Bachelor's project

NTNU
Norwegian University of Science and Technology
Faculty of Engineering
Department of Mechanical and Industrial Engineering

Ada Kristine Ocares Moen, Eivind Sjøvold and Ola Jordheim

Implementation of FMECA in Small Satellite Development

Bachelor's project in Drifts-og vedlikeholdsteknikk
Supervisor: Viggo Gabriel Borg Pedersen
May 2019

NTNU
Kunnskap for en bedre verden

Ada Kristine Ocares Moen, Eivind Sjøvold and Ola Jordheim

Implementation of FMECA in Small Satellite Development

Bachelor's project in Drifts-og vedlikeholdsteknikk
Supervisor: Viggo Gabriel Borg Pedersen
May 2019

Norwegian University of Science and Technology
Faculty of Engineering
Department of Mechanical and Industrial Engineering

NTNU
Norwegian University of
Science and Technology

Summary

This bachelor project was started from an initiative from Evelyn Honore-Livermore, project leader of the HYPSO project. The HYPSO team plans to develop a Hyper Spectral Imager satellite with the main purpose of mapping algae growth in the Norwegian ocean territories. The satellite contains complex subsystems, utilizing high tech solutions in several different fields of technology. Even small failures during operation can have severe consequences for mission success. Repairing breakdowns in space is easier said than done. In order to achieve better risk management, a bachelor group from mechanical engineering was engaged to facilitate and implement FMECA as a measure to highlight and mitigate risk. The task was to conduct FMECA on critical parts of the satellite and tailor a standardized approach for upcoming HYPSO satellites.

The situational analysis revealed a lack of organized and documented risk management. Because of this, the bachelor group performed a function FMECA with the purpose of quality checking the initial work, creating documentation to avoid a potential backlash. As expected, most failure modes were already considered. However, some new failure modes were discovered, and some failure modes turned out to have been underestimated initially. The bachelor group also conducted a Hardware FMECA on the mechanical parts of the satellite. The second FMECA showed that the outer objective and lens are some of the most critical components to mission success. This project showed the benefits of FMECA as a risk management tool.

After two FMECAs, valuable feedback has been provided and more control gained. This thesis has highlighted more than 30 critical failure modes and mis-

sion requirements are being modified based on the work of this thesis.

Preface

This is a bachelor assignment written by three undergradute students at NTNU, mechanical engineering.

During the span of this project we have learned a lot about FMECA-implementation through a learning-by-doing approach, learning from our mistakes and successes. In addition, literature study and advising from academic supporters has been crucial in the learning process. Therefore, we would like to thank Professor Viggo Gabriel Borg Pedersen, and Evelyn Honorè-Livermore, project leader of the HYPSO-project, for receiving this thesis and advising during this period.

Throughout this period two students have lived in Trondheim and the third has been living in Salt Lake City, Utah, USA. This gave us the opportunity to reach out to a broad network of people, and we would like to thank everyone that helped us with this assignment. This includes professors in Norway, professors in Utah, friends, family, and PhD/MSc students. We also want to thank the HYPSO team for prioritizing time for our work.

Due to the multinational environment we have been operating in, we decided to write this thesis in English. This way, our work can be easily utilized by international members in the HYPSO-team, but also by others finding this thesis interesting.

Estimated, the group spent around 500 hours per person on this project. The bachelor project's duration was from 04.01.2019 - 20.05.2019.

Contents

Abbreviations

ADCS	Attitude Determination and Control Subsystem
AI	Artificial intelligence
AMOS	Centre for autonomous marine operations and systems
BoB	Break out board
COTS	Commercial of the shelf parts
CSLI	CubeSat launch initiative
FDIR	Fault detection, isolation and recovery
FMECA	Failure mode, effects and criticality analysis
FPGA	Field programmeable gate array
HSI	Hyper Spectral Imager
HSIA	Hardware/software interaction analysis
HYPSO	Hyper Spectral Surveillance of the Ocean
IOT	Internet of things
IT	Information technology
M.Sc	Master of Science
NTNU	Norwegian University of Science and Technology
OPU	Onboard processing unit
PhD	Doctor of Philosophy
RAMP	Risk Analysis and Management for Projects
RFA	Risk Factor Analysis
RGB	Red, green and blue(as in camera)
RPN	Risk priority number
SDR	Software defined radio
SHAMPU	Shape, Harness, And Manage Project Uncertainty

Chapter 1

Introduction

"The engineering risks are increasing as projects become more complex. In response to this, risks need to be identified, evaluated and managed in a formal system of control rather that the informal system which have existed in the past." ([23], p.12)

In the fall of 2018 we were asked by our supervisor if we wanted to be part of a satellite project, called the HYPSO-project, for our upcoming bachelor project. We were told they needed someone to conduct an FMECA on the satellite. After some contemplation we contacted our supervisor Viggo Pedersen and the HYPSO-project leader, Evelyn Honoré-Livermore, to announce our interest.

