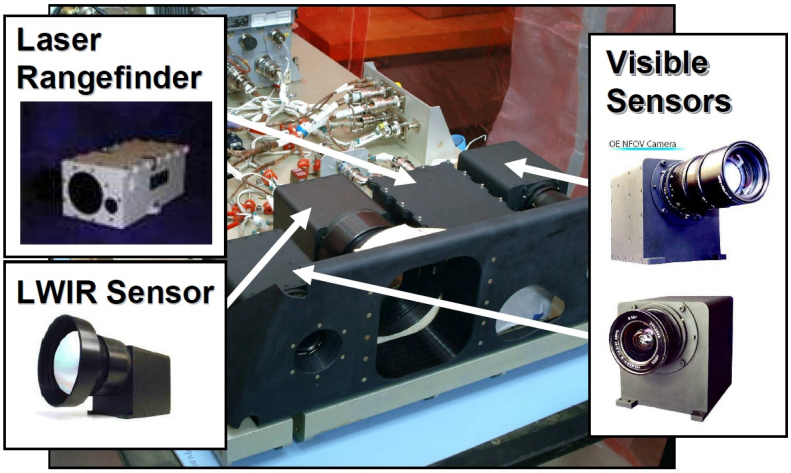


Figure 2.6: ARCSS cameras

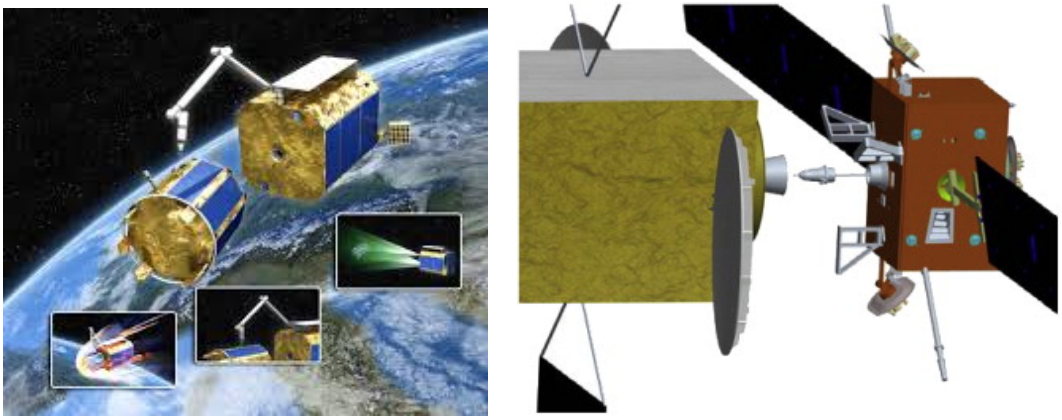
In the final approach corridor (less than $200\,m$), the Advanced Video Guidance Sensor (AVGS) was used to provide 6-degrees navigation data to GN&C system. In addition, the Vis-STAR software determined the passive relative range and attitude of the target, based on the images taken by ARCSS.
In conclusion, Orbital Express was a successful mission that demonstrated the technical feasibility of fully autonomous OOS. [9]

2.2.2 DLR'S robotic servicing projects

From 2007 to 2018, the German space agency DLR had been developing and funding two robotic servicing projects, DEutsche Orbital Servicing mission (DEOS) and Orbital Life Extension Vehicle (OLEV), but unfortunately both of them were canceled after definition phase, due primarily to high production costs. [10]
DEOS consisted of a servicing and a client satellite, that would have been launched together into orbit, and its main goals were to capture a tumbling non-cooperative target satellite with a robotic manipulator mounted on the servicer and eventually de-orbit the mated configuration at the end of life. Secondary

objectives were to test and perform rendezvous, capture and docking operations as well as orbit maneuvers in the coupled configuration. DEOS would have been equipped with both a robotic arm to grapple the target and a docking port to perform a docking with it. [11,12]
The design and development of SMART-OLEV was a European partnership between ESA, several national space agencies (including DLR) and three private companies (Swedish Space Corporation, Kaiser-Threde and Sener). It would have granted life extension to GEO communication satellites close to EOL, taking over their attitude and orbit control functions allowing them to continue their task and produce further revenue even after fuel depletion. SMART-1 was chosen as the most suitable bus, because of its reliability and its Hall Effect thrusters, that were the only way to perform this space-tug task without a significant fuel mass on board the tug. SMART-OLEV could have performed several tasks, such as:

- relocate a satellite in GEO arc, with a small amount of fuel;
- remove inclination from a client satellite, with a significant fuel mass cost;
- rotate the orbital nodes of a satellite in an inclined orbit, with a fuel consumption that is function of the client mass and inclination;
- stationkeeping operations;
- remove the client from its GEO slot at the EOL and bring it to the graveyard orbit 300 Km above GEO. [12,13]



(a) DEOS mission phases (b) SMART-OLEV docking to a GEO satellite

Figure 2.7: Simulations of DLR missions

2.3 Importance and feasibility of OOS

In the last decade, space operators are showing interest in OOS because it can provide flexibility and reliability for their satellites. In fact, the aforementioned demonstration missions proved that OOS is technically feasible and all useful components (such as robotic arm, refuel mechanism, AR&D system) have an high TRL (Technology Readiness Level) and are ready to flight, but there are still issues to discuss:

1. types of servicing required by customers;
2. number and location of possible clients;
3. cost of an OOS mission.

2.3.1 Servicing opportunities

There are thousands of satellites on orbit and each of them has different tasks and goals to reach, but every satellite's owner wants that its space asset could last for all the time it is designed for. Unfortunately, failures and malfunctions can occur and drastically reduce satellite functionality or even prematurely end its operations. So, practical ways to extend lifetime of satellites are to:

- relocate it;
- take control of its AOCS functions;
- refuel it;
- repair it by replacing failed components.

Basically, a failure during launch can happen and it can affect the mission success, in fact the launcher could fail to put a satellite in the right orbit. In this case, it can work in a different orbit or inclination but in a sub-optimal way, with several issues related to different ephemeris and external disturbance forces than the ones for which it was designed. In some extreme cases, the satellite can't perform its tasks at all and it's left unused in the wrong orbit. [14]
A solution for the wrong orbit insertion problem exists and it's a so called *tug boat* that rendezvous and dock to several clients and perform maneuvers to put clients in their right orbit (change of inclination or raising of semiaxis or both). This service can extend satellite lifetime of months or years, depends on how far from optimal situation it was, or can even save the entire mission from failure.
A similar situation can occur when a satellite already on orbit suffers an AOCS failure and loses control of its attitude. It becomes an hazard for other satellites on orbit and a significant money loss for the owner. To fulfill its mission, a servicer can capture it, implement a coupled configuration with it and take control of its attitude with the servicer AOCS. So the tug deals with stationkeeping of the client satellite and enables it to perform its original mission until tug fuel depletion. This kind of solution can be useful in case the client propellant mass is too high and the launch of payload and propellant together too expensive. A tug could perform all maneuvers and save mass aboard the customer satellite, so that it can be launched without propellant on board and even without a propulsion system. [6,14]
About that, there are tens of cases per year of fuel depletion before mission completion and these are caused by several problems such as AOCS malfunctions that force the propulsion system to perform

corrective maneuvers or wrong orbit insertion or need to perform collision avoidance maneuvers. In this case, a multi-client servicer needs to approach each client, perform rendezvous and docking maneuvers and connect the refueling mechanism to the client feed system to refuel it. If the target satellite is non-cooperative, without a refueling port where to insert the servicer refueling probe, the servicer must use a robotic arm and specialized tools to remove safety caps and arrange satellites to fluid transfer. There are already all technologies to fulfill fluid transfers with almost every type of propellant, including cryogenic ones. [15,16]
Currently, when a component of primary importance (on-board computers, engines, batteries, gyros etc.) undergoes a significant malfunction, the satellite can be considered dead and there are two options: leave it there and abandon the mission or launch another satellite to take its place. In this case, it's more simple to replace the entire space asset for low-cost commercial satellites than repair the one already in orbit. However, it cannot be applied for high-cost unique space assets such as observatories, military reconnaissance satellites or space stations, which must be repaired because their scientific or strategic importance is beyond every economic revenue or servicing cost. In addition, beacuse of the increasing modularity in satellite design, a purpose-dedicated servicer could replace entire modules of even low-cost satellites without complex dexterous actions of the robotic arm. [6]

2.3.2 Database of satellites and failures on orbit

A database of on orbit failures must be investigated to understand how broad servicing market could be and which opportunities it offers. Sullivan and Akin report is taken in consideration because it shows a complete point of view on each and every Earth Orbit even if it considers satellites launched between 1984 to 2003.
It begins individuating the number of payloads of interest for this database, counting in every successful launch in those 20 years and filtering out a priori amateur radio satellites, human spaceflight vehicles, satellites exploded on orbit and others.
Considering only GEO satellites, there are on average, per year:

- 1 wrong orbit insertion;
- 13 satellites that relocate themselves using stationkeeping fuel;
- 10 dead satellites that need to move to a graveyard orbit;
- 20 fuel depletion.

GEO satellites have been considered because financial investments vary significantly by orbit. In fact, GEO was far more populated than LEO and MEO and moreover GEO total investment was an order of magnitude higher than MEO one and almost 3 times LEO one. So GEO tends to be a solid market to service.

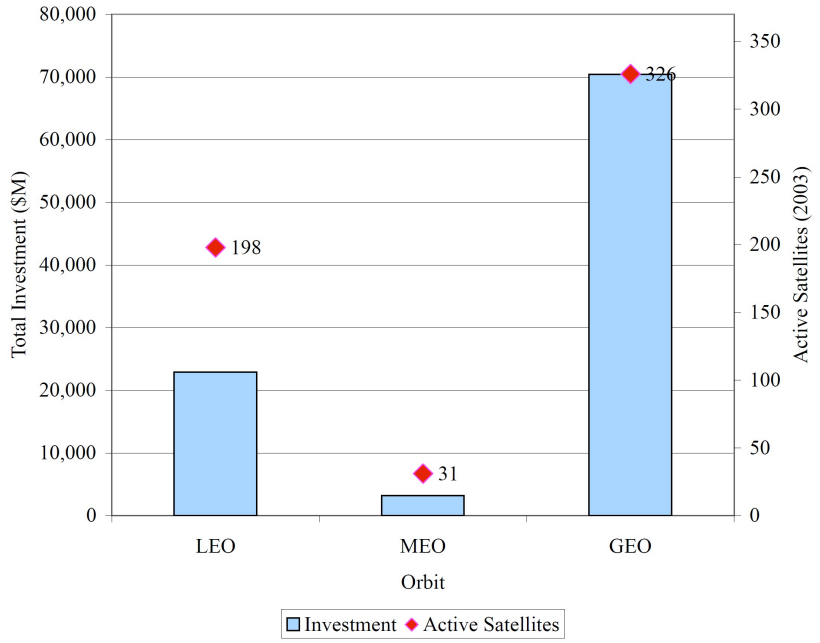


Figure 2.8: Total investment and active satellites by orbit

Performing relocation or rephasing maneuvers can extend operational lifetime of satellites, in particular there is an high potential demand of relocation for GEO satellites with an average of 13 relocations per year.

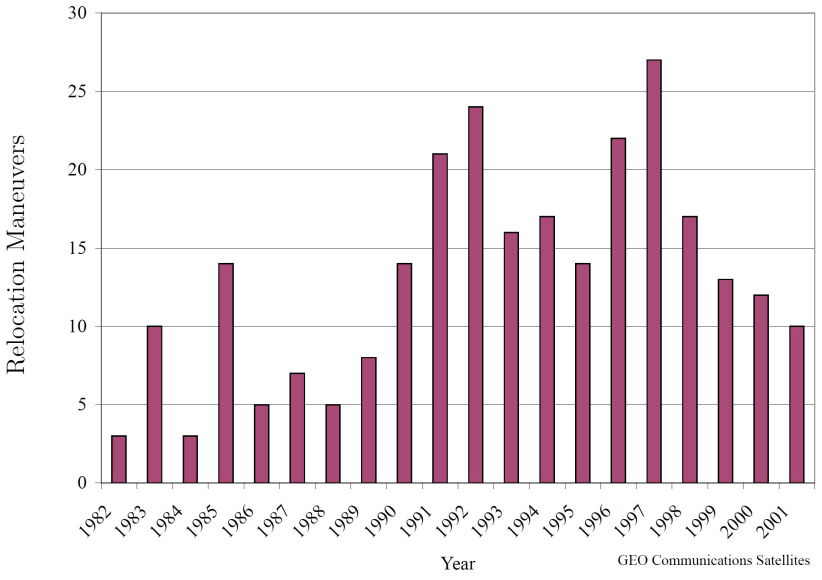


Figure 2.9: GEO relocation maneuvers over the years

To know the total time loss for a certain type of maneuver, it can be calculated first the ΔV required:

$$\Delta V = 5.66\frac{\Delta\lambda}{n}$$

where $\Delta\lambda$ represents the change in longitude and n the number of days spent to perform the relocation. After, fuel mass required for the maneuver m_p can be calculated from the Tsiolkovsky rocket equation:

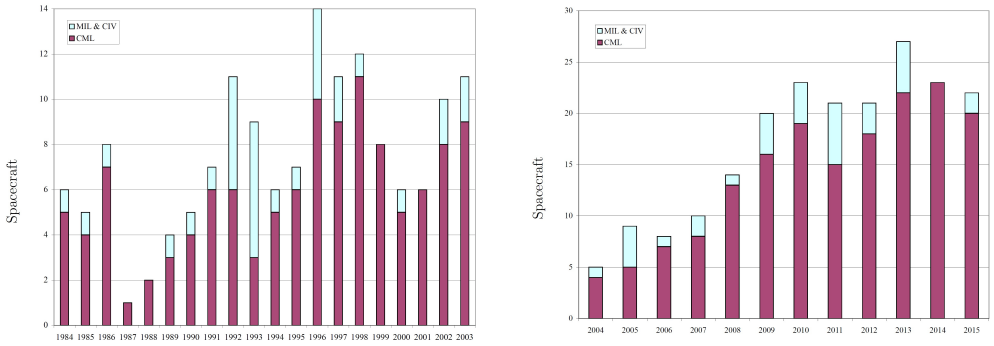
$$m_p = m_i[1 - e^{(-\frac{\Delta V}{I_{sp}g_0})}]$$

where m_i is the initial mass of the satellite vefore the burn, I_{sp} is the specific impulse and $g_0 = 9.81 m/s^2$ is the gravitational constant. A typical GEO communication satellite has a stationkeeping fuel burn rate of $0.16\ kg/day$. The total time loss T_{loss} is composed by n the number of days spent to perform the relocation and $T_{lifetime}$ is the operational time lost to perform the maneuver with on-board propellant:

$$T_{loss} = n + T_{lifetime} = n + \frac{m_p}{0.16\ kg/day}$$

It is found a minimum of 76.4 days for T_{loss} that corresponds to 2.5 months. Considering an average monthly revenue for GEO CommSats of $3.7M\$$, a relocation maneuver could costs at least $9.2M\$$. If a servicer provided at least half of the fuel required, $4.6M\$$ could be saved. Moreover, if 13 relocations per year happened, a servicing relocation mission could save about $60M\$$ per year.

When satellites reach end of life, they must perform a maneuver to move away from GEO to a graveyard orbit at about $300\ km$ above it, to avoid physical and communication interference with other active satellites. A typical GEO CommSat uses an amount of fuel for the retirement operation comparable to the one used in at least 3 months of stationkeeping, equal to $11.1M\$$. Until 2003, there were about 10 retirements per year, but the increasing population in GEO leads to increasingly more satellites to retire. So the trend would probably lead to 15 to 25 decommisionings per year, this means that retirement servicers would save 45 to 75 total months of operations per year.