From the beginning, the HYPSO project leader was clear about the need for an FMECA. No one in the HYPSO-team neither had the time nor the knowledge to conduct an FMECA. Therefore, the project needed an initiative to do this task. This made us confident that our assignment was well anchored in the HYPSO-project's management.

We were introduced to the FMECA tool in our third semester of our major in mechanical engineering. We learned how to perform an FMECA, its purposes and its limitation through theory and a few examples. This gave us a basic understanding of FMECA as a tool. However, we had never implemented FMECA on an actual system, which made this project a good learning opportunity.

No financial resources were necessary for our works within this project. The equipment needed was available in the HYPSO-team's work space, SmallSat-lab. We also had access to the HYPSO-projects cloud database, hereby referred to as the HYPSO drive.

1.1 The HYPSO-project Background

Certain types of algae in large quantities can be detrimental to the marine ecosystem and damage the fish stocks. Keeping track of these algae is therefore important to maintain control. Autonomous submarines, boats, planes and satellites equipped with advanced technology, communicating with each other will make this possible.

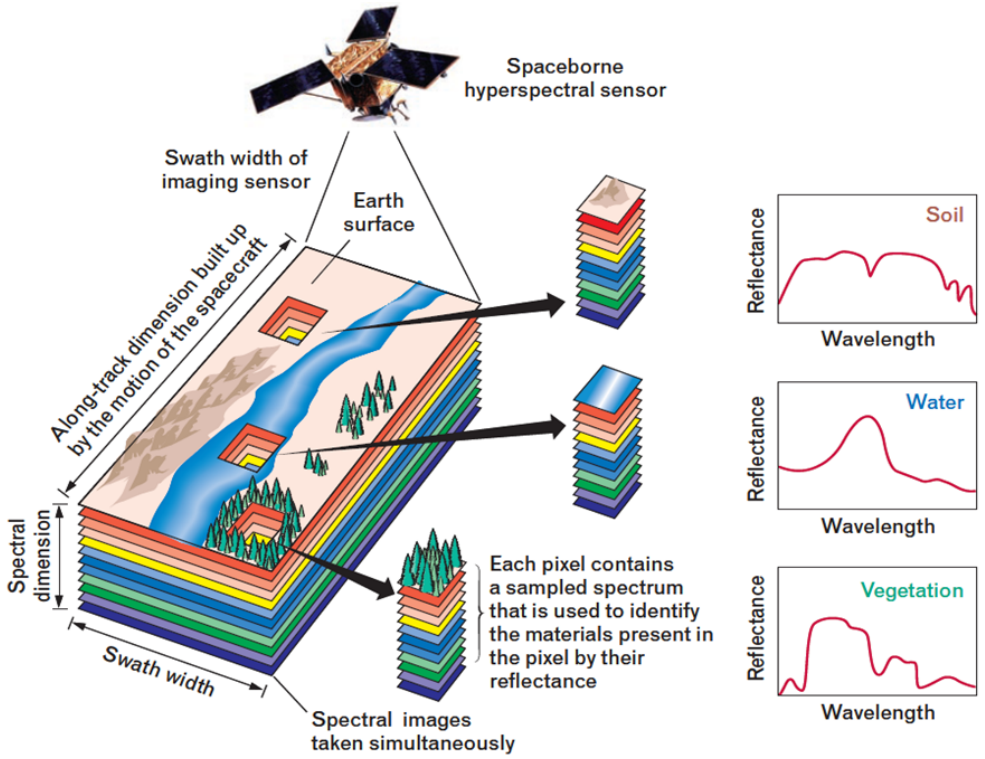


Figure 1.1: Visualization of hyper spectral imaging

The HYPSO satellite contains a Hyper Spectral Imager, a camera capable of capturing images in the spectral dimension, as illustrated in figure 1.1. This allows the satellite's camera to capture blooming algae in the Norwegian waters, giving

fish farming companies a forewarning of this. With aspects of machine learning, the satellite will be able to recognize detrimental algae, and decrease the need of manned boats taking algae tests.

AMOS is a project organization connected to NTNU, and is described as a "center for excellent science". AMOS stands for "Centre for Autonomous Marine Operations and Systems". They already have autonomous systems offshore, supervising the Norwegian oceans[13]. As a supplement to these systems, AMOS wants to implement satellite surveillance. These satellites will communicate with the existing systems, as illustrated in figure 1.2. This was the foundation on which the HYPSO-project was established in august 2018.