(a) GEO retirements data for the 20 years interval considered

(b) GEO retirements previsions

Figure 2.10: GEO communication satellites retirements over the years

Considering GEO satellites retired since 1980, they have on average exceeded their design life by 24%, that are additional 1.6 years of potential service, but they reached the end of their stationkeeping

fuel before other primary systems fail, so refueling missions can extend these satellites lifetime beyond their design life. In figure 2.11 the actual life of GEO CommSats versus their design life is represented: satellites before the 31st reached end of life before their design life, the ones after the 31st exceeded their design life instead. The client's revenue for a refueling service is about $44.4M\$$ per year. [14]

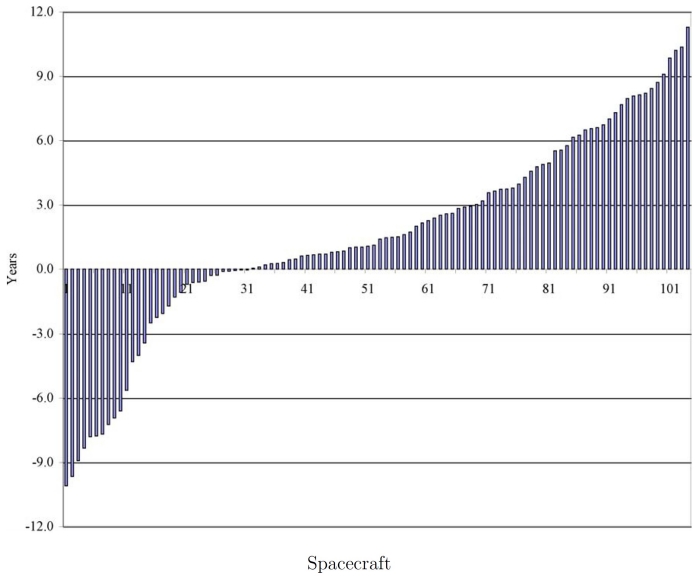


Figure 2.11: Actual life versus design life of GEO CommSats

2.3.3 Cost of an OOS mission

It has been established previously how much a servicing mission could yield to clients in terms of revenue, but it's not completely clear if an OOS mission can be economically viable for the servicer owner. The goal is to understand how much a customer would pay to service his own Commsat, so the cost of the servicer (or *Repairsat*) should be determined as a proportion of the Commsat to be serviced. In particular, the revenue that each service supplies to the client can be considered as the maximum price the customer would be willing to pay to Repairsat's owner and can be taken as the maximum cost of an OOS mission.
A servicer should cost at most 60% of Commsat average cost ($325M\$$) or its owner can't have a return on investment and the mission wouldn't be financially viable. [17]
Six financial scenarios are considered: 3 different years-to-payback periods and 2 discount rates to apply to each period. The former are 5, 6 and 7.5 years to payback as the best case, mid case and worst case scenario, the latter are 3.6% and 6.35%.
Four types of servicing mission are evaluated by the effect they cause on the Commsat and the period of time for which this effect increase satellite's capability and value:

1. SAO, array operations anomalies at the BOL that cause irreparable damage to power production, so the Repairsat mates with the client for its entire life to supply power;

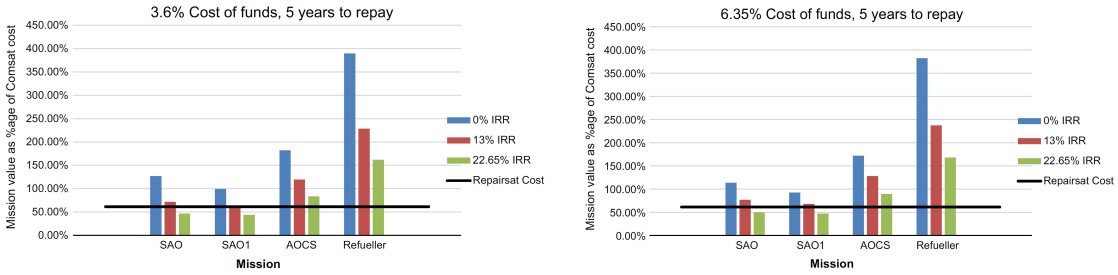
2. SAO1, array operations (covers the 75% of array anomalies) at mid-life, client satellite undergoes power failures that reduce its power capacity by 50%, it's similar to SAO but happens some years after array deployment;

3. AOCS, life extension made by the Repairsat that takes control of Commsat's orbit and attitude at EOL to relocate it and perform stationkeeping for 2 additional years in which its capability increase from about 0% to 100%, the Repairsat can perform up to 5 relocating missions;

4. On-orbit refueling up to 10 refueling operations, each of them extends client satellite's lifetime of 2 years increasing its capability from about 0% to 100%, assuming it at EOL.

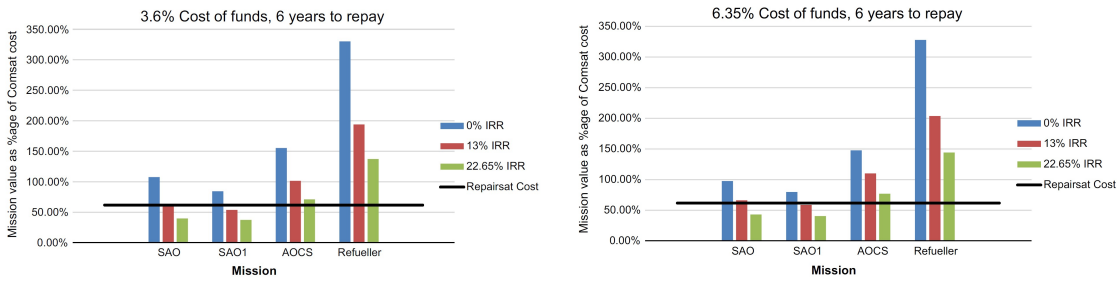
Three financial scenarios are considered for Repairsat's operator:

- zero return, no return on investment, it's the limiting case and the maximum price of the Repairsat;
- 13% return, it's the lowest Internal Rate of Return (IRR) for a Commsat operator and it's the most probable scenario in the future, when servicing will become a mature market;
- 22.65% return, it's the highest Internal Rate of Return (IRR) for a Commsat operator and it's the most probable scenario right now for the rising servicing industry.



(a) (b)

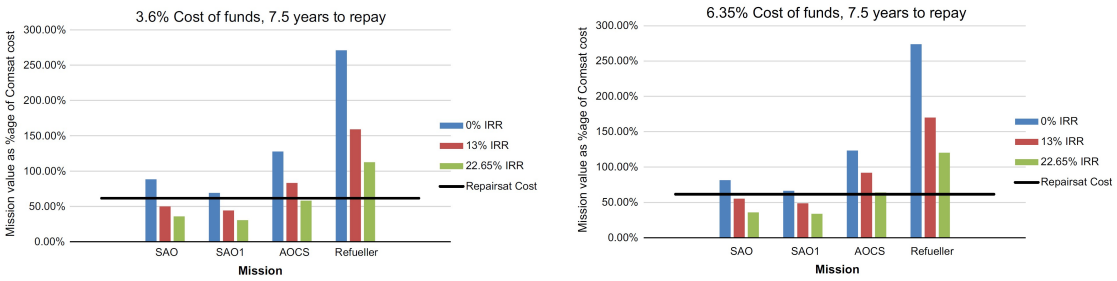
Figure 2.12: 5 years payback



(a) (b)

Figure 2.13: 6 years payback

All 4 missions can be evaluated commercially viable in the no-return scenario for all the payback periods considered, but only on-orbit refueling and AOCS remain viable from 13% profit return on. This means



(a) (b)

Figure 2.14: 7.5 years payback

that a servicing mission should completely restore the target capability to be commercially feasible.
It's clear that a servicing mission could provide the highest revenue to 5 years-to-payback clients, with potential returns on investment of about 350% of Commsat cost in case of a refueling mission (2.12). About that, refueling is the servicing task showing most potential, in fact even in the worst case scenario (2.14) a refueling mission could provide about 120% of Commsat cost and double the Repairsat cost, so that it would be feasible and profitable to perform this servicing mission for both Commsat and Repairsat operators.
In conclusion, servicing missions will focus on refueling and AOCS operations, because these one are, above all the others, the most technically and commercially feasible.

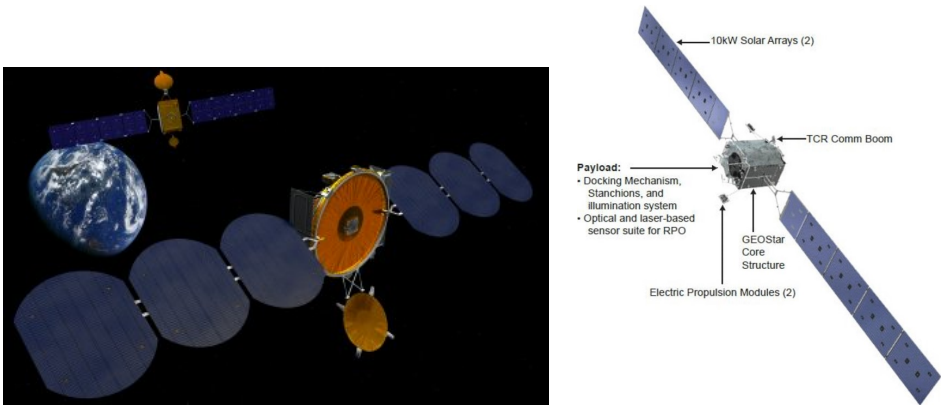
Chapter 3

Case study and methodology

3.1 Space tug mission

The space tug is a widespread concept, that consist of a chaser rescuing inoperative or near-EOL satellites with the aim of extend their working life by means of relocating,taking control of stationkeeping activities or refueling them. Currently, there are several tug design examples:

1. ConeXpress, funded by ESA and Orbital Recovery, performs stationkeeping, relocation and disposal maneuvers for multiple client satellites in GEO;
2. O.Cubed is an Airbus project providing inspection, relocation, stationkeeping, refueling, delivery from GTO to GEO and refueling services to both LEO or GEO customers;
3. Mission Extension Vehicles (MEV-1 and MEV-2) are designed by Orbital ATK, now part of Northrop Grumman, to relocate GEO satellites and perform stationkeeping.



(a) ConeXpress rendering of a rendezvous (b) MEV schematics

Figure 3.1: Space tug designs

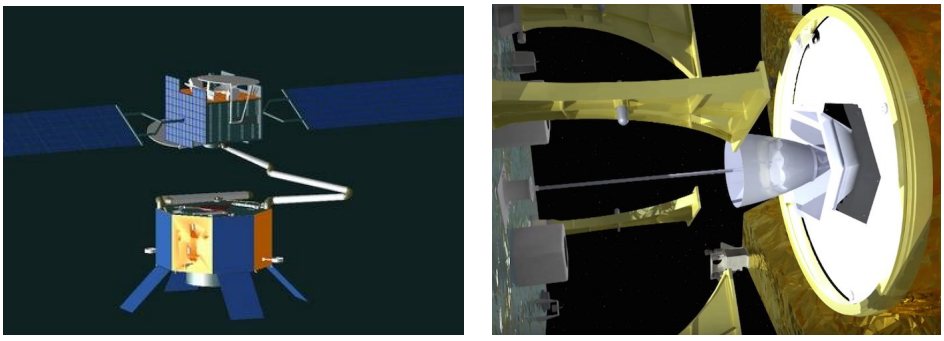
The space tug concept here discussed has some aspects similar to those mentioned above and is based on the work of Cresto, Viola et al.[18]. Main services supported by this tug would be delivery from GTO to GEO, on-orbit relocation, refueling and eventually disposal of EOL satellites. It's intended for GEO

operations mainly but it could perform on-orbit servicing also in LEO. GEO has been chosen as orbit of interest because there are space assets with higher revenues than in LEO.
An important feature of the space tug is reusability, it should service multiple satellites before retirement but it would need to refuel itself to perform several servicing operations. To do so, it's necessary to take in consideration a fuel depot permanently in orbit:

- ISS could work as a spaceport for refueling in LEO;
- an Orbital Tank could be the perfect solution for each orbit of interest but it's costly and complex to put one in orbit.

So a reusable multi-customer tug would be financially possible only if a third space entity provides a refueling asset between each servicing mission.
From the design point of view, the tug would be composed of:

- a 7-DOF robotic arm to grapple and maintain in fixed configuration chaser and client satellites and to perform dexterous operations during refueling;
- a 2-DOF (translational and rotational) capture tool (CT) to dock to customer's apogee engine nozzle when possible;
- an electric propulsion system that consists of 2 Hall Effect thrusters (HET) designed by Sitael and relative Xenon tanks and feed system;
- a conventional GEO platform with subsystems such as Thermal Control, EPS, AOCS, Communication System;
- an innovative GNC subsystem to perform autonomous navigation;
- a fluid transfer system to refuel client satellites with both fuel and oxidizer, liquid or cryogenic;
- an advanced On-Board Computer to autonomously implement recovery strategies and adapt to unpredictable circumstances.



(a) Berthing with a robotic arm

(b) Docking with a capture tool to an apogee motor

Figure 3.2: Docking and berthing alternative methods

A robotic arm and a capture tool are both implemented in the conceptual design to have functional redundancy for capture maneuver, however the latter would be used only for cooperative satellites that have a docking port where this CT fits or an adapt apogee kick nozzle. The former, instead, would be the main grappling mechanism, because it only needs a grappling fixture on the client chassis.
To perform as much as possible on-orbit services taking in consideration fuel saving, Electric Propulsion (EP) is the only option viable. So 2 $5kW$-HET will be mounted on board the tug for transfer phases and relocation maneuvers. Between each servicing mission the tug would need Xenon refurbishment, so it's necessary to design a Xenon refueling system to connect to the orbital tank one.
GNC system is crucial for mission success, especially in a semi-autonomous mission like a servicing one. Main components of this subsystem are sensors and estimating software. The initial identification of the client satellite should take advantage of the continuous ground contact in GEO, so both servicer and customer would be tracked by ground station and client's position and orientation data would be transmitted to the tug. This type of navigation is called absolute navigation and it can be used until relative distance reaches 5 km for safety reasons. [12]
After that, the tug will enter the far range rendezvous corridor (from 5 km to 500 m) in which angles-only navigation should be used. In this case two different sensor could be used: a narrow FOV acquisition and track camera with high resolution and a long wave infrared sensor. The former acquire client position in condition of favorable lighting, the latter provides continuous tracking data also in poor lighting conditions. After processing images, a Kalman Filter would estimate client position and trajectory, so that a line of sight between tug and customer could be determined. [9,12,19]
For mid range rendezvous(from 500 m to 50 m), the main objective is to determine and estimate the pose of the customer spacecraft. To do so, a camera-based relative navigation will be used, that consists of wider FOV mono cameras and 3D sensors such as LIDAR or RADAR. Combining both kind of sensors, a complete 6D pose can be determined using an Extended Kalman Filter, which will make the pose estimation much smoother compared to sensors measurements one. [12,19]
In the close range rendezvous phase (from 50 m to capture), a continuous video contact with the target should be observed, so wide FOV stereo cameras mounted on the robotic arm and in proximity of the capture tool will be used in combination with an infrared sensor or an artificial illumination.
The space tug mission scenario consist of 10 phases:

1. post launch system check, in which solar arrays and antennas are deployed, all subsystems are checked, communication link with ground is established;

2. transfer from GTO to GEO, in which the thrusters are fired to perform a eccentricity change maneuver to raise perigee and optionally it could include a delivery service for a wrong orbit insertion client satellite;

3. arrival at the parking orbit in GEO, where to refuel from the Orbital Tank and wait until next servicing mission;

4. transfer to customer GEO slot, performing an in-plane or inclination change maneuver to reach it;

5. rendezvous with the satellite to service, in which perform image processing and pose estimation of it;

6. capture the client satellite, in which robotic arm and/or capture toll are used to berth/dock to it and make a stacked configuration;

7. servicing the satellite, in which the tug refuels and/or relocate the satellite in accordance with its owner request;
8. unberth/undock and move away from the client satellite safely preventing debris creation or damage to both the spacecrafts;
9. return to parking orbit to refuel and then start all over again;
10. at the EOL of the tug, it must reach a graveyard orbit 300 km over GEO for disposal.

3.2 Functional analysis

Functional analysis has a significant role in the conceptual design methodology of a space mission. It is considered as a process of identifying, describing and relating all the basic functions a system has to fulfill to accomplish the mission objectives, which can be derived from the mission statement.[20] The mission statement is a brief description of a company, agency or single mission that outlines:

- goals and purpose;
- market target or customers;
- the way to reach the goal.

The mission statement for the reusable space tug mission is "To extend the working life of both private and government satellites by means of refueling and relocating them in the appropriate orbit".
Generally, mission requirements should be written down right after mission statement and objectives definition, then a system architecture can be derived from the requirements.[21] In this particular case, a functional architecture is developed after objectives definition, without requirements definition, in order to draw out all the functions the system must perform to evaluate possible risks for each one. Main outputs of this section are:

1. functional tree, a top-down definition of system functions from top level to basic ones;
2. functional flow block diagram (FFBD), a functionally oriented sequence of events;
3. functions/components matrix, which correlates functions identified in the functional tree with devices that can properly perform them.

3.2.1 Functional tree

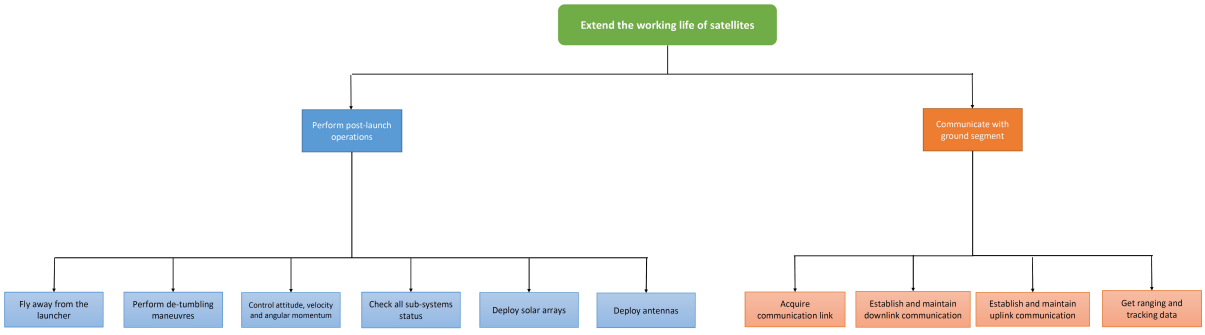


Figure 3.3: Functional tree example of the space tug mission

The first step is to produce a functional tree, starting from top-level functions and decomposing them into simpler lower-level subfunctions in various branches.[22] Each function should be written in the most simple and general way possible: they should be composed of verb and noun and they should be described with as much generality as possible, although this is easier to do for high-level functions than lower-level ones.

Decomposition of functions should be performed from the top of the tree to the bottom asking "how" and from the bottom to the top asking "why". This process stops when the desired level of detail is reached.[21]
In this way, each function of the future mission is identified and the last building blocks of the functional tree are called basic functions and they will be the starting point of the Failure Mode, Effect and Criticality Analysis (FMECA). Moreover, after basic functions identification, functional requirements could be defined, although this is not part of this Master Thesis work. The functional tree is a functionally oriented representation of the mission, so it does not consider the physical view, like a product tree would do.

3.2.2 Functional Flow Block Diagram

The second step consists in making a time sequence of all functions identified in the functional tree, from the top to the bottom of it.
To do so, the functional events described in the previous phase become functional blocks, with a label consisting of a numbering scheme to identify and relate each function to its higher and lower levels. FFBDs are a natural consequence of functional trees, so they are still functionally oriented and not solution oriented, as they express the event itself and not the way to accomplish it.[22]
FFBDs must take trace of relationships and origins of each function, to do so they can be performed:

1. on different layers, that stand for each level of detail;

2. or in a single diagram, where every lower-level function are incorporated in their "parent" function.

The second option has been chosen due to its consistency.

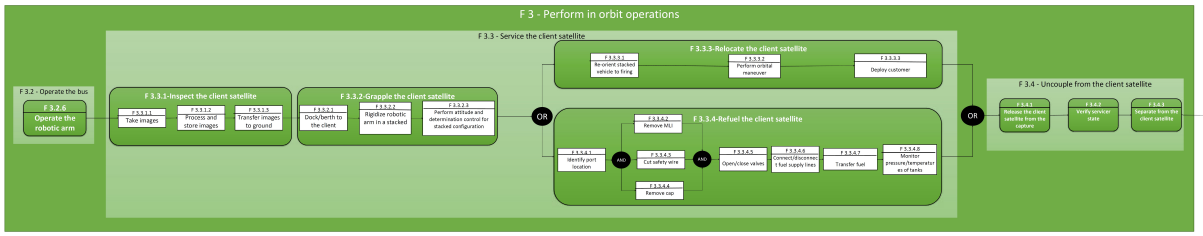


Figure 3.4: FFBD example of the space tug mission

There are 3 considerations about figure 3.4:

1. arrows represent functional flow through the diagram and their direction is conventionally from left to right;

2. each line does not indicate lapsed time between functions but only succession between those functions, so that inputs and outputs for each one are shown;

3. circles represent summing gates, such as AND, OR, GO, NO GO, IT (iteration), RP (repetition) or LP (loop), in particular AND implies that all parallel functions must be accomplished to proceed, while OR implies that alternative conditions can be satisfied to proceed. [23]

3.2.3 Functions/components matrix

The third step consists of connect the basic functions identified at the bottom of the functional tree with a component or device that can perform the corresponding function. The so-called functions/components (or functions/devices) matrix is built by putting all the basic functions in a row and by matching each one of them with one or more devices that can carry out the duty described. So the upper row is filled with functions while the first column will be filled with devices by means of asking "which component is able to perform that function". Each component could perform more than one function and each function can be carried out by several components, so there isn't a unique matching in this matrix. This matrix aims to map all necessary components and to exclude unnecessary ones. [21,24]
A progressive approach is used to fill this matrix:

1. alternative devices that can perform a function are identified using as references [9,15,18,25,26,27,28,29];
2. if there are more solutions, the most feasible one is considered and listed in the devices column;
3. if a device can carry out multiple functions, it will be listed to match all the functions performed;
4. new devices will progressively fill their column and all necessary components will be identified.

Subsystem	Functions / Components	Receive ground orders	Plan trajectory path	Get state vector measurements	Determine present position and trajectory	Estimate future position and trajectory	Control trajectory changes	Produce/store energy	Convert energy into electrical power	Regulate electrical power	Distribute electrical power	Identify port location	Remove MLI	Cut safety wire	Remove cap	Open/close valves	Connect/disconnect fuel supply lines	Transfer fuel	Monitor pressure/temperature of tanks
Comms	Antennas	x																	
	RF network	x																	
	Transponders	x																	
GNC	GNC processor		x		x	x	x												
	Star trackers			x															
	Sun sensors			x															
	GNSS receiver			x															
Propulsion	Thruster orientation mechanism						x												
	Hall Effect thrusters						x												
EPS	Solar arrays							x	x										
	Batteries							x											
	Power peak tracker (PPT)									x									
	Switch-mode regulators									x									
	Cabling										x								
	Switching gears										x								
	PCDU (Power Conditioning and Distribution Unit)									x	x								
Refueling servicing subsystem	Stereo cameras											x							
	Wire cutter tool												x	x					
	Safety cap tool														x				
	Nozzle tool															x			
	Active coupling																x		
	Bellows																x		
	Transfer hose																	x	
	Fuel transfer tank																	x	
	Variable flow rate gear pump																	x	
	Flow sensor																	x	
	Propellant transfer management processor																	x	x

Figure 3.5: Example of a function/components matrix of the space tug mission

3.3 Functional FMECA

In space projects, reliability is considered a fundamental part of the concurrent design nowadays, because if space assets underwent some failures that undermine their functionality or put prematurely end to their mission, it's really difficult to restore proper functionality on orbit and financial loss could be extremely high. Considered the above, reliability analysis has to be performed in all design phases, in particular during early concept design phase when it can identify potential problems and prevent them before design implementation. [30,31]
The Failure Mode Effect and Criticality Analysis (FMECA) is a widely used reliability analisys tool that allows to identify potential failure modes, causes, effects and severity of a product or a mission in the initial stages of its development. In particular, it's called Functional FMECA when performed during phase 0/A with only functions describing the mission/product and in these phases would have more impact on the final product because major changes are still possible in these phases than later on during the development. Nevertheless, FMECA is an iterative process during all product life cycle so that all potential failures can be identified and corrective actions can be taken. [30,31,32]
Principal scope of a FMECA is to understand:

1. how failures can happen;
2. why failures occur;
3. which component/function fails;
4. the consequences of each failure;
5. the severity of each failure;
6. how to avoid or mitigate failures.

FMECA is a bottom-up methodology, so it analyzes the lowest level functions/components possible and identifies each failure mode, cause and effect at that level. After that, the process should be iterated to the next higher level until top level functions, so FMECA is an inductive synthesis process.
To perform a Functional FMECA all basic functions need to be identified and classified, so a functional tree and an FFBD are developed as mentioned above. Subsequently, a FMECA worksheet has to be completed. It should include at least:

1. an identification number and a brief description,verb noun phrase, of each function;
2. all potential failure modes are postulated for each function;
3. causes and a probability of occurance ranking of each failure;
4. potential local and end level effects of each failure and a severity ranking;
5. mitigation factors that could detect, prevent or mitigate the impact of a failure and a mitigation ranking;
6. Risk Priority Number (RPN), that comes from the moltiplication of occurance, severity and mitigation ratings;
7. any recommended action considered to minimize the risk. [30,32,33]

A failure mode is the way a part can fail to operate, in case of functional FMECA the failure mode is often described as an "anti-function" or using basic failure conditions, such as:

- unscheduled operations;
- fail to operate when required;
- fail to cease operation when required;
- over or under performing;
- malfunction during operation;
- impossibility to operate at all.

Obviously a function or a part can fail in several different ways and each of these way has a specific cause such as mechanical, electrical, software, incorrect design or wear out. Each failure mode has a probability of occurrence, that is determined by previous failures on similar missions and by risk analysis team expertise. So occurrence ratings tend to be subjective, like severity and mitigation ones.In this case, a scale between 1 and 4 is used, where 1 stands for a very low probability of failure and 4 represents an almost certain failure. If two different teams performed a FMECA of the same mission/product, they would probably use different rating scales and ratings but would obtain similar results in terms of RPN and critical functions/items identified. [30]
The failure effect can be considered as the worst potential consequence of each failure mode and its propagation through higher levels until mission level (end effect). Different failure mode could have same effects. To evaluate the consequences on mission success a severity rating is used with a scale between 1 and 4 again, where:

- 1 stands for a minor damage, almost insignificant loss of mission objectives;
- 2 stands for a major damage, a significant loss that can lead to a degradation of mission objectives or a minor loss of time;
- 3 stands for a critical damage, loss of one or more mission objectives or a significant loss of time;
- 4 stands for a catastrophic damage, loss of mission. [33,34]

Mitigation factors are workarounds for potential failures and must be taken in consideration during design phase. Possible factors are redundancy (functional or backup components), reliability of choosen components, ground intervention during operations in orbit and so on. Mitigation scale is from 1 to 4, where 1 stands for an high mitigation capability and 4 no mitigation possible, but the latter ranking won't be used in this case because the space tug will perform operations already tested on orbit and will use design solutions with high TRL.
RPN is calculated by the moltiplication of occurrence, severity and mitigation ratings and represents an indicative factor of risk. In fact, the larger this number is, more critical the respective failure mode would be. Failure modes with RPN>8 would be considered as critical risk, so a list of most critical functions/parts will be drafted to highlight those operations where corrective actions must be taken first. In this list all failure mode with a severity ranking equal to 4 will be included even if their RPN<9, because those failures would impede mission completion. Last but not least, recommended actions or other notes will be identified in order to suggest design changes to prevent or minimize the risk of each failure

mode. Obviously, corrective actions of critical functions/parts will be prioritize in the next design phase. [30,33] FMECA methodology is widely used because it offers several applications such as reduction of development time and cost, selection of an optimal design, identification of critical components and diagnostic procedures to overcome potential failures. It's also very easy to learn and implement for almost all kind of systems, even complex ones. Nevertheless, it's time and resource-consuming and not very useful during advanced design phases where only minor design changes can be implemented. Moreover, it doesn't take in consideration human errors that don't cause directly equipment or operation failures and it only analyse on failure at a time, so combinations of failure are excluded from this analysis. [30,31]

					Potential Effects of Failure						
ID	Function	Potential Failure Modes	Failure Causes	Occurence	Local Effect	End Effect	Severity	Mitigation Factors	Mitigation	RPN	Recommended Actions
1.5	Deploy solar arrays	Total failure of deployment mechanism	Mechanical	1	Inability to deploy solar arrays	No power production, lost of mission	4	Reliability	3	12	Ground test on deployment mechanism
3.2.1.3.1	Stabilize the tug	Gyros or reaction wheels failure	Wear out, poor lubrication of bearings, electrical	2	Uncontrolled spinning	Possible lost of mission	4	Redundancy	1	8	Use of both gyros and reaction wheels or dual-fail redundancy of one of them
3.2.3.3	Dissipate extra heat fluxes outside the tug	Radiators failure	Wear out, mechanical	2	Overheating	Degraded performances and possible loss of mission	3	Redundancy and change in operations	1	6	Louvers can be used outside radiators to enhance their dissipation capability
3.2.5.4	Distribute electrical power	Wiring failures	Electrical, short circuit, wire cut	2	No power to a subsystem	The subsystem can't work	3	Redundancy, fault isolation	1	6	Use of redundant wiring and fuses to open the failed circuit and make it unusable
		Command processor failure	Electrical, software	2	No power to all subsystems	Lost of mission	4	Redundancy, reboot the processor	1	8	Put the tug in safe mode to reset distribution computer
3.3.2.1	Dock/berth to the client	Grappling mechanism failure	Mechanical, software	2	Inability to berth to the client	Lost of mission	4	Reliability, functional redundancy	2	16	Ground testing, provide the tug of an alternative way to mate the client, such as a docking mechanism
3.3.3.1	Re-orient stacked vehicle to firing position	Gyros or reaction wheels failure	Wear out, poor lubrication of bearings, electrical	2	Incorrect pointing	Minor loss of time	2	Redundancy	1	4	Use of both gyros and reaction wheels or dual-fail redundancy of one of them
4.1.1	Use on board data	Communication or relative navigation system failure	Electrical, software	2	Inability to get customer position data	Lost of time	3	Functional redundancy	1	6	Use different methods to get customer position, such as ground data from customer's owner and GPS data from the customer itself
		Processing malfunction	Software	1	Inability to process data correctly	Lost of time	3	Ground intervention	2	6	Send raw data to ground station to process them

Figure 3.6: FMECA example of several space tug functions

3.4 Fault Tree Analysis

3.4.1 Fault Tree construction and qualitative analysis

Fault Tree Analysis (FTA) is a top-down deductive qualitative technique in which an undesired event called *Top Event* is broken down into its causing *intermediate events* and *Basic Events* (BE) and the TE is analyzed in order to find all the possible ways in which it could occur. The fault tree is tailored to the TE, that is usually a system failure or loss of mission, so it should include only events that cause or contribute to the undesired event. [3,4,35]
A FTA needs to follow several steps in order to be correct and successfull:

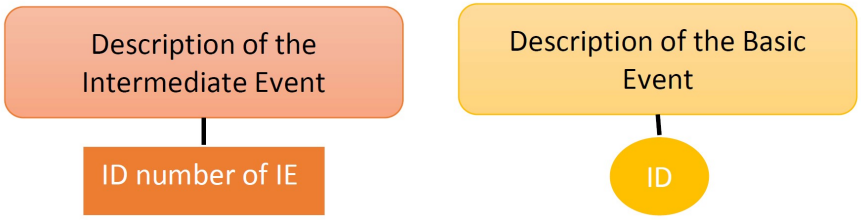
1. identification of objective and top event;
2. definition of scope, resolution and ground rules;
3. construction of fault tree;
4. qualitative evaluation;
5. quantitative evaluation;
6. interpretation and presentation of results.

The first step consists in deciding the objective of the analysis, that usually is a system/subsystem failure or Loss of Vehicle/Crew/Mission (LOV/LOC/LOM), and this choice define consequently the TE of the fault tree. This study case aims to evaluate a space tug OOS mission reliability so Loss of OOS Mission is identified as TE of the fault tree.
The second step is made up of 3 sub-steps that should be performed at the same time to set boundaries to the construction of the FT. Defining the *scope* of the analysis means to point out which failures and risk contributors will be included and which won't. In the study case, only the servicing space asset will be taken in consideration, so launcher, ground segment and project management will not be analyzed. The FTA will focus on space tug subsystems and components and the level of detail (or *resolution*) up to which search for failure causes will be set at major components such as solar cell, robotic arm, thruster and so on. FTs are generally developed to a level of detail where failure data are available or, in this case, where a group of experts can unequivocally judge the possibility of failure of each component. In advanced design phases, FTs are further developed to subcomponents and parts level of detail to improve the reliability analysis, but as this study is analyzing an early design phase, a further development of the FT would be time consuming and counterproductive. To produce an understandable FT it's necessary to implement *ground rules*, which include procedures for FT construction and the nomenclature of events and gates. 3 general ground rules will be followed:

1. events should be written as fault statements, that should highlight which component fails and possibly in which way;
2. FT should be developed in levels and each level should be completed before passing to a lower level;
3. gate inputs should be fault events and gates should not be directly connected to other gates.