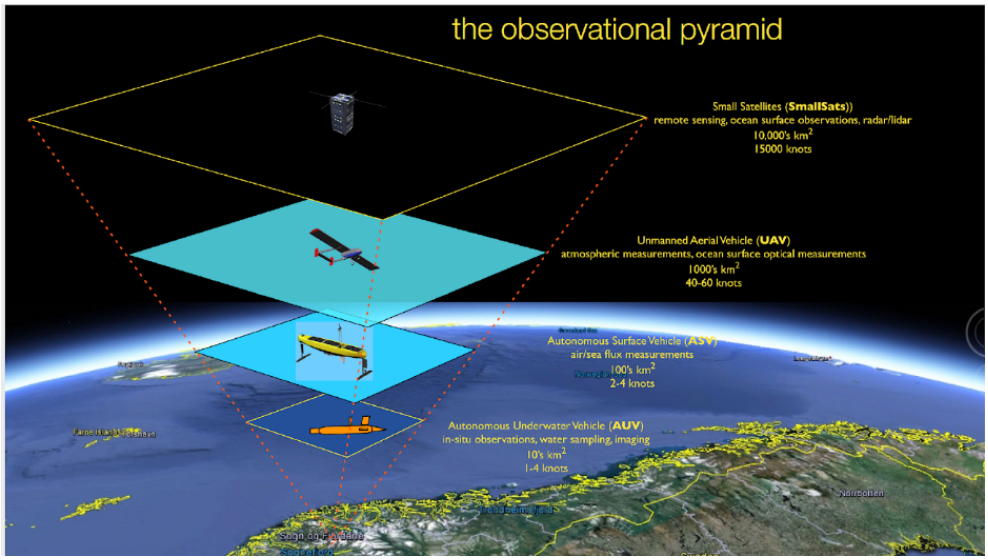


Figure 1.2: Satellites are superior surveillance tools

The HYPSO-team, will deliver a satellite called HYPSO-sat to AMOS. The HYPSO-team are not developing the whole satellite. A Lithuanian company called NanoAvionics is producing parts of the satellite called "the bus". The HYPSO-team is designing the rest of the satellite, called the payload. The payload has to be customized to the bus. In addition, the HYPSO-team is developing and adapting the necessary software.

The HYPSO satellite is the first satellite in AMOS' commitment. The satellite

will include solar panels, a camera, computers for on board processing and antennas. The size of the satellite is 6U. This means that the size corresponds to 6 cubes, each $10cm^3$. The total weight of the satellite is approximately 7500 grams. HYPSO-sat and several other small satellites will be attached to a rocket when the time comes to launch. At about 500 km above sea level the HYPSO-sat will be detached from the rocket, and will start its orbit around the earth.

If several HYPSO satellites are to be produced, they will be called HYPSO-sat 2, HYPSO-sat 3, etc. Then the current satellite will be called HYPSO-sat 1. But before that time, the current satellite is only called HYPSO-sat or simply HYPSO.

1.2 Problem Definition

Our missions are, as specifically defined by the project leader:

- To conduct an FMECA to highlight and mitigate critical failure modes in the HYPSO-system.
- Adapt a standardized FMECA procedure for the HYPSO-team to use as a foundation or guide to implement FMECA. To do this, we will find an already excising procedure, and adapt it.

1.3 Project Goals

We created six project goal in order to complete our missions. The project goals are listed and described below. When doing this project, the project goals were important guidelines to help us stay on track. The methods used for reaching these goals are described in chapter 3.

1. **Project goal 1: Conduct a situational analysis of the HYPSO team's current level of risk assessment**

A situational analysis evaluates the projects internal and external environment to understand the current state of the problem that is to be solved. In this case, the problem is a lack of FMECA and documented risk management on the HYPSO satellite, as well as a standardized FMECA procedure. The situational analysis includes, but is not limited to:

- What has been done in terms risk management in the HYPSO project.
- How the HYPSO project is organized.
- What kind of expertise exists in the HYPSO team.
- Collect background material in order to conduct and facilitate FMECA
- What types of FMECA could benefit the project.

2. **Project goal 2: Create a simple technical description of the HYPSO satellite**

   Understanding the structure of the system being analyzed is necessary for organizing the FMECA, and setting its scope. The technical description includes, but is not limited to:

   - An overview of how the satellite is designed, which subsystems there are, and what function each subsystem has. The functions of the subsystems provides a base for the FMECA.

3. **Project goal 3: Identify suitable standards for conducting FMECA in this specific project**

   There are hundreds FMECA standards available, most of which are company specific. The purpose of this goal is to identify the standards most relevant for space technology. The selected standards will be the foundation for project goal number 4.

4. **Project goal 4: Two parts, a and b.**

   (a) **Describe the FMECA-method according to the chosen standards**. In order to facilitate and perform an FMECA, a plan and knowl-

edge is necessary. This goal will create the base for our final result. The description should contain, but is not limited to:

- A general description of FMECA;
- Pros and cons of FMECA;
- How the group is planning to conduct the FMECA on HYPSO-sat;
- A standardized approach for upcoming HYPSO satellites.

(b) **Define success factors for implementing FMECA in the HYPSO project**. This will increase the possibility of a successful FMECA, if defined before the implementation.

5. **Project goal 5: Plan and conduct FMECA on HYPSO-sat**

   The purpose is dual. First, the result of the FMECA itself will help improve the HYPSO-sat 1. Second, after conducting and implementing an FMECA, the group will have a better foundation to create a standardized FMECA approach.

6. **Project goal 6: Choose 5 critical failure modes on the HYPSO satellite and discuss possible mitigation of risk**

   The main goal of an FMECA is identifying unacceptable risks in order to find countermeasures to reduce it. Achieving this goal highlights the FMECAs purpose as a tool.

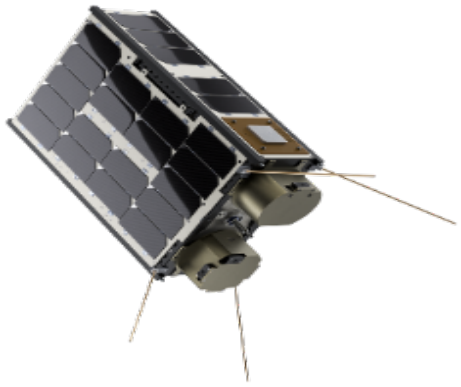


Figure 1.3: The HYPSO-satellite

1.4 Outcome Goals

The bachelor group's outcome goals is to write a bachelor thesis to be proud of, and be able to show in future professional context as a demonstration of our skills. This project will also be a good exercise in working in a high-tech project with highly educated people from different fields of expertise. The bachelor group also wants to build its competence on FMECA.

The HYPSO-team's outcome goals for this thesis is both to obtain a good and useful FMECA for this satellite, and a good foundation to implement FMECA earlier in the the next satellite project. The outcome of a good FMECA can be a higher reliability on the satellite because potential problems are brought up to light and can be discussed, although measuring this improvement is difficult.

1.5 Target Group and Stakeholders

The target group for this project is the HYPSO-team, as well as any other person with an interest in FMECA.

In addition, all other CubeSat-teams around the world can find parts of this thesis interesting. All the CubeSat projects are part of a community that shares information between them to support each other. Therefore, any CubeSat-team interested in implementing FMECA will have access to this thesis.

Apart from the HYPSO team, stakeholders include the bachelor group, the supervisor, NTNU AMOS, Orbit and the media. See attachment number 7.5 for a visualized stakeholder analysis.

Chapter 2

Theory

This chapter contains theory related to this thesis. It starts off looking at risk management and FMECA in general. These sections build a foundation for analyzing the risk management in the HYPSO project. They also explain why and how FMECA is used and why FMECA is applicable in this project. Then the FMECA method is discussed, including success factors. The last section of the theory chapter is dedicated to back up the findings in project goal 6.(chapter 5.6)

2.1 Risk Management

In all kinds of projects and operation there will be some degree of risk of failure. Risk is what you get if you combine the consequence caused by the failure with the probability of the failure. It is impossible to avoid. However, learning how to handle risk is essential for the project's success. Risk handled the right way will minimize setbacks and economic loss in the long run. This is where risk management comes in.

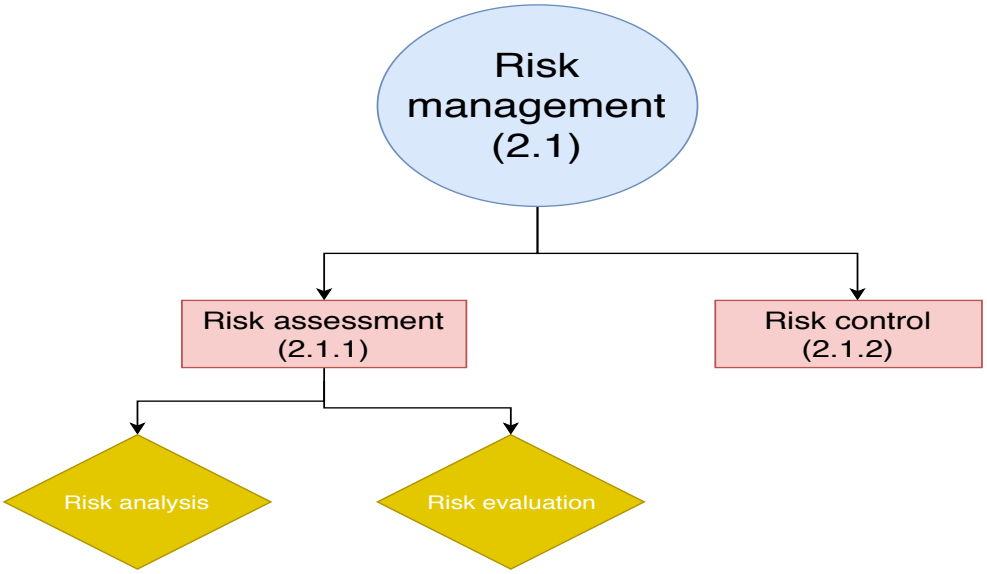


Figure 2.1: Concepts of risk management

Risk management is an integrated process, and consists of **risk assessments** and **risk control**[30].