After laying the foundations of the FT, the next step is the actual construction. The basic paradigm in FT construction is "think myopically", that means that just the *necessary and sufficient immediate events* which cause a certain event should be investigated. So it's recommendable to take little steps backwards from the Top Event through Intermediate Events without reaching immediately basic causes, in this way all the causal relationships between components will be identified. FT logic model is basically composed of Events and Gates, that can vary according to the type of FT chosen. In the study case, Standard Fault Tree (SFT) will be chosen for simplicity, so it implies that only these Events and Gates will be used:

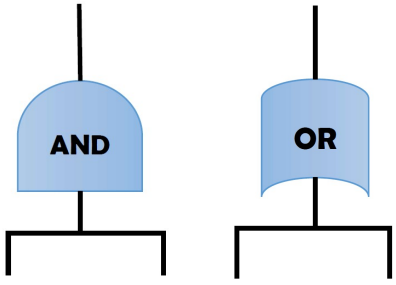
- *Basic Events* are initiating failures that don't require any further development, they are the lowest level of resolution in the FT and are represented by a circle;
- *Intermediate Events* are failure caused by logical combination of other (Basic or Intermediate) events at a lower level and their combination cause the *Top Event* occurrence, both Intermediate Events and Top Event are depicted by a rectangle;
- **AND** gate represents a causal relationship between its inputs and output, in fact the output event occurs if all input events occur;
- **OR** gate shows how the output event occurs if at least one input event occur, input events can be developed as restatements of output event or, if the output is a subsystem, the OR gate can be viewed as a breakdown into its components. [35,36,37,38]



(a) Intermediate Event schematic representation

(b) Basic Event schematic representation

Figure 3.7: Examples of events in FT



(a) AND gate

(b) OR gate

Figure 3.8: Examples of gates in FT

Starting from the TE, FT construction continues its development further down the tree by means of deductively determine the causes of higher level events, until reaching the lower level of detail predetermined, where failure data are available.
To fully evaluate FTs both qualitative and quantitative techniques are necessary. The main qualitative one consists of reducing all BEs causing TE to occur to cut sets, that are collections of BEs that if they simultaneously occur they certainly cause TE failure. In particular, *Minimal Cut Sets* (MCS) are important in order to provide information about system vulnerabilities, they are evaluated by application of Boolean algebra to FT logic model in order to reduce it to the simplest form possible that is MCS.
Quantitative analysis techniques can be divided into *stochastic* and *importance measures*: the former can provide failure probabilities of BEs and after that determine failure probability of TE and system/mission reliability, the latter can identify which BE or MCS contribute the most to the failure probability of TE. This part of the analysis will be further explained in 3.4.2.

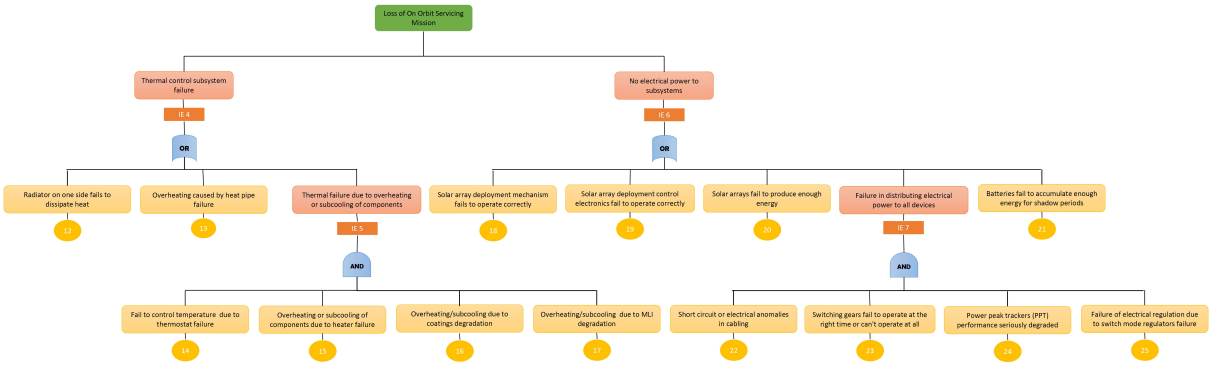


Figure 3.9: Example of a Fault Tree

After these analysis FTA can be considered concluded, but there is a last step fundamental in order to present results to decision makers of the mission analyzed: interpretation and presentation of results. In fact, FTA as it stands is just a huge amount of numerical values, that could be difficult to comprehend for decision makers and mission managers. So linguistic explanation of results must be given in order to support the numerical report and important results, such as major contributors to failure probability of TE, should be highlighted in order to be easily identified. [35,38]
FTA is just one PRA technique and like the others has pros and cons. FTA plays a fundamental role in risk management, in particular:

- it identifies logic relationship between events and across subsystem boundaries that cause the Top Event and in this way it's possible to identify subsystem interaction that can impact redundancy and also detect components of whose only failure would bring to occurrence of TE;
- it helps to prioritize risk contributors causing the Top Event thanks to the importance measures, in such way resources (time and money) can be allocated adequately to minimize failure probabilities of major risk contributors and they can be relaxed for unimportant contributors with negligible changes to TE probability;
- it can be a proactive tool used to monitor and upgrade or correct vulnerable subsystems before TE

occurs;

- it can be used as a decision tool to determine design alternatives that can satisfy performance requirements;
- it can be used as a diagnostic or corrective tool to identify the logic relationships and the BEs that lead to the occurrence of TE when the TE is already happened or is still happening. [35]

As it can be seen, FTA has different uses and many advantages throughout all life cycle, nevertheless it has several limitations especially for modern complex systems. In fact large systems could be composed of a great amount of devices and software, so the dimension of the fault tree can become larger and larger if all the system is analyzed, which brings to an extremely time consuming analysis.
Moreover modern space assets are considered dynamic in nature, that means that when a partial failure occurs, the system can mitigate it by switching instantly to redundant components or correcting it by self-repair. This implies that the system has a dynamic behaviour that can change according to its mode of operation and it brings more uncertainty into the analysis. SFTs can't handle dynamic behaviours of components, so for more detailed analysis in advanced design phases *Dynamic Fault Tree* (DFT) or *Temporal Fault Tree* (TFT) should be used.
FTA is considered a subjective technique in that it relies on the analyst's experience and knowledge of the system considered, so it can vary basing on the analyst and it can't be considered as an objective and exact technique at all.
At last, failure data of BEs can present inaccuracy and uncertainty so they can contribute to an overestimation or underestimation of failure probability of the TE if not treated adequately.
Nevertheless SFT method has been selected and considered adapt for the study case for the following reasons:

- the TE analyzed is limited to a single space tug, that does not include launch, ground, production and management segments, so even if it's a complex system, the resulting FT won't be as large as it would have been including all mission segments and time consumption can be considered negligible;
- an OOS spacecraft is surely a dynamic system and its dynamic behaviour should not be neglected during Probabilistic Risk Assessment, nonetheless this work aims to evaluate its reliability in an early design phase where functional dependency between components is still unclear, but it will be an important step for future work, however functional and component redundancy can be implemented in SFTs;
- subjectivity is a key factor of the whole work and it can't be eliminated;
- using ranges of fuzzy failure possibilities can partially solve the problems of inaccuracy and uncertainty of crisp exact values for failure data.

In 3.4.2 the use of fuzzy failure possibilities will be further discussed.

3.4.2 Fuzzy quantitative reliability analysis

The objectives of this section are to:

1. obtain failure probabilities of each Basic Event at the bottom of the Fault Tree;
2. perform a quantitative analysis on the Minimal Cut Sets and the Top Event of the Fault Tree;
3. evaluate contribution of each BE or MCS to the TE failure probability using importance measures.

Since the failure probability of the TE is a function of failure probabilities of each component, the first step in the quantitative analysis is to estimate or obtain failure data for each component. The conventional approach to this issue consists in obtaining failure rates, probability distributions or other numerical data related to the failure behaviour of a device. There are several handbooks and reliability databases that contain past failure data, especially of electronic devices, but they are not updated with new technologies and so they are inconsistent with the design of technologically advanced systems. When consulting these databases, it's important to check for failure data of the same component in the same environment specified in the mission considered, otherwise the analysis could lead to incorrect results. Alternatively, similar device in the same environment or same device in similar environment can be considered taking uncertainties into account.
Moreover the Fault Tree Analysis should be performed in the early design phases to be effective and in these phases there could be only a partial knowledge of the system or the environment in which it should operate, so a partial understanding of the process could lead to an incorrect estimate of system reliability. To overcome this difficulties, fuzzy fault trees were introduced by Tanaka et al. [41] and the use of fuzzy numbers for failure probability represents an uncertainty because,rather than specifying an exact number, they are a range of possible values which contains the correct value. In several industrial applications such as nuclear power plants, aerospace systems or pipelines, the use of fuzzy set theory caught on in the last decades by means of experts' judgment elicitation. A set of experts will subjectively evaluate failure possibilities of basic events using qualitative linguistic terms, such as "low", "moderate" or "high". [39,40,42,43,44]
However it's necessary to translate linguistic expressions into fuzzy failure possibilities to perform a quantitative analysis. In other terms, every linguistic opinion should be mapped into a membership function, usually a triangular or trapezoidal one. A failure probability distribution should be defined in order to convert every expert's opinion into membership functions of fuzzy numbers. Taking triangular fuzzy distributions into account, a triangular fuzzy number may be expressed by a triplet (a_j, b_j, c_j) where a_j is the lower boundary, b_j is the average and most likely value and c_j is the upper boundary. A generic membership can be written as:

$$\mu_j(x) = \begin{cases} \frac{x-a_j}{b_j-a_j}, & for\ a_j < x \leq b_j \\ \frac{c_j-x}{c_j-b_j}, & for\ b_j < x < c_j \\ 0\ otherwise \end{cases} \tag{3.1}$$

Each BE failure possibility and membership function can be considered as a subset of the interval $[0, 1]$, so it's necessary to subdivide this interval to convert linguistic terms in clear numerical ranges. In [45,46] it's theorized that the optimal human memory capacity number is 7 ± 2, so the suitable range of numbers for linguistic term selection for human experts is $[5, 9]$. In this work, 7 linguistic expression will be used to judge BE failure possibilities: {*very low, low, reasonably low, moderate, reasonably high, high, very high* }. Each linguistic expression is represented as a triplet of fuzzy numbers and in particular:

Linguistic expression	TFN(a,b,c)
Very low	(0, 0.05, 0.1)
Low	(0.08, 0.15, 0.23)
Reasonably low	(0.21, 0.31, 0.41)
Moderate	(0.39, 0.5, 0.61)
Reasonably high	(0.59, 0.69, 0.79)
High	(0.77, 0.85, 0.92)
Very high	(0.9, 0.95, 1)

Table 3.1: Conversion of linguistic expressions into Triangular Fuzzy Numbers

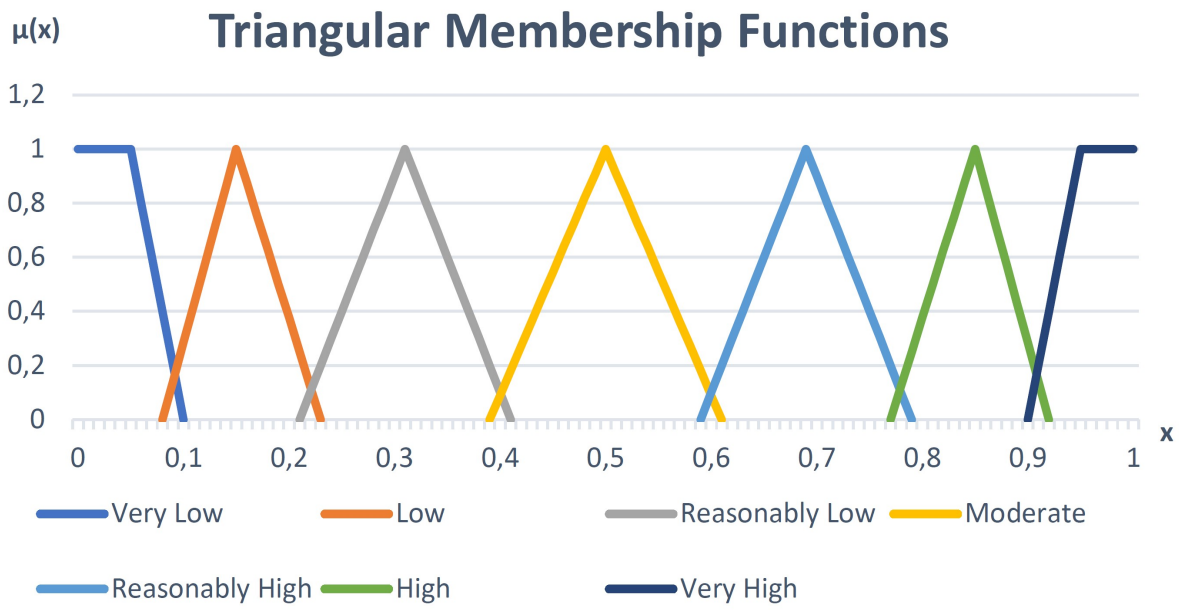


Figure 3.10: Graphical representation of Triangular Fuzzy Numbers membership functions

After converting all experts' judgements in triangular fuzzy numbers (TFN), they have to be aggregated into a single TFN for each BE. To do so, experts' experience and knowledge of the system and the environment in which it should operate will be evaluated to determine the relative quality of each opinion.[39,47]
An expert is a person who is familiar with the system under analysis, understands the system environment and has training in and knowledge of system operations. Since experts may have different levels of experience and expertise and they evaluate basic events failure probabilities relying on their own knowledge about each component, they could have different perceptions of the same issue and they could provide different linguistic assessments. For this purpose, it's necessary to aggregate each expert's opinion using weighting factors to account for relative reliability and quality of each expert's opinion. To do so, 3 weighting criteria are established:

Title or Profession	Score	Professional experience	Score	Educational or technical qualification	Score
Professor, Chief Engineer, Director	5	20+ years	5	Ph.D.	5
Assistant Professor, Senior Engineer, Manager	4	between 10 and 20 years	4	Master degree	4
Junior Engineer, Factory inspector	3	between 5 and 10 years	3	Bachelor degree	3
Technician, graduate apprentice	2	between 2 and 5 years	2	ITI diploma	2
Operator	1	<2 years	1	Diploma	1

Table 3.2: Weighting criteria and scores for experts

- title or professional position, such as professor, chief engineer, junior engineer;
- professional experience in years;
- educational or technical qualification, such as master, bachelor or technical secondary school diploma.

For each criteria, scores from 1 to 5 will be assigned, then the 3-criteria scores will be summed for each expert to obtain a weighting score. The sum of all weighting score will be calculated and the weighting factor of each expert can be calculated by a simple relation.

$$w_i = \frac{WS_i}{WS_{tot}}$$

Where w_i is the weighting factor of the i-th expert, WS_i is the weighting score of the i-th expert and WS_{tot} is the sum of all WS_i. Thanks to these factors, aggregation of experts' opinion would not neglect their experience and knowledge of the issue. [43,44]
After collecting all experts' opinion , a problem still remains: there are n experts' opinion (EO), in form of triangular fuzzy numbers, for each of the m BEs. An aggregation of these EOs becomes necessary to obtain a unique TFN for each BE. Considering an heterogeneous group of experts, a linear opinion pool approach can be used:

$$P_j = \sum_{i=1}^{n} w_i EO_{ij} \quad with\ j = 1, 2, ..., m$$

Where P_j is the range of possibility of failure of the j-th BE, n is the number of experts, m is the number of BE, w_i is the weighting factor of the i-th expert and EO_{ij} is the TFN of the i-th expert and j-th BE. All BE's failure possibility will be calculated repeating this process for every BE.[39,42,43]
The next step consists in evaluate failure possibility of intermediate events, until reaching the top event of the fault tree. Intermediate events are a combination of BE, by means of **AND** and **OR** operators. In conventional FTA, resolution of these operators is linear because of crisp exact values. In fact:

1. **AND** gate operator is solved by $P_{AND} = \prod P_j$;
2. **OR** gate operator is solved by $P_{OR} = \prod(1 - P_j)$.

In fuzzy FTA instead, there are triplets of values(a_j, b_j, c_j) representing ranges of potential failure possibilities, so gate operations change:

1. **AND** gate operator is now solved by $P_{AND} = \prod P_j = (\prod a_j, \prod b_j, \prod c_j)$;
2. **OR** gate operator is now solved by $P_{OR} = 1-\prod(1-P_j) = 1-[\prod(1-a_j), \prod(1-b_j), \prod(1-c_j)] = (1-\prod(1-a_j), 1-\prod(1-b_j), 1-\prod(1-c_j))$.