2.1.1 Risk Assessment

Risk assessment provides insight about how likely a system is to fail, and what the consequence will be. Risk assessments provides the answer to the following three questions:

1. *"What can go wrong within an engineering system?*
2. *How likely is the failure to happen?*
3. *What will be caused by the failure as a consequence?"*

([23], p.4)

Risk assessment can be divided into risk analysis and risk evaluation.

Risk analysis is about identifying hazards and estimating risk in regards to

people, property or the environment. Risk analysis also includes identifying the cause, effect and probability of the hazard. Risk analysis may be qualitative or quantitative depending on the situation. In a quantitative analysis the probability and/or consequences of failure are represented by numbers. In a qualitative approach the probabilities and consequences of failure are determined without using numerical parameters[30].

Risk evaluation is where the acceptability of the risks are evaluated. Factors like economics, reputations of businesses and environmental consequences are included in the evaluation. In the establishment of a risk assessment, the risk evaluation criteria is set. The team compares the risk based on the criteria, and decides whether to take action or not[30].

2.1.2 Risk Control

If the team finds the risk too high, they want to find countermeasures to reduce the probability to an acceptable level. If that is not possible, they need to find ways to mitigate the consequences. This is called **risk control**. Risk control is the most important part of risk management. How the company or organization proceeds to avoid or mitigate the risks will have a big impact on the results of the project. It is important to keep in mind that with avoidance of some types of risk follows potential loss in success [30] [32].

2.1.3 Other Concepts in Risk Management

Risk identification: When an engineer is designing a system, it is crucial to understand the limits and breaking points of the design. By identifying every mechanism that can possibly fail, the potential risks can be minimized during the design phase. Therefore, the first step for identifying risks is a description of the system, and the system's interference with the environments.

Risk acceptability is a level of uncertainty that can be controlled throughout the systems entire life cycle.

There are several types of risk management tools and methods, some of them described later in this chapter. The different types of risk management methods have more or less the same purpose and are performed in a similar way. There are five general steps of risk management. **The five steps are:**

1. Identify the hazards.
2. Decide who might be harmed and how.
3. Evaluate the risks and decide control measures.
4. Record your findings and implement them.
5. Review your assessment and update if necessary.

Research shows that the financial benefits from risk management is less dependent on what method you are using, but more about the frequency and how you do it [32].

2.2 FMECA and its Purpose

FMECA is a method to *"solve potential problems in a system before acting"* (SEMATECH1992)

FMECA is categorized as a risk assessment tool or a risk management tool, dependent on whether you do risk minimizing actions or not.

Failure Mode, Effects and Criticality Analysis (FMECA), was first developed by the US military in 1940 with the release of the standard MIL-P-1629. The method was further developed by NASA during the Cold War. [25] Because of its origin, FMECA is widely used for risk management in space missions.

FMECA is organized and relatively easy to understand and perform. Summarized you (1.)start with collecting information about the system to be analyzed, determine ground rules, evaluation criteria and determine assumptions of the analysis. (2.)Then you brainstorm failure modes, organize them the most expedient way, and analyze them. (3.)Lastly you rank the failure modes and finds countermeasures to avoid them or mitigate the consequences.

2.2.1 Purpose

As a risk management tool, FMECA has several purposes in order to keep control over certain factors.

The purpose of FMECA itself is to localize, organize and highlight as many ways a system can fail as possible, and prevent or mitigate these failures. Before a project starts, or in the initial stages, is it common to perform a short risk assessment to map out potential obstacles. Because of its simplicity and flexibility, FMECA is well suited for this purpose. In fact, the method is one of the most widely used in reliability analysis of initial stages of a general design process.[30] In later stages of projects, FMECA is used to revise and insure the reliability of components before manufacturing and usage.

Another important purpose of FMECA is the documentation of a risk assessment. If a project should fail in a way that it is causing damage to people or materials, insurance companies often demands some sort of documentation of mitigation/barriers of incidents.

Risk management is deeply integrated in the overall project management. FMECA can be used as foundation for developing a maintenance program specific to each individual system. To make decisions over what factors to pay attention to and take control over in order to secure desirable outcome, FMECA is useful.

2.2.2 Concepts

FMECA contains some important concepts that are important to understand in order to succeed in performing an FMECA. Here follows an explanation of some important concepts in FMECA illustrated by a fire alarm.

- **Function** is described by the dictionary as an activity or purpose natural to or the purpose intended for a person or thing.

  Example of a function: A smoke detector's function is to alert when there is smoke, and not alert when there are no smoke.

- **Failure mode** is defined as the partial or full absence of a function.