In this way, also intermediate events are TFNs and the uncertainty of fuzzy numbers is brought up to the Top Event, which could be represented as both TFN and crisp exact value by means of a defuzzification process.[39,40]
Another way to advance upwards the fault tree is through defuzzification of intermediate events: this method approximates all intermediate events TFNs resulting from **AND** and **OR** gate operators into exact values. This approach can minimize uncertainty related to fuzzy numbers but creates an approximation uncertainty that would influence negatively the final reliability result, so it will be neglected in this work.
In order to provide a single possibility value for the TE rather than a range of possibilities, a defuzzification process will be necessary, which consists in converting fuzzy numbers in a crisp value, called Failure Possibility Score (FPS). There are several defuzzification methods: the weighted average, the centre of area, the mean max membership, the centre of maxima, the mean of maxima and so on. No defuzzification method is suitable for all application, but the centre of area is the most widely used technique.[39,42,44] According to these method, defuzzification of a triangular fuzzy number $A = (a, b, c)$ is obtained using the membership function $\mu_A(x)$:

$$FPS = \frac{\int x\mu_A(x)dx}{\int \mu_A(x)dx} = \frac{\int_a^b \frac{x-a}{b-a}xdx + \int_b^c \frac{c-x}{c-b}xdx}{\int_a^b \frac{x-a}{b-a}dx + \int_b^c \frac{c-x}{c-b}dx} = \frac{1}{3}(a+b+c)$$

Once obtained FPS, a probability value has to be calculated in order to quantify the TE. So FPS can be converted into a Failure Probability (FP) as follows:

$$FP = \frac{1}{10^K}$$

Where $K = C(\frac{1-FPS}{FPS})^{\frac{1}{3}}$ and C is a constant $C = 2.301$. [48] Obtaining the failure probability of the Top Event is the main objective of a reliability analysis but it's not the only one. In fact a sensitivity analysis could be performed. It consists of determining the contributions of basic events or minimal cut sets to the failure probability of the top event and the results obtained are also called importance measures and they may help identify critical components, in particular major contributors to overall risk as well as major contributors to system uncertainty. The former ones can be mapped by calculating the fuzzy importance measure (FIM), the latter instead with the fuzzy uncertainty importance measure (FUIM). [39,42,49,50]
First, the concept of BE fully unavailable or fully available has to be introduced:

- a BE or a MCS *j* is considered fully unavailable when its failure possibility is $P_j = (1, 1, 1)$;
- a BE or a MCS *j* is considered fully available when its failure possibility is $P_j = (0, 0, 0)$.

Then, the failure possibility of the TE with the BE or MCS *j* fully available and unavailable should be evaluated, which means that all the rest of the contributors to the TE will remain the same except for P_j. PTE is the fuzzy failure possibility of TE as it is calculated normally, PTE_1 is the version with $P_j = (1, 1, 1)$ and PTE_0 is the one with $P_j = (0, 0, 0)$. Both of these have to be calculated for each BE or MCS to analyze and then the distance between them has to be found. Since these failure possibilities are still in the fuzzy triangular number form, the conventional approach to sensitivity analysis should be remodeled, so the Euclidean Distance (ED) will be used to obtain FIM and FUIM.

$$FIM(P_j) = ED[PTE_1, PTE_0] = \sqrt{(a^1_{TE} - a^0_{TE})^2 + (b^1_{TE} - b^0_{TE})^2 + (c^1_{TE} - c^0_{TE})^2}$$

It's necessary to consider the failure possibility of the BE or MCS *j* as a crisp value equal to its average value $P_j = b_j$ to calculate FUIM. In fact, FUIM can be calculated as the ED between the normal PTE and the one (PTE_j) calculated with the exact value $P_j = b_j$ corresponding to the failure possibility of the BE or MCS *j*.

$$FUIM(P_j) = ED[PTE, PTE_j] = \sqrt{(a_{TE} - a^j_{TE})^2 + (b_{TE} - b^j_{TE})^2 + (c_{TE} - c^j_{TE})^2}$$

The higher $FIM(P_j)$ and $FUIM(P_j)$ are the higher is the contribution of P_j to the failure probability of TE or its uncertainty respectively. In this way major contributors (with high FIM or FUIM) will be identified and more reliability tests or failure data research could be done in order to minimize their influence on the TE.

Chapter 4

Results and comments

The scope of this Master Thesis work is to produce a complete Risk Assessment report of an On Orbit Servicing mission in an early design phase (0/A). In real life Risk Assessment reports, it's not sufficient to only submit tables full of failure modes or numbers, but it's necessary to comment and explain all results in order to facilitate risk managers comprehension and help to perform an adequate risk mitigation during mission life cycle.
So, in this section, results of the risk analysis performed will be shown and commented starting from auxiliary instruments upon which all risk analysis is based on, passing through the 2 complementary methods used: FMECA (with CFL) and FTA.

4.1 Auxiliary analysis methods

The first step consisted of a functional analysis, divided in 3 sub-methods:

1. Functional Tree, a deductive technique used to break down all mission operations in sub-functions easy to analyze;
2. Functional Flow Block Diagram, which puts in a correct chronological order all basic functions identified in the Functional Tree;
3. Functions/components matrix, an inductive method which correlates each basic function with the component which fulfills that operation.

Functional Tree is a standard technique from which to start a functional analysis. In this case, the tree is limited to operations performed only by the space tug, so ground or launch operations will not be included in this analysis. Since the tug is basically an electric propulsion spacecraft with a standard bus, including standard subsystems (EPS, AOCS, Comms), the functions identified for bus operations are similar to every other EP spacecraft bus. Nonetheless, peculiarities of this mission are:

- acquisition, tracking and approach of a target satellite operations;
- docking/berthing of satellites;
- inspecting, refueling and relocation.

The operations in figure 4.1 imply the use of several components such as:

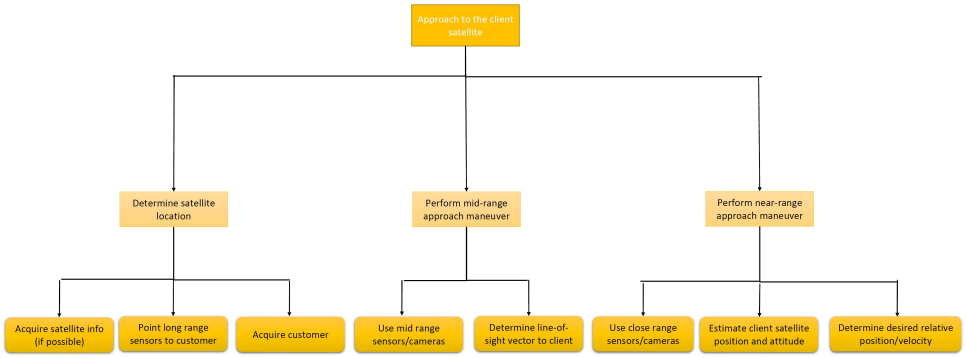


Figure 4.1: Extract of the Functional tree: acquisition, tracking and approach operations

- a GPS receiver to communicate with client satellite to find out its location and state;
- a tracking and acquisition subsystem that can operate from far range to close range;
- software and processors that can elaborate images and data and calculate client position and attitude and the path to follow to reach it.

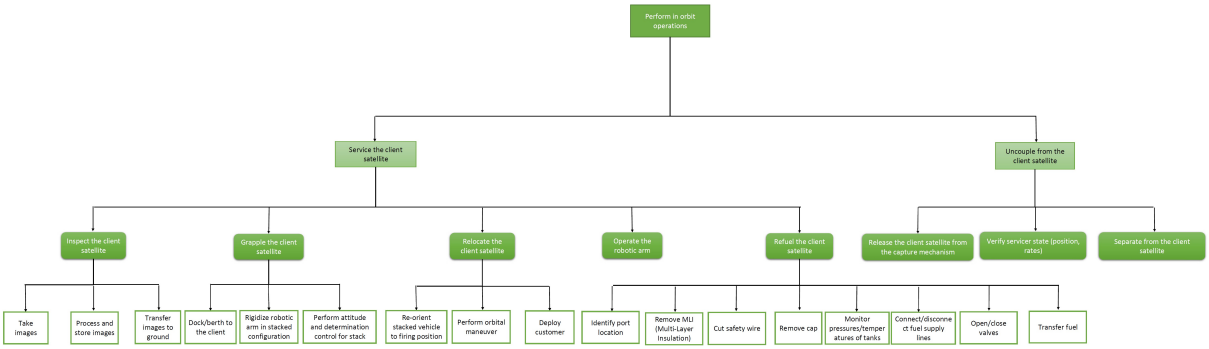


Figure 4.2: Extract of the Functional tree: servicing operations

In figure 4.2, instead, all servicing operations are identified and they represents the core of the mission. They include 2 main subsystems: AOCS and the payload. In fact, the docking/berthing equipment, stereo cameras for external inspection and all refueling tools can be considered as the payload of the space tug and in combination with AOCS components can fulfill servicing duties.
Next auxiliary step of the analysis is the FFBD, which identifies each function with a unique identification number and order them chronologically. In this way inputs and outputs of each function are well established and this helps with the definition of causes and effects of failures during FMECA.

Post-launch phase is crucial for mission success, in fact a single major failure in this early operative phase could impact negatively on operative lifetime of the spacecraft. So particular attention has to be paid in designing and testing components involved in this phase, such as communication devices, external structure, separation mechanism, deployment mechanism (for both solar arrays and antennas) and attitude control components (thrusters and reaction wheels).

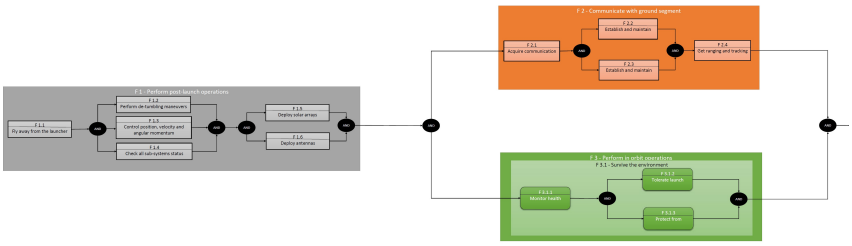


Figure 4.3: Extract of the FFBD: post-launch operations

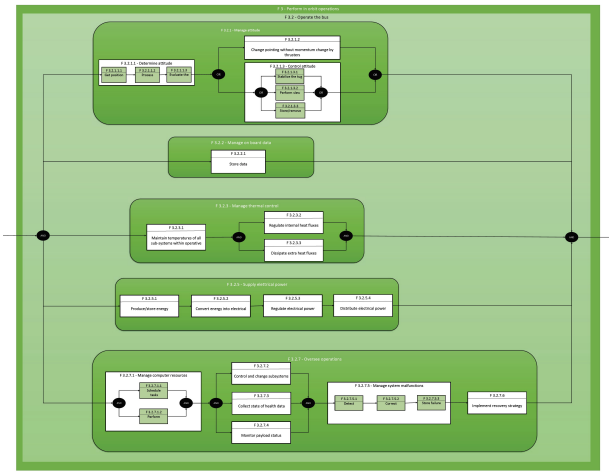


Figure 4.4: Extract of the FFBD: bus operations

As it can be seen in figures 4.3 and 4.4, a "parent" function such as *Perform in orbit operations* can be disassembled in a FFBD in order to depict a correct order of operations. It's necessary that each subsystem works correctly to successfully operate the bus, so all major functions connected to each subsystem are linked by **And** gates.

Figure 4.5: Extract of the FFBD: target approaching operations

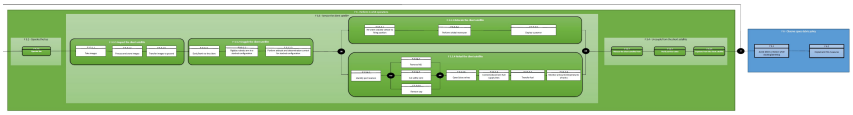


Figure 4.6: Extract of the FFBD: servicing and EOL operations

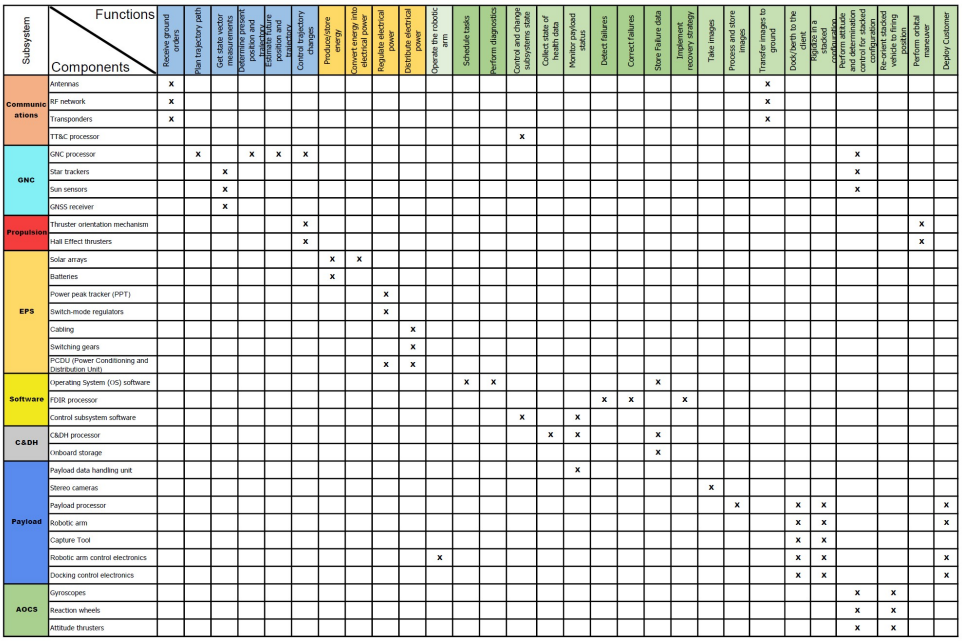
Figures 4.5 and 4.6 are linked together by an **Iteration** gate, which means that after servicing a client satellite, the space tug will restart target approaching operations in order to service another client and this iteration will continue until mission completion.
The last fundamental auxiliary step before proceeding to risk assessment is drawing up a functions/components matrix, in fact this passage will be useful for both FMECA and FTA. This matrix correlates each basic function of the functional tree to one or more components of the space tug, that are inserted in the matrix after consulting previous works on space tug concept, Orbital Express technical overviews, NASA and ESA handbooks and product tree for small spacecraft and the new SMAD. After identifying major components, they have to be connected to the respective functions, however unique correlations are not mandatory, in fact several functions can be performed by more than one component and this could be a case of functional redundancy or there is simply need of more components to perform such operation. Nonetheless there are some components that should develop multiple operations so they can be considered critical issues during design phase. In figures 4.7, 4.8, 4.9 the complete matrix is reported.

Subsystem	Components \ Functions	Detach from the launcher	Perform de-tumbling maneuvers	Control position, velocity and angular momentum	Check all sub-systems status	Deploy solar arrays	Deploy antennas	Acquire communication link	Establish and maintain downlink communication	Establish and maintain uplink communication	Get ranging and tracking data	Monitor health status	Tolerate launch loads	Protect from radiation	Get position data	Process data	Evaluate the attitude	Change pointing without momentum change by	Stabilize the tug	Perform slew maneuvers	Store/remove momentum	Store data	Maintain temperatures of all sub-systems within operative range	Regulate internal heat flows	Dissipate extra heat to outside the tug	Store and distribute propellant
Structure	Separation system	x																								
AOCS	Magnetometers		x												x		x									
	Gyroscopes			x											x		x	x	x							
	Reaction wheels			x														x	x							
	Thruster orientation mechanism			x																x						
	Attitude thrusters			x																x	x					
Propulsion	Xenon tank																									x
	Feed system																									x
Software	Subsystem operations processor				x																					
EPS	Solar array deployment mechanism					x																				
	Solar array deployment control electronics					x																				
Communications	Antennas deployment mechanism						x																			
	Antennas deployment control electronics						x																			
	Antennas							x	x	x	x															
	RF network							x	x	x																
	Transponders							x	x	x	x															
	TT&C processor							x	x	x	x															
C&DH	C&DH processor											x										x				
	Onboard storage																					x				
Structure	Structure												x													
	Radiation shielding													x												
AOCS	Star trackers														x		x									
	Inertial Measurement Unit (IMU)														x		x									
	Sun sensors														x		x									
	AOCS processor															x	x									
Thermal Control System	Thermostats																						x			
	Heaters																						x			
	Coatings																						x			
	Multilayer Insulation (MLI)																						x			
	Heat pipes																						x	x		
	Radiators																						x		x	

Figure 4.7: Extract of the functions/components matrix

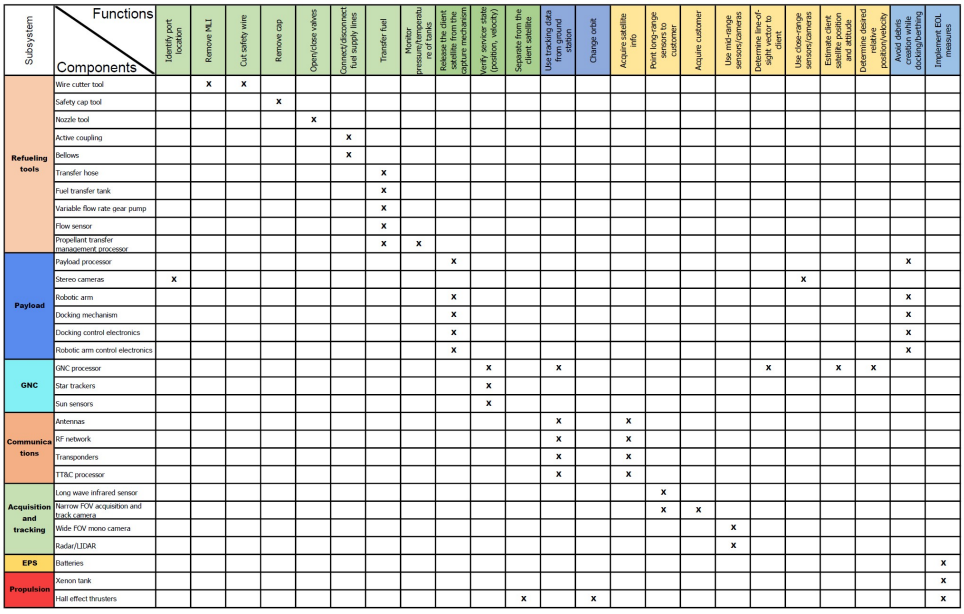
In figure 4.7 there are 2 remarks to do:

- there are multiple devices that perform the same function for AOCS, Communications and Thermal Control subsystems, but it's indeed functional redundancy in case of attitude determination sensors while it's not for the rest of devices: in fact communication and thermal ones work together to accomplish each function so they can be considered complementary instead of redundant;
- there are some components that perform only one operation, such as separation mechanism, deployment mechanisms or Xenon tank and feed system, they should be considered critical parts as a major failure of these devices could seriously impact on mission success, so they should be taken in consideration during Risk Assessment.