  A failure mode occurs when:

  1. Preferred action is not happening at all, because of an unintentional error.
  2. Preferred action is happening at the wrong time or with wrong duration, causing an unwanted effect.
  3. There is an error related to the instruments. An instrument is for some reason giving incorrect data or reading[22].

  Example of a failure mode: The smoke detector not alerting during a fire is a failure mode. The smoke detector alerting when there is no fire is another failure mode.

- **Failure effect** is the consequence of a failure mode. How will the failure mode influence main function and other units?

  Example of a failure effect: If the fire detector does not detect smoke, a failure effect can that the fire develops unnoticed.

- **Failure cause** is the circumstances during specification, design, manufacture, installation, use or maintenance that result in failure.

  Example of failure cause: Lack of batteries in the fire detector, or error in the speaker.

- **RPN** stands for Risk Priority Number.

  "An essential element of risk is the uncertainty - the fact that engineers don't know exactly what failures will occur. However, if we can not express what we know in the form of numbers, we really don't know much about it. If we don't know much about it, we can not expect to optimally control it. That is why we need to quantify potential failures."([23], p.4)

  When performing an analysis, each failure mode gets a Severity, Probability and Detection number based on criteria made in the first part of the analysis. RPN is used in the quantitative approach of FMECA. The RPN says a lot about the failure mode and is a decisive part of the analysis. In order to get an accurate measure the scale needs to be balanced. For example if the occurrence scale gives a score too high compared to consequence, failure modes with a high probability but low consequence will get a high RPN. This can change the results of the FMECA. The RPN is calculated by formula 2.1

  $$RPN = Severity * Occurrence * Detection \tag{2.1}$$

  Components with a high RPN ranking, is typically critical for the system performance, and should be paid special attention to [22].

2.3 Types of FMECA

There are several types of FMECA, varying after what type of system being analyzed, phase of the design process and the goal of the analysis. E.g, a different approach is used in the initial design stages than in the final design review. Based on the standard MIL-STD-1629A, the two main types are **function FMECA**, also called top-down, and **Hardware** approach or Bottom-up. Other standards and websites define other types of FMECA such as the website FMEA-FMECA.com[2] defines process FMECA, design FMECA and concept FMECA as the most common types. Each FMECA follows mostly the same approach, but have slightly different

goals and focusing at different factors of the system.

Function FMECA is usually used in initial stages, when the design is still unclear. By creating some sort of function hierarchy, for example a block diagram or a function tree of a system, and analyze how these functions might fail, will clarify risks and provide guidelines for the design.

Hardware FMECA is used in a later phase of the project. When the design starts to take form, you switch the direction of the FMECA build up. Instead of starting at the top of the main system and work your way down to the components, you start on the bottom and analyze the components. What level of subsystem you analyze depends how close to the final design the project has come. Earlier in the design phase, frequent changes are made, and a high detailed FMECA will get outdated quickly and be a waste of resources. On the other hand, a low level analysis late, is less likely to detect new failure modes.

Some standards also mention **Process FMECA** as a third main FMECA. Process FMECA is normally used to analyze manufacturing and assembly processes, focusing on finding failure modes caused by manufacturing or assembly process deficiencies [3].

2.3.1 Standards

To utilize the full potential in FMECA, it is necessary to perform the analysis several times. Overlooked failure modes typically keeps showing up every time an FMECA is conducted. Furthermore, former FMECAs are an important part of the base for improvements of the design, and new FMECA is conducted to analyze current state. In order to be able to compare former and current state, its essential that the FMECA is done the same way every time.

FMECA is a method used worldwide in all kinds of ways and contexts. There exists hundreds of standards. The oldest, most recognized standards originates from

the military and space industry.

These are some examples of existing standards: [16] [12]

- MIL-STD-1629A, (1980) "Procedures for performing a failure mode and effect analysis";
- MIL-STD-1543B(1988) "Reliability program requirements for Space and Launch Vehicles";
- ECSS-Q-30-02C(2009) "Space product assurance – Dependability, FME(C)A";
- SEMATECH (1992) "Failure Modes and Effects Analysis (FMEA): A Guide for Continuous Improvement for the Semiconductor Equipment Industry".

Which standard being used is more about preference and less about standard. FMECAs differ between different industries, and most large companies develop and use their own standard specialized for their needs. In this thesis, the standards found most relevant for extracting knowledge and requirements for FMECA were chosen, and used to tailor a method for the HYPSO satellite.

2.3.2 Pros and Cons

In this section we look at the strengths and weaknesses of FMECA as a risk management tool. Other risk assessments are also described and compared to FMECA.

In general we consider FMECA **pros** as:

- Structured and reliable method for hardware and system analysis;
- Simple concept, requires little training and prior knowledge;
- Makes analysis of complicated systems easy.

FMECA **cons**:

- Can be time-consuming and resource-intensive;
- Not suitable for finding consistency when several errors occur simultaneously;
- Does not take into account human error.