Subsystem	Components \ Functions	Receive ground orders	Plan trajectory path	Get state vector measurements	Determine present position and velocity	Estimate future position and velocity	Control trajectory changes	Produce/store energy	Convert energy into electrical power	Regulate electrical power	Distribute electrical power	Operate the robotic arm	Schedule tasks	Perform diagnostics	Control and change subsystems state	Collect state of health data	Monitor payload status	Detect failures	Correct failures	Store Failure data	Implement recovery strategy	Take images	Process and store images	Transfer images to ground	Dock/berth to the client satellite	Rigidize in a stacked configuration	Perform attitude and determination control for stacked configuration	Re-orient stacked vehicle to firing direction	Perform orbital maneuver	Deploy Customer
Communications	Antennas	x																					x						
	RF network	x																					x						
	Transponders	x																					x						
	TT&C processor														x														
GNC	GNC processor		x		x	x	x																			x			
	Star trackers			x																						x			
	Sun sensors			x																						x			
	GNSS receiver			x																									
Propulsion	Thruster orientation mechanism						x																					x	
	Hall Effect thrusters						x																					x	
EPS	Solar arrays							x	x																				
	Batteries							x																					
	Power peak tracker (PPT)									x																			
	Switch-mode regulators									x																			
	Cabling										x																		
	Switching gears										x																		
	PCDU (Power Conditioning and Distribution Unit)									x	x																		
Software	Operating System (OS) software												x	x						x									
	FDIR processor																	x	x		x								
	Control subsystem software														x		x												
C&DH	C&DH processor															x	x			x									
	Onboard storage																			x									
Payload	Payload data handling unit																x												
	Stereo cameras																					x							
	Payload processor																						x		x	x			x
	Robotic arm																								x	x			x
	Capture Tool																								x	x			
	Robotic arm control electronics											x													x	x			x
	Docking control electronics																								x	x			x
AOCS	Gyroscopes																										x	x	
	Reaction wheels																										x	x	
	Attitude thrusters																										x	x	

Figure 4.8: Extract of the functions/components matrix



Subsystem	Components \ Functions	Identify port location	Remove MLI	Cut safety wire	Remove cap	Open/close valves	Connect/disconnect fuel supply lines	Transfer fuel	Monitor pressure/temperatu re and status	Release the client satellite from the capture mechanism	Verify servicer state (position, velocity)	Separate from the client satellite	Use tracking data from ground station	Change orbit	Acquire satellite info	Point long-range sensors to customer	Acquire customer	Use mid-range sensors/cameras	Determine line-of-sight vector to client	Use close-range sensors/cameras	Estimate client satellite position and attitude	Determine desired relative position/velocity	Avoid debris creation while docking/berthing	Implement EOL measures
Refueling tools	Wire cutter tool		x	x																				
	Safety cap tool				x																			
	Nozzle tool					x																		
	Active coupling						x																	
	Bellows						x																	
	Transfer hose							x																
	Fuel transfer tank							x																
	Variable flow rate gear pump							x																
	Flow sensor							x																
	Propellant transfer management processor							x	x															
Payload	Payload processor									x													x	
	Stereo cameras	x																		x				
	Robotic arm									x													x	
	Docking mechanism									x													x	
	Docking control electronics									x													x	
	Robotic arm control electronics									x													x	
GNC	GNC processor										x		x						x		x	x		
	Star trackers										x													
	Sun sensors										x													
Communications	Antennas												x		x									
	RF network												x		x									
	Tranesponders												x		x									
	TT&C processor												x		x									
Acquisition and tracking	Long wave infrared sensor															x								
	Narrow FOV acquisition and track camera															x	x							
	Wide FOV mono camera																	x						
	Radar/LIDAR																	x						
EPS	Batteries																							x
Propulsion	Xenon tank																							x
	Hall effect thrusters											x		x										x

Figure 4.9: Extract of the functions/components matrix

In figures 4.8 and 4.9 core servicing components are listed besides other standard bus devices , for which the remarks stated above are valid. Approaching and rendezvous phase is performed by:

1. acquisition and tracking sensors/cameras used in different moments based on distance from the target;
2. GNC processor used to process data and evaluate line of sight, position, velocity and attitude of the client satellite;
3. Hall effect thruster for orbit changing and approaching.

Payload devices are used to grapple the client, rigidize stacked configuration and finally release it. If relocation is needed, space tug AOCS would intervene and take control of stacked configuration attitude and orbit. If refueling is needed, refueling tools would be used. While robotic arm and capture tool are functionally redundant for grappling operations (docking mechanism is used when client satellite is cooperative), refueling tools are not and they represent the most critical issue of the mission. Spare redundancy of these devices is almost impossible for cost, weight and design reasons so a failure of one of them can be considered a single point failure. For this reason, this subsystem will be considered as the most critical one afterward.

4.2 FMECA and CFL/CIL

					Potential Effects of Failure						
ID	Function	Potential Failure Modes	Failure Causes	Occurrence	Local Effect	End Effect	Severity	Mitigation Factors	Mitigation	RPN	Recommended Actions
1.5	Deploy solar arrays	Total failure of deployment mechanism	Mechanical	1	Inability to deploy solar arrays	No power production, lost of mission	4	Reliability	3	12	Ground test on deployment mechanism
3.2.1.3.1	Stabilize the tug	Gyros or reaction wheels failure	Wear out, poor lubrication of bearings, electrical	2	Uncontrolled spinning	Possible lost of mission	4	Redundancy	1	8	Use of both gyros and reaction wheels or redundancy of one of them
3.2.3.3	Dissipate extra heat fluxes outside the tug	Radiators failure	Wear out, mechanical	2	Overheating	Degraded performances and possible loss of mission	3	Redundancy and change in operations	1	6	Louvers can be used outside radiators to enhance their dissipation capability
3.2.4.2.3	Estimate future position and trajectory	Estimation algorithms failure	Software	2	Incorrect position and trajectory	Inability to reach the customer, lost of time	3	Re-program algorithms from ground	2	12	Combine multiple data types/sources can reduce estimation errors,safe mode needed while re-programming
3.2.5.4	Distribute electrical power	Wiring failures	Electrical, short circuit, wire cut	2	No power to a subsystem	The subsystem can't work	3	Redundancy, fault isolation	1	6	Use of redundant wiring and fuses to open the failed circuit and make it unusable
		Command processor failure	Electrical, software	2	No power to all subsystems	Lost of mission	4	Redundancy, reboot the processor	1	8	Put the tug in safe mode to reset distribution computer
3.2.6	Operate the robotic arm	Control algorithm failure	Software, human error	2	Uncontrolled arm	Inability to perform servicing	3	Ground intervention	2	12	Ground station puts the tug in safe mode to check control laws
		Robotic arm failure	Mechanical, radiation, electrical	2	Unusable arm	Inability to perform servicing, lost of mission	4	Reliability, radiation shielding in stand-by position, ground intervention	2	16	Intensive ground testing, use of a complete prototype on ground to check for failures
3.3.2.1	Dock/berth to the client	Grappling mechanism failure	Mechanical, software	2	Inability to berth to the client	Lost of mission	4	Reliability, functional redundancy	2	16	Ground testing, provide the tug of an alternative way to mate the client, such as a docking mechanism
3.3.3.1	Re-orient stacked vehicle to firing position	Gyros or reaction wheels failure	Wear out, poor lubrication of bearings, electrical	2	Incorrect pointing	Minor loss of time	2	Redundancy	1	4	Use of both gyros and reaction wheels or redundancy of one of them
3.3.4.1	Identify port location	Cameras failure	Electrical, software, impact	2	Insufficient images taken	Inability to find fuel port	4	Redundancy	1	8	Mount several close range cameras on the robotic arm and on the tug
3.3.4.6	Connect/disconnect fuel supply lines	Precision tools failure	Electrical, mechanical, software	3	Inability to connect/disconnect fuel supply	Inability to refuel	4	Redundancy, reliability, ground	1	12	Use a protoylpe arm on ground to simulate all procedures in real time
4.1.1	Use on board data	Communication or relative navigation system failure	Electrical, software	2	Inability to get customer position data	Lost of time	3	Functional redundancy	1	6	Use different methods to get customer position, such as ground data from customer's owner and GPS data from the customer itself
		Processing malfunction	Software	1	Inability to process data correctly	Lost of time	3	Ground intervention	2	6	Send raw data to ground station to process them
5.3.2	Estimate client satellite position and attitude	Estimation algorithms failure	Software	2	Inability to determine client position and attitude	Inability to perform rendezvous	4	Re-program algorithms from ground	2	16	Combine multiple data types/sources can reduce estimation errors,safe mode needed while re-programming
5.3.3	Determine desired relative position/velocity	Navigation system failure	Software, electrical	2	Inability to determine desired relative position/velocity	Inability to perform rendezvous	4	Reliability, ground intervention	2	16	Ground testing, send customer position/velocity data to ground to process them

Figure 4.10: FMECA extract

FMECA is considered as a qualitative subjective inductive bottom-up technique and this means that the analysis starts from basic functions of the fault tree and identifies their failure modes, causes, effects

and mitigation factors inductively. The role of the analyst is fundamental in this type of methodology because he/she has to evaluate each failure occurrence, severity and level of potential mitigation with his/her experience. In this case, failure data from several database are used in order to evaluate occurrence and severity of each failure mode in the most accurate way possible. Although the subjective nature of FMECA, its result, that is CFL/CIL, is almost independent from analyst's experience. In fact, besides score grades of Occurrence, Severity and Mitigation, the most important number in FMECA worksheet is the Risk Priority Number (RPN), that is the product of Occurrence, Severity and Mitigation scores. CFL/CIL is developed according to RPN and maximum severity score, which means that each failure mode with an $RPN > 8$ or a severity number $SN = 4$ is listed as critical.
Over 100 failure modes have been identified and each one have been rated properly, but because of the large number of failure modes and the repetitiveness of some of them an extract of the entire FMECA is showed and commented here. FMECA worksheet construction is explained in 3.3.
Considering all *failure causes*, mechanical, electrical and software are the most frequent ones, while 2 is the most common occurrence score.
End effects are more important rather than local ones because they establish the severity number of each failure mode. Most common end effects are degraded performance, lost of time and lost of mission: the first two effects are rated with $S = 2 - 3$ while lost of mission is obviously catastrophic and $S = 4$.
Most frequent *mitigation factors* identified are: ground intervention, redundancy and reliability of component chosen. The column of *recommended actions* is a hint for the following Risk Management phase and if these or other corrective actions are taken in response to a potential failure, RPN would decrease in a subsequent FMECA and the corresponding function/component would no more considered critical. In fact, FMECA and CIL must be developed iteratively during all product design cycle in order to constantly control how effectively risks are mitigated and if failures in CIL are decreased in number.
Considering all failure modes identified, there are several remarks to do:

- Hall Effect thrusters failure could be critical in that they are continuously used during almost all lifetime operations, moreover they perform fundamental operations, failures of which could be major or catastrophic, so it's essential to test them properly and use redundancy;

- generally speaking functions that would be performed by the bus are considered "safe", because of years and lot of launches of heritage of the devices considered, in particular communication, attitude and orbit determination, power production and distribution and thermal control operations could be affected by minor faults which would not impact severely on space tug functionality;

- Robotic arm and docking operations could represent a weak point during design and operations on orbit, in fact, although docking and berthing have been performed extensively in space during past decades, there are still several difficulties to perform these operations autonomously onboard without ground teleoperation and moreover a malfunction of robotic arm or Capture Tool can severely damage the space tug and/or the client satellite, causing mission to fail;

- another weak point of the mission can be found in the group of precision tools used to refuel the client satellite, because of lack of historical failure data and the intrinsic difficulty to utilize them properly and autonomously on orbit.

54 functions/devices are listed as critical out of a total of 104 failure modes. This is a common result for a CFL developed during conceptual design, when the product design is not consolidated, moreover it's fruitful to identify as much critical tasks as possible in order to focus future efforts on mitigating

ID	Function	Potential Failure Modes	Occurence	Severity	Mitigation	RPN
1.1	Detach from the launcher	Get stuck in the fairing	1	4	1	4
1.2	Perform de-tumbling maneuvers	Magnetometers failure	1	4	1	4
1.5	Deploy solar arrays	Total failure of deployment mechanism	1	4	3	12
2.1	Acquire communication link	Total failure of antenna	1	4	2	8
3.1.2	Tolerate launch loads	Resonance with the launcher	1	3	3	9
3.1.3	Protect from radiation	Contamination of internal components	2	4	1	8
3.2.1.3.1	Stabilize the tug	Gyros or reaction wheels failure	2	4	1	8
3.2.1.3.2	Perform slew maneuvers	Thrusters failure	3	3	1	9
3.2.1.3.3	Store/remove momentum	Thrusters failure	3	4	1	12

(a) Part 1

ID	Function	Potential Failure Modes	Occurence	Severity	Mitigation	RPN
3.2.2.1	Store data	Computer failure	1	4	2	8
3.2.3.1	Maintain temperatures of all sub-systems within operative range	Coating degradation	3	3	1	9
3.2.4.1.1	Receive ground orders	Communication system failure	1	4	2	8
3.2.4.2.2	Determine present position and trajectory	Process algorithms failure	2	3	2	12
3.2.4.2.3	Estimate future position and trajectory	Estimation algorithms failure	2	3	2	12
3.2.4.3	Control trajectory changes	Thrusters failure	3	3	1	9
		Control laws failure	2	3	2	12
3.2.5.1	Produce/store energy	Solar array operation partial failure	3	3	1	9
		Solar array operation failure	2	4	2	16
3.2.5.4	Distribute electrical power	Command processor failure	2	4	1	8

(b) Part 2

Figure 4.11: Critical Functions/Items List

ID	Function	Potential Failure Modes	Occurence	Severity	Mitigation	RPN
3.2.6	Operate the robotic arm	Control algorithm failure	2	3	2	12
		Robotic arm failure	2	4	2	16
3.2.7.1.1	Schedule tasks	Commanding processor failure	1	4	2	8
3.2.7.5.1	Detect failures	FDIR system failure	2	3	2	12
3.2.7.5.2	Correct failures	FDIR system failure	2	3	2	12
3.2.7.5.3	Store Failure data	FDIR system failure	2	3	2	12
3.2.7.6	Implement recovery strategy	FDIR system failure	2	4	2	16
3.3.2.1	Dock/berth to the client	Grappling mechanism failure	2	4	2	16
		Docking mechanism failure	2	4	2	16
3.3.2.2	Rigidize robotic arm in a stacked configuration	Robotic arm failure	1	4	2	8
3.3.2.3	Perform attitude and determination control for stacked configuration	Gyros or reaction wheels failure	2	4	1	8
		Thrusters failure	3	4	1	12
3.3.3.2	Perform orbital maneuver	Thrusters failure	3	4	1	12

Figure 4.12: Critical Functions/Items List part 3

ID	Function	Potential Failure Modes	Occurence	Severity	Mitigation	RPN
3.3.4.1	Identify port location	Cameras failure	2	4	1	8
3.3.4.2	Remove MLI	Precision tools failure	3	4	1	12
3.3.4.3	Cut safety wire	Precision tools failure	3	4	1	12
3.3.4.4	Remove cap	Precision tools failure	3	4	1	12
3.3.4.5	Open/close valves	Precision tools failure	3	4	1	12
3.3.4.6	Connect/disconnect fuel supply lines	Precision tools failure	3	4	1	12
3.3.4.7	Transfer fuel	Fuel pump failure	2	4	2	16
3.3.4.8	Monitor pressure/temperature of tanks	Pressure/temperatures sensors failure	2	3	2	12
3.4.1	Release the client satellite from the capture mechanism	End effector failure	2	4	1	8
3.4.3	Separate from the client satellite	Thrusters failure	3	4	1	12

(a) Part 4

ID	Function	Potential Failure Modes	Occurence	Severity	Mitigation	RPN
4.2.1	Change orbit	Thruster failure	2	4	1	8
5.1.1	Acquire satellite info	Communication or relative navigation system failure	2	4	1	8
5.1.2	Point long-range sensors to customer	Long range sensors failure	2	4	1	8
5.1.3	Acquire customer	Tracking algorithm failure	2	3	2	12
5.2.1	Use mid-range sensors/cameras	Long range cameras failure	2	4	1	8
5.2.2	Determine line-of-sight vector to client	Autonomous processing computer failure	1	4	1	4
5.3.1	Use close-range sensors/cameras	Close range cameras failure	2	4	1	8
5.3.2	Estimate client satellite position and attitude	Estimation algorithms failure	2	4	2	16
5.3.3	Determine desired relative position/velocity	Navigation system failure	2	4	2	16
6.2	Implement EOL measures	Thrusters failure while decommissioning	2	3	2	12

(b) Part 5

Figure 4.13: Critical Functions/Items List

them.
Some observations about which type of functions are listed in figures 4.11, **??**, 4.13 can be done:

- several post-launch operations, structural survivability and basic attitude control functions are considered critical because if they fail in the first phases of the mission, they will severely impact on operative lifetime or end the mission prematurely;
- all Fault, Detection, Identification and Recovery tasks are considered critical because they could enhance the severity of an undetected or unsolved failure and allow the propagation of the failure;
- several operations that require use of robotic arm, docking mechanism and refueling tools are obviously critical for the reasons stated above;
- almost all acquisition, tracking and approach tasks are critical, especially on the severity point of view there could be the inability to properly track the target and so the inability to fulfill the servicing task, even if sensors and cameras are well-known and often-used devices, major problems can derive from processors and algorithms used to estimate client position, attitude and velocity and to calculate a path to reach it.