Hazard analysis is a type of risk assessment similar to FMECA. The difference is where FMECA strive to identify all failure modes from a function perspective, Hazard analysis only identifies hazards. A Hazard analysis is better suited in situations where people are more involved, for examples at a hospital. [10].

There are several types of **Risk analyses methods.** RAMP, SHAMPU and RFA are examples of this. A stand alone risk analysis examines specific aspects of a project and attempts to map out the risks. One typical approach like Shape, Harness, And Manage Project Uncertainty(SHAMPU), take base in some specific keywords such as humans, environment, capital, etc, and list every risk attached to those. Other approaches like Risk Factor Analysis(RFA) focuses more on scenarios and potential negative outcome. This way of considering risk is better suited in less specific projects. It is more used when analyzing strategies and plans[4].

2.4 Success Factors

Due to the structural and organized approach, FMECA is in principle a very simple and straight forward tool to use. Still, there are some pitfalls to look out for. To achieve better results and higher probability for success we have included this section listing some proven success factors. C.Carlsons from Accendo Reliability identified these 6 success factors[15]:

1. **Understanding the fundamentals and procedures of FMECA, including the concepts and definitions.** An FMECA process includes lots of comparisons and repeated actions. As mentioned above in the section about standardization, it is important that all failure modes are analyzed the same

way every time. If the team fails to achieve a standardized approach, the result will be less correct and the value of the analysis limited.

2. **Selecting the right FMECA projects.** The benefits from an FMECA variate from situation to situation. FMECA demands a lot of resources, like time and documentation. Performing FMECA on the right systems at the right time is important to maximize the effect and optimize the resource usage.

3. **Preparation steps for each FMECA project.** Without paying attention to the scope of the analysis, the FMECA has a tendency to grow out of scale. Properly preparation, deciding the scope and make it visible (e.g block diagram), determine assumptions and ground rules, gather the right team and relevant information is necessary to a high quality, efficient process.

4. **Applying lessons learned and quality objectives.** FMECA is a repeated process and learning from former mistakes and success is a decisive to improve the process.

5. **Qualified facilitation.** Achieving the goals and desired result of an FMECA is challenging. A leader or facilitator has shown to be an important factor to hit the targets of the analysis.

6. **Implementing an effective company-wide FMECA process.** FMECA is an interdisciplinary process, and to get complete and solid results it is very favorable to get input from all departments/sections within a project.

2.5 General Method

The method of FMECA is to systematic find all failure modes of the system to be analyzed, the cause, the effect and eventually countermeasures. Here follows a general approach based on the standards mentioned, independent of type of FMECA. **This is part of the answer of project goal 4**.

In order to perform an FMECA there are three main phases, each containing several steps:

1. Preparation
    - Define the scope;
    - System missions and functions;
    - Collecting relevant data and information;
    - Define ground rules;
    - System structure analysis;
    - Team gathering;
    - FMECA worksheet.
2. Workshop
    - Brainstorming.
3. Review and Corrective actions
    - Review;
    - Corrective actions.

2.5.1 Phase 1: Preparation

Most of the work of the FMECA analysis is in the preparation phase. In order draw the right conclusions and get a best possible result, the base of the review needs to be good. To be able to perform the analysis, some prerequisites needs to be met. **The scope** of the analysis needs to be defined. Which parts and subsystems should be included in the analysis. **System mission and functions** needs to be defined, and **Environmental conditions** need to be considered. When the boundaries of the system, main missions and environmental conditions are defined and considered, it is time to **collect available information** about the system being analyzed.

This includes drawings, components lists, descriptions, interface information, etc. **Information about former similar design**, and interviews with personnel with relevant experience could also be beneficial[26].

Ground rules of the analysis needs to be set. It needs to be decided if the analysis uses a qualitative approach or a quantitative approach. If quantitative risk evaluation, the RPN scales needs to be defined[16].

Before the analysis can start a **System structure analysis** needs to be performed. A system structure analysis divides the system into manageable units. The level of detail and content of the units varying after the objective of the analysis. The system structure is often illustrated by a component hierarchical tree or a function block diagram.

The team gathered depends on the system being analyzed. But in general you want an interdisciplinary group with relevant knowledge of the system. Other qualifications that is beneficial to the team is a leader or person with power to push actions and bring in some load to the analysis. It can also be favorable to include an individual with little or no connection to the project to get a different point of view[31][30].

The layout of the **Worksheet** is decided in the preparation phase. The worksheet is used during the review and needs to be comparable/ the same from FMECA to FMECA in order to achieve the wanted outcome. A standardized FMECA worksheet contains cause, effect, criticality analysis (e.g RPN) and countermeasures. Usually, general information such as date, type of FMECA, participants, responsible are included as well.