Functions and items listed as critical will be prioritized during Risk Management process according to their RPN: more higher the RPN is, more resources (time and money) will be spent to mitigate the corresponding risk, if possible. After the first Risk Management phase, FMECA and CIL will be repeated in order to establish if some of the major risk contributors have been mitigated effectively.

4.3 FTA

A Fault Tree has been constructed starting from the Top Event, which is Loss of Mission, and breaking it down into Intermediate and Basic Events that represent potential failure causes. Since LOM has been chosen as TE, only relevant events that would bring to major failures are considered in the analysis, malfunctions or minor faults are neglected.

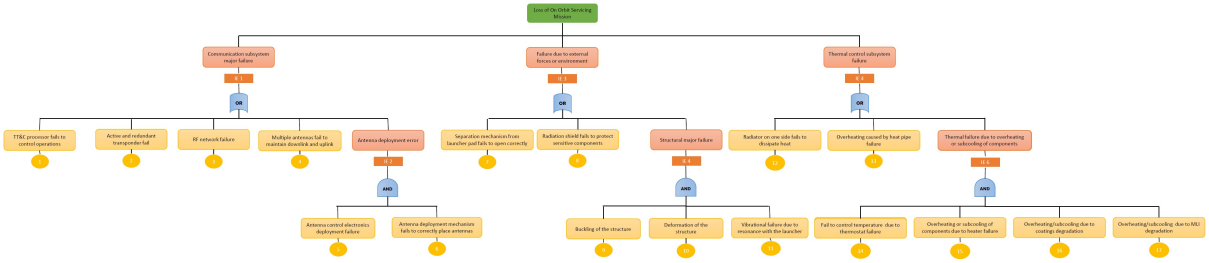


Figure 4.14: Fault Tree: first extract

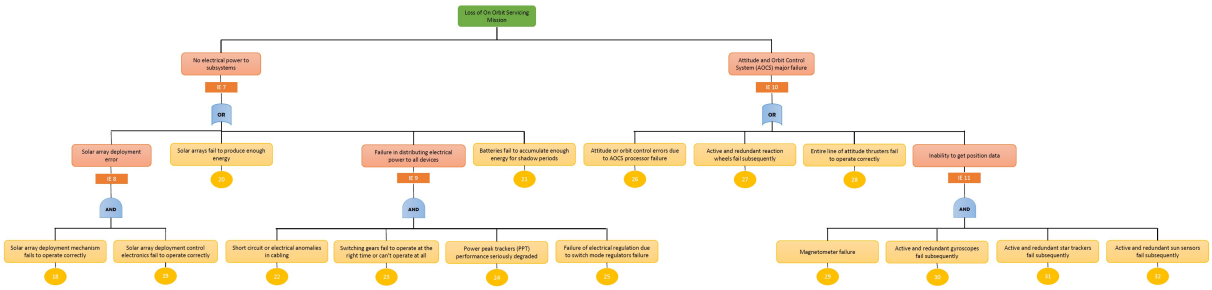


Figure 4.15: Fault Tree: second extract

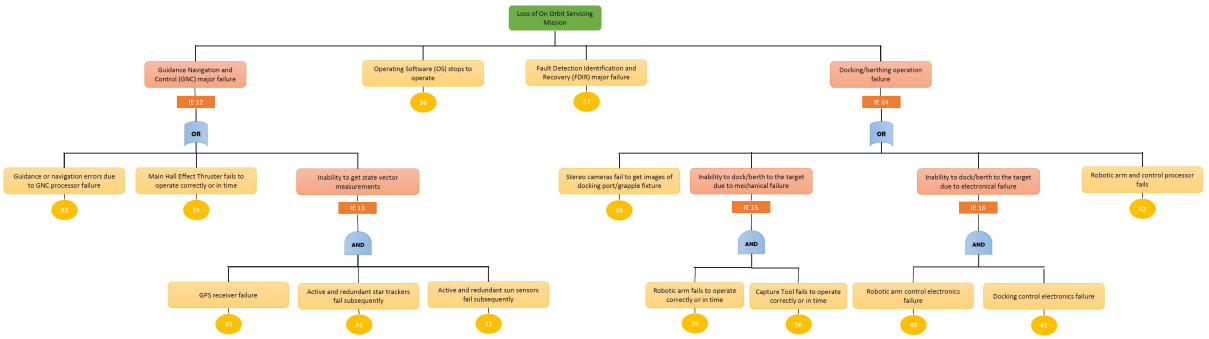


Figure 4.16: Fault Tree: third extract

Each branch of FT represents a subsystem failure and it's further developed into component-level failures in order to reach the level of resolution required to estimate accurate failure data. Once all FT is

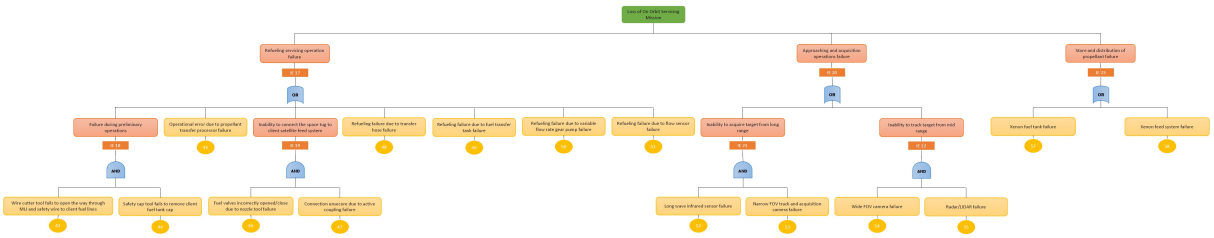


Figure 4.17: Fault Tree: fourth extract

developed, qualitative analysis can be performed: Minimal Cut Sets (MCS) are identified and expressed with Boolean algebra. MCS order depends on how many BEs each cut set contains. In particular, first order MCS are composed of only one BE, which could cause by itself TE to occur, so they are considered weak design points to prioritize during risk mitigation. As MCS order increase more and more, BEs that form these MCS assure a much more reliable operation and they can be neglected during subsequently risk management to favor resource allocation to first order ones.

MCS order	ID BE	Boolean expression
First	1,2,3,4	ID number
	7,8	
	12,13	
	20,21	
	26,27,28	
	33,34	
	36	
	37	
	38,42	
	45,48,49,50,51	
	57,58	
Second	5,6	5∩6
	18.19	18∩19
	39,56	39∩56
	40,41	40∩41
	43.44	43∩44
	46,47	46∩47
	52,53	52∩53
	54,55	54∩55
Third	9,10,11	9∩10∩11
	35,31,32	35∩31∩32
Fourth	14,15,16,17	14∩15∩16∩17
	22,23,24,25	22∩23∩24∩25
	29,30,31,32	29∩30∩31∩32

Figure 4.18: MCS order list

Identification numbers of BEs in figure 4.18 arise from FT construction (figures 4.14,4.15,4.16,4.17). As described in 3.4.2, fuzzy set theory is applied to this work in order to obtain failure data from experts'

elicitation, interviewing them and then translating their opinion in range of fuzzy numbers. Fuzzy set theory has been used for industrial application such as nuclear power plants or pipelines until now, but it can be applied also to space systems thanks to its general nature. The theory is based on the use of ranges of numbers to express a failure possibility instead of a crisp exact value estimated using handbooks or historical database. For this purpose, Triangular Fuzzy Numbers have been used.
The elicitation process consists of filling in a questionnaire about his/her profession, experience and educational qualification in order to evaluate the quality of each experts' opinion. Subsequently, failure possibilities are required for each BE in form of linguistic expression, such as "low","moderate","high". For this task, 4 experts, which is the minimum number to have an accurate aggregation, have been chosen.

Subsystem	Component failure	Linguistic judgment about failure possibility
Communication	Telemetry Tracking and Control(TT&C) processor	Very Low
	Transponder	Low
	Radio Frequency (RF) network	Reasonably Low
	Antenna	Low
	Antenna control electronics	Low
	Antenna deployment mechanism	Reasonably Low
Structure	Separation mechanism (from launcher)	Moderate
	Radiation shield	Very low
	Buckling of external structure	Very low
	Deformation of external structure	Very low
	Harmful resonance with the launcher	Very low
Thermal control	Radiator	Low
	Heat pipe	Reasonably low
	Thermostat	Low
	Heater	Reasonably low
	External coating	Very low
	Multi Layer Insulation (MLI)	Very low
EPS	Solar array deployment mechanism	Reasonably low
	Solar array deployment control electronics	Low
	Solar array	Low
	Battery	Very low
	Cabling	Moderate
	Switching gear	Low
	Power Peak Tracker (PPT)	Low
	Switch mode regulator	Low
AOCS	AOCS processor	Very low
	Magnetometer	Reasonably low
	Gyroscope	Reasonably low
	Star tracker	Low
	Sun sensor	Low
	Reaction wheel	Moderate
	Hall Effect attitude thruster	Moderate

(a) Part 1

Subsystem	Component failure	Linguistic judgment about failure possibility
GNC	Guidance, Navigation and Control (GNC) processor	Very Low
	GPS receiver	Low
	Hall effect main thruster	Moderate
Operating System (OS) software		Low
Fault Detection Identification and Recovery (FDIR) processor		Very low
Payload	Stereo camera	Reasonably low
	Robotic arm mechanism	Reasonably low
	Capture tool docking mechanism	Reasonably low
	Robotic arm control electronics	Low
	Docking control electronics	Low
	Robotic arm and docking processor	Very low
Refueling tools	Wire cutter tool	Moderate
	Safety cap remover tool	Moderate
	Nozzle connection tool	Moderate
	Active coupling	Moderate
	Transfer fuel hose	Reasonably low
	Tank for servicing fuel	Moderate
	Variable flow rate gear pump	Low
	Flow sensor	Moderate
	Propellant transfer processor	Very low
Acquisition and tracking	Long wave infrared sensor	Low
	Narrow FOV track and acquisition camera	Reasonably low
	Wide FOV camera	Reasonably low
	Radar/LIDAR	Reasonably low
Propulsion	Xenon fuel tank	Reasonably low
	Xenon feed system	Reasonably low

(b) Part 2

Figure 4.19: Experts' interview

After each expert has given his/her opinion, aggregation process is performed in order to obtain a single range of failure possibilities by a weighted sum of each expert's opinion about each BE. Then IE failure possibilities are evaluated using AND and OR operators, until reaching TE, which failure possibility is calculated in form of TFN and then translated into a failure probability by $FP = 1/10^K$ where $K = C(\frac{1-FPS}{FPS})^{1/3}$ and $FPS = 1/3(a+b+c)$ is the Failure Possibility Score derived from defuzzification of TE and C is an empirical variable depending from the industrial application considered. From [48] $C = 2.301$ for naval industry. In this work C is obtained by a reverse engineering process:

1. reducing the servicing mission FT to a standard GEO EP satellite FT;
2. calculating TE failure possibility after FT changes but with the same experts' opinions on subsystems remained;
3. using failure probability of a GEO EP satellite derived from [51] and replacing the actual TE failure probability;
4. calculating C by inverting K equation, $C = 13.754$.

TE failure possibility obtained belongs to "Very high" membership function as expected and this is due to several causes:

- since this work is part of a conceptual design phase, space tug design is still unclear and this causes the design supposed here to be not perfected;
- although Standard Fault Tree turned out to be the simplest way to analyze a system, it lacks of depth and precision especially for what concerns dynamic behaviour, use of spare parts and time-related aspects;
- since this study is the first iteration of the FTA, it can be considered unpolished and can show inaccuracies, which would be eliminated after few FTA iterations during following design phases.

TFN	Mission failure possibility
a	0,97900601
b	0,99857999
c	0,99995177

Figure 4.20: TE failure possibility in form of TFN

Later, this failure possibility has been converted into a crisp exact failure probability, which is:

$$FP = 2 * 10^{-3}$$

It can be calculated also in form of Mean Time Between Failures:

$$MTBF = \frac{1}{FP} = 498.3h = 20.76days$$

Although these results may not seem optimal, they can be definitely considered conservative for several reasons:

- conceptual design phase does not require precise failure probabilities and it's not even possible to expect them in this early phase, it's more sensible to estimate mission reliability conservatively;
- MTBF result does not represent the actual potential mission lifetime, in that all subsystems should constantly operate simultaneously to obtain that MTBF, instead this result should be related to the mission phases when all FT operations are really being performed at the same time and this happens especially during rendezvous and servicing phases;
- FTA hasn't been iterated and this means that some redundancies or design details may have been neglected and that the more FT construction is improved the more TE failure probability decreases and gains accuracy.

At last, a sensitivity analysis has been developed in order to identify which MCS are the major contributors to TE failure possibility and which are major contributors to its uncertainty. For this purpose, FIM and FUIM are used as described in 3.4.2.

	MCS	FIM	FIM rank	FUIM	FUIM rank
Communication	Telemetry Tracking and Control(TT&C) processor	0,024914	3	0,001932	2
	Transponder	0,02122	5	0,000389	3
	Radio Frequency (RF) network	0,024121	3	0,001938	2
	Antenna	0,021413	5	0,000535	3
	Antenna deployment failure	0,021853	5	0,000982	3
Structure	mechanism (from launcher)	0,031022	1	0,003127	1
	Radiation shield	0,021824	5	0,001282	3
	Structural failure	0,021043	5	1,46E-05	4
Thermal control	Radiator	0,023624	4	0,001806	2
	Heat pipe	0,024121	3	0,001938	2
	Subsystems temperature beyond operative	0,021045	5	1,77E-05	4
EPS	Solar array deployment error	0,022724	4	0,00145	3
	Solar array	0,023624	4	0,001806	2
	Battery	0,022499	4	0,001471	3
	Distribution network failure	0,021045	5	2,32E-05	4
AOCS	AOCS processor	0,023048	4	0,001635	2
	Inability to get data	0,021042	5	6,59E-07	5
	Reaction wheel	0,022719	4	0,001427	3
	Hall Effect attitude thruster	0,021053	5	5,29E-05	4

(a) Part 1

	MCS	FIM	FIM rank	FUIM	FUIM rank
GNC	Guidance, Navigation and Control (GNC) processor	0,021926	5	0,001312	3
	Inability to get state vector measurements	0,021042	5	3E-06	5
	Hall effect main thruster	0,026155	2	0,002289	1
Operating System (OS) software		0,022894	4	0,001586	2
Fault Detection Identification and Recovery (FDIR) processor		0,021926	5	0,001312	3
Payload	Stereo camera	0,021792	5	0,000867	3
	Inability to dock/berth	0,023312	4	0,00175	2
	Control electronics failure	0,021622	5	0,000744	3
	Robotic arm and docking processor	0,022784	4	0,001553	2
Refueling tools	Preliminary operations failure	0,022481	4	0,001264	2
	Connection failure	0,022767	4	0,001402	3
	Transfer fuel hose	0,028223	1	0,002704	1
	Tank for servicing fuel	0,027524	2	0,00247	1
	Variable flow rate gear pump	0,030253	1	0,002982	1
	Flow sensor	0,026155	2	0,002289	1
	Propellant transfer processor	0,023521	4	0,001759	2
Acquisition and tracking	Long range acquisition failure	0,021673	5	0,000815	3
	Mid range tracking failure	0,021716	5	0,000844	3
Propulsion	Xenon fuel tank	0,024624	3	0,002087	1
	Xenon feed system	0,024624	3	0,002087	1

(b) Part 2

Figure 4.21: FIM and FUIM of all MCS

Each MCS has been ranked for its FIM and FUIM score, where 1 and 2 rank represent major contributors and they are highlighted in red in figure 4.21. There are some remarks to do about this analysis:

- the majority of FIM high rank MCS have also a FUIM high rank which means that they have to be mitigated and deeply investigated to decrease their impact on TE failure probability and uncertainty;
- there are much more critical components among refueling tools rather than in other subsystems and this implies that refueling subsystem should be prioritized over the others;

- all propulsion components (Hall effect thruster, tank and feed system) may seriously impact on mission success, so the choice of propulsion subsystem supplier is fundamental;
- all MCS listed as critical, both for Fim and FUIM, are only first order ones, which signifies that the quantity of these MCS should be reduced as much as possible during following analysis in order to mitigate risks.

These importance measures would help decision makers and risk managers in their duties, because they can focus on most impacting MCS and allocate more resources for their mitigation. FUIM high ranking components should be investigated and tested properly in order to reduce failure data uncertainty.
Making a comparison between this analysis and the CFL/CIL developed in 4.2, some analogies and differences can be noted:

1. critical functions in CFL are more in quantity than impacting MCS in FTA;
2. FTA detected 2 critical communication devices such as TT&C processor and RF network that are absent in CFL;
3. thruster is considered a weak point in both methods;
4. most of processor/algorithms failures considered critical in FMECA are negligible in FTA because of the low failure possibility assigned by experts;
5. some EPS and Thermal Control failures are listed as critical in both reports;
6. docking/berthing mechanisms and refueling tools are considered as the most critical components of the whole mission.

Chapter 5

Conclusion and future work

Literature review in 2.3 outlines that On Orbit Servicing is not just a pioneering sector, but could be a new flourishing market. Several technological demonstrations have been made and tested several mission operations, from rendezvous to refueling. All components required to a servicing tug have already been tested, so a relocation and refueling servicing mission is technically feasible, nonetheless a test flight should be performed before building a constellation of tugs, in order to test autonomous tasks and computer response to unpredictable circumstances.
Under an economic point of view, servicing GEO satellites results to be the most convenient strategy because of their high revenue. Regarding the kind of servicing to do, 4 mission have been analyzed in 2.3: 2 of them consist of repairing the client and bring it back from partial to full functionality, an attitude and orbit control service (relocation or stationkeeping) and a refueling mission. Only the last two ones of these missions are economically viable for both the servicer and the client owners, for all Internal Rate of Return and all payback periods considered in [17]. So a GEO servicing space tug is also economically feasible if relocation/stationkeeping and/or refueling are performed, because these operations can bring back to full functionality an almost EOL satellite and extend its operative lifetime of years, increasing revenues of several billions of dollars.
Risk assessment of the conceptual design of the space tug have been performed using both qualitative and quantitative techniques. In particular a FMECA and a FTA have been done without compromising each other results by contaminating FTA with failure modes identified in FMECA or viceversa. In fact these two methods can be viewed as complementary ones, which outcomes can help risk mitigation and design choices. FMECA is a qualitative and subjective technique, where analyst's expertise has an huge influence on the outcome, so historical failure data have been used in order to better judge a failure occurrence or severity. In this way critical functions/items are identified based on their Risk Priority Number, which the higher it is the more urgent the respective failure mode should be mitigated during risk management. 54 critical functions are listed out of 104 failure modes initially identified.
FTA is different from FMECA in that it considers only major relevant failures that could cause the Top Event(Loss Of Mission) to occur. So the number of Basic Events identified is 58, less than total failure modes in FMECA but comparable with only critical ones. The principal scope of this analysis is to quantify TE probability and the secondary one is to evaluate the impact that each Minimal Cut Set has on it. To do so, fuzzy set theory by Tanaka is applied to this scenario and, however it's already been used mainly in nuclear, naval or pipelines application, it can be easily suited on space applications with few adjustments. This unconventional method has a proper use especially in early design phases, when design is not consolidated and failure data on generic components would bring only uncertainty and in-

accuracy into the analysis. Remarkable results of FTA are: TE failure probability of $FP = 2 * 10^{-3}$ corresponding to a Mean Time Between Failures of $498.3h$ considered when all subsystems work simultaneously and a list of major contributors to to TE failure probability and uncertainty developed after a sensitivity analysis. These components can be compared with CIL in order to outline similarities and differences. Both methods however would help during following design phases.
Although fuzzy set theory has no theoretical issue for space application, results obtained with this method should be validated by comparison with other risk quantification techniques on the same Fault Tree. For example, a future work should be the application of conventional acknowledged techniques such as Monte Carlo simulation and comparison of outcome of this analysis with the one performed with fuzzy numbers.
Regarding FMECA, a risk mitigation should be performed during conceptual design phase and then FMECA and CIL should be repeated during all following design phases in order to control how effectively risk management and design choices impact on the quantity of critical components identified. After a design optimization and consolidation, components to mount onboard will be chosen and accurate historical failure data could be obtained for each of them. In this way, it will be possible to perform a FTA with exact crisp values instead of ranges of fuzzy numbers and more accurate TE failure probability will be obtained. In addition, this result can be compared to the one obtained with fuzzy numbers in order to evaluate how much accurate the fuzzy technique is. At last, the construction of the Fault Tree can be improved by considering also the dynamic behaviour of the space tug and using Dynamic or Temporal Fault Trees in following design phases. These kind of trees should be analyzed again with the same fuzzy technique and both results compared in order to evaluate the uncertainty derived from the use of a Standard Fault Tree instead of a Dynamic or Temporal one.

Bibliography

[1] E. Zio, *Reliability engineering: Old problems and new challenges*, Reliability Engineering & System Safety, Volume 94, Issue 2, Pages 125-141, 2009;

[2] Elisabeth Pate'-Cornell, Robin Dillon, *Probabilistic risk analysis for the NASA space shuttle: a brief history and current work*, Reliability Engineering & System Safety, Volume 74, Issue 3, Pages 345-352, 2001;

[3] Stamatelatos, Michael & Dezfuli, Homayoon & Apostolakis, George & Everline, Chester & Guarro, Sergio & Mathias, Donovan & Mosleh, Ali & Paulos, Todd & Riha, David & Smith, Curtis & Vessely, William & Youngblood, Robert, *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners*, 2011;

[4] Ahmadi, Mohammad Amin Saleh, *Risk Analysis in Engineering Techniques, Tools, and Trends*, Mohammad Modarres , 2003;

[5] Cioaca, Catalin, *Qualitative risk analysis methods in aviation projects*,Journal of Defense Resources Management , Volume 2, Number 1, 2011, Pages 77+;

[6] NASA GSFC, *On-Orbit Satellite Servicing Study Project Report*, October 2010

[7] Robert B. Friend, *Orbital Express program summary and mission overview*, Sensors and Systems for Space Applications II , Volume 6958, Pages 11-21, 2008;

[8] Wikipedia, *Hubble Space Telescope*, 2021;

[9] Manny R. Leinz & Chih-Tsai Chen & Michael W. Beaven & Thomas P. Weismuller & David L. Caballero & William B. Gaumer & Peter W. Sabasteanski & Peter A. Scott & Mark A. Lundgren, *Orbital Express Autonomous Rendezvous and Capture Sensor System (ARCSS) flight test results*, Sensors and Systems for Space Applications II, Volume 6958, Pages 62-74, 2008;

[10] Gaias, Gabriella & Ardaens, Jean-Sébastien & Terzibaschian, Thomas, *Paving the Way for Future On-Orbit-Servicing Missions: the AVANTI Experiment*, 25th International Symposium on Space Flight Dynamics (ISSFD) , Munich, Germany, 2015;

[11] Rupp, Thomas & Boge, Toralf & Kiehling, Reinhard & Selllmaier, Florian, *Flight Dynamics Challenges of the German On-Orbit Servicing Mission DEOS*, 21st International Symposium on Space Flight Dynamics (ISSFD), Toulouse, France, 2009;

[12] Sellmaier, Florian & Boge, Toralf & Spurmann, Jörn & Gully, Sylvain & Rupp, Thomas & Huber, Felix , *On-Orbit Servicing Missions: Challenges and Solutions for Spacecraft Operations* , American Institute of Aeronautics and Astronautics Inc. , 2010

[13] Clemens Kaiser & Fredrik Sjöberg & Juan Manuel Delcura & Baard Eilertsen, *SMART-OLEV—An orbital life extension vehicle for servicing commercial spacecrafts in GEO*, Acta Astronautica, Volume 63, Issues 1–4, Pages 400-410, 2008;

[14] Sullivan, Brook, *Technical and economic feasibility of telerobotic on-orbit satellite servicing* , University of Maryland Space Systems Laboratory, 2005

[15] Scott Rotenberger and David SooHoo and Gabriel Abraham, *Orbital Express fluid transfer demonstration system*, Sensors and Systems for Space Applications II, Volume 6958, Pages 41-49, 2008;

[16] C.H. DeLee & P. Barfknecht & S. Breon & R. Boyle & M. DiPirro & J. Francis & J. Huynh & X. Li & J. McGuire & S. Mustafi & J. Tuttle & D. Wegel, *Techniques for on-orbit cryogenic servicing*, Cryogenics, Volume 64, Pages 289-294, 2014;

[17] Andrew Robert Graham & Jennifer Kingston, *Assessment of the commercial viability of selected options for on-orbit servicing (OOS)*, Acta Astronautica, Volume 117, Pages 38-48, 2015;

[18] Sara Cresto Aleina & Nicole Viola & Fabrizio Stesina & Maria Antonietta Viscio & Simona Ferraris, *Reusable space tug concept and mission*, Acta Astronautica, Volume 128, Pages 21-32, 2016;

[19] Frei, Heike & Boge, Toralf & Rems, Florian, *Autonomous Navigation for On-Orbit Servicing*, KI - Künstliche Intelligenz, Volume 28, Pages 77-83 , 2014;

[20] NASA, *Systems Engineering Handbook*, Rev 2, 2016;

[21] Nicole Viola & Sabrina Corpino & Marco Fioriti & Fabrizio Stesina, *Functional Analysis in Systems Engineering: Methodology and Applications*, Systems Engineering, IntechOpen, Chapter 3, 2012;

[22] Bob Lightsey, *Systems Engineering Fundamentals*, Defense acquisition university press Fort Belvoir, Virginia, 2001;

[23] Steven R. Hirshorn, *Expanded Guidance for NASA Systems Engineering*, Volume 2: Crosscutting Topics, Special Topics, and Appendices, NASA, 2016;

[24] Viscio, Maria Antonietta & Viola, Nicole & Corpino, Sabrina & Stesina, Fabrizio & Circi, Christian & Fineschi, Silvano & Fumenti, Federico, *Interplanetary CubeSats mission to Earth-Sun libration point for space weather evaluations*, Proceedings of the International Astronautical Congress, 2013;

[25] Shimmin, Rogan & Schalkwyck, James & Perez, Andres & Weston, Sasha & Rademacher, Abraham & Tilles, Julia & Agasid, Elwood & Burton, Roland & Karacalioglu, Arif & Carlino, Roberto, *Small Spacecraft State of the Art Report*, NASA Technical Memorandum , 2015;

[26] Ines Alonso Gomez, *ESA Generic Product Tree*, ESTEC, 2011;

[27] Everett, David F. & James Richard Wertz & Jeffery John Puschell & Henry Apgar, *Space Mission Engineering: The New SMAD*, Microcosm Press, 2018;

[28] Guillermo Ortega, *ESA Guidance, Navigation, and Control Systems*, Dresdner Automatisierungstechnischen Kolloquien, ESA, 2014;

[29] Doug Caswell & Gianfranco Visentin & Guillermo Ortega & Jaap de Kam & Paul Robert Nugteren & Han Scholten, *ConeXpress Orbital Life Extension Vehicle*, ESA bulletin 127, ESTEC, 2006;

[30] Stuart Bulge, *The Systems Engineering Tool Box*, 2008;

[31] Mozaffari, F. & Eidi, A. & Mohammadi, Leila & Alavi, Zahrasadat, *Implementation of FMEA to improve the reliability of GEO satellite payload*, Pages 1-6, 2013;

[32] Flight Assurance Procedure, *Performing a Failure Mode and Effect Analysis*, Number P-302-720, 1996;

[33] Flight Assurance Procedure, *Standard for Performing a Failure Mode and Effects Analysis (FMEA) and Establishing a Critical Items List (CIL) (DRAFT)*, Number 322-209, 2010;

[34] ECSS, *Space product assurance: Failure modes, effects (and criticality) analysis (FMEA/FMECA)*, ESA Requirements and Standard Division,ESTEC, 2009;

[35] Micheal Stamatelatos & William Vesely, *Fault tree handbook with aerospace applications*, NASA, 2002;

[36] Baig, Ahmed & Rusli, Risza & Buang, Azizul, *Reliability Analysis Using Fault Tree Analysis: A Review*, International Journal of Chemical Engineering and Applications, Volume 4, Pages 169-173, 2013

[37] Sohag Kabir, *An overview of fault tree analysis and its application in model based dependability analysis*, Expert Systems with Applications, Volume 77, Pages 114-135, 2017;

[38] Enno Ruijters & Mariëlle Stoelinga, *Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools*, Computer Science Review, Volumes 15–16, Pages 29-62, 2015;

[39] Sohag Kabir & Martin Walker & Yiannis Papadopoulos & Erich Rüde & Peter Securius, *Fuzzy temporal fault tree analysis of dynamic systems*, International Journal of Approximate Reasoning, Volume 77, Pages 20-37, 2016;

[40] Mahmood, Yasser & Ahmadi, Alireza & Verma, A. & Srividya, A. & Kumar, Uday, *Fuzzy fault tree analysis: A review of concept and application*, International Journal of System Assurance Engineering and Management, Volume 4, 2013;

[41] H. Tanaka & L. Fan & F. Lai & K. Toguchi, *Fault-tree analysis by fuzzy probability*,Volume 5, Rel. 32, Pages 453–457, 1983;

[42] Sohag Kabir & Yiannis Papadopoulos, *A review of applications of fuzzy sets to safety and reliability engineering*, International Journal of Approximate Reasoning, Volume 100, Pages 29-55, 2018;

[43] Dong Yuhua & Yu Datao, *Estimation of failure probability of oil and gas transmission pipelines by fuzzy fault tree analysis*, Journal of Loss Prevention in the Process Industries, Volume 18, Issue 2, Pages 83-88, 2005;

[44] Sivaprakasam Rajakarunakaran & A. Maniram Kumar. & V. Arumuga Prabhu, *Applications of fuzzy faulty tree analysis and expert elicitation for evaluation of risks in LPG refuelling station*, Journal of Loss Prevention in the Process Industries, Volume 33, Pages 109-123 , 2015;

[45] Miller, G.A. , *The magical number seven plus or minus two: some limit on our capacity for processing information*, Psychol, Rev. 63, 1956;

[46] Norris, J.R., *Markov Chains, Statistical and Probabilistic Mathematics: Series 2* , Cambridge university Press, second ed. , 1998;

[47] Julwan Hendry Purba & Jie Lu, Guangquan Zhang & Witold Pedrycz, *A fuzzy reliability assessment of basic events of fault trees through qualitative data processing*, Fuzzy Sets and Systems, Volume 243, Pages 50-69, 2014;

[48] T.Onisawa, *An approach to human reliability in man-machine systems using error possibility*, Fuzzy Sets and Systems, Volume 27, Issue 2, Pages 87–103, 1988;

[49] P.V. Suresh & A.K. Babar & V.Venkat Raj, *Uncertainty in fault tree analysis: A fuzzy approach*, Fuzzy Sets and Systems, Volume 83, Issue 2, Pages 135-141, 1996;

[50] Antonio C.F. Guimarees & Nelson F.F. Ebecken, *FuzzyFTA: a fuzzy fault tree system for uncertainty analysis*, Annals of Nuclear Energy, Volume 26, Issue 6, Pages 523-532, 1999;

[51] Saleh, Joseph & Geng, Fan & Ku, Michelle & Walker, Mitchell, *Electric propulsion reliability: Statistical analysis of on-orbit anomalies and comparative analysis of electric versus chemical propulsion failure rates*, Acta Astronautica, Volume 139, 2017