System: Performed by:

Ref. drawing no.: Date: Page: of

Description of unit			Description of failure			Effect of failure		Failure rate	Severity ranking	Risk reducing measures	Comments
Ref. no	Function	Opera-tional mode	Failure mode	Failure cause or mechanism	Detection of failure	On the subsystem	On the system function				
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)

Figure 2.2: Example of a traditional standardized FMECA worksheet

2.5.2 Phase 2: Workshop/Analysis

The workshops starts with a **brainstorming**. The system, subsystems or components in the scope of the analysis are listed with its appertaining functions. The workshop team looks at each unit and tries to find every way each unit can fail its function or mission. These failure modes are then sorted, organized and filled into the FMECA worksheet[31].

In the **Worksheet** all failure modes are being analyzed one at the time. Every failure mode is analyzed as if that was the only failure in the system[26].

2.5.3 Phase 3: Review and Corrective Actions

When the brainstorming is complete, a **review** is performed. In the review the team studies the criticality of the failure modes, and decides whether or not the risk is acceptable. If not acceptable, the team finds countermeasures to reducing the likelihood of occurrence, reduce the effect of failure or/and increasing the detectability before the failure occurs [30].

After the system is improved and **corrective actions** are conducted, the new state is analyzed and the worksheet updated. The actions are typically design changes, safety features and safety devices, warning devices, training, etc.

2.6 Industry 4.0, and FMECA in The Future?

This section will discuss shortly how FMECA is standing the test of time.

The last decade we have seen a big change in use of technology, improving productivity and quality of factories. As new technology are being utilized, products and systems are getting more and more complicated. As a result of change in technology, increasing competition and diminishing margins Risk management is getting more and more important. This leads to the demand of more flexible and precise production, contributing to a higher level of system control. Failures and mistakes can create big damage and lead to decisive losses.

The current digital revolution is called Industry 4.0 and includes concepts as sensors, Internet of Things, predictive maintenance, cyber-physical systems, machine learning, Artificial Intelligence and so on. This technology opens up for possibilities such as continuous regulations, digital wireless control and communications and also continuous risk management.

FMECA as a tool can be adjusted after different objectives and targets. RPN scales can be adjusted, different situations gives different functions to analyze, etc. Due to this flexibility of FMECA, the methods is adapting in several ways. Digitization makes it possible to perform, update and make changes to FMECA across platform and from different locations. Computers opens up for different ways to build and perform analysis. Statistical data of components gets available, workshops can be held online, worksheets can be made in several dimensions, etc.

Another big change that comes with digitization, is the extended use of software. Most of the functions in a lot of systems lies in the software. As a consequence, bad

software performance and software-hardware interaction failures is now a huge part of the total failures. Just in the USA, IT failures costs the U.S. economy about 50 - 150 billion dollars every year[11].

In order to mitigate these losses, companies uses software FMECA(sFMECA) and HSIA(Hardware software interface analysis). SFMECA is traditional FMECA that focuses on identifying and mitigation of software failure modes. HSIA is a tool to identify software response to hardware failure and can be used as an extension to sFMECA.[14] Using the results from sFMECA and HSIA, it is possible to build a FDIR(Fault detection, isolation, and recovery) plan. A FDIR plan creates barriers against consequences and the plan is executed if failures are detected. The goal of FDIR is automated self repair or some sort of shutdown/safe mode/lockout before the failure develops and consequences gets big. [12]

2.7 Theory Related to Chosen Failure Modes

This section is meant as a short explanation to the failure modes mentioned in chapter 5.6, and is not related to FMECA theory.

2.7.1 Outgassing

The lack of hydrostatic pressure in space and outer layers of the atmosphere have an effect on materials. Gas particles trapped inside the macro structure of the material can precipitate, and latch or "condensate", on to other parts of the space carriage. This phenomena is referred to as outgassing. Since there is no way to clean the space carriage, outgassing can ruin optical missions. There exists a standard containing outgassing data for space approved materials [7].

2.7.2 Radiation Effect on Optical Glass and Lenses

Ionization effects by radiation on optical glasses and lenses is a field of study which have been researched since the 1960, and is still not fully understood. The mechanism is referred to as "color centres". The radiation effects the crystal structure in the glass, and changes the glass' ability to absorb light. This means that over time, glass exposed to radiation will not let certain wavelengths pass through, or pass through less effectively[21].

2.7.3 Watchdog Timer

A watchdog timer is a hardware device that automatically resets the computer if a software malfunction occurs. The timer has a set maximum value, and if the watchdog gets no response from the computer within the given time, the computer resets, either to a safe mode or just reboots the software[9].

Chapter 3

Method

This chapter contains a description of the methodology used in this bachelor thesis, in order to reach the project goals set in chapter 1.3. The first section contains a general method description. The second section contains a methodology description for each project goal.

Accessing and understanding information is a large part of this project. Implementing FMECA requires detailed information about the engineering and functionality of the system in question. In this case, a large part of the satellites mission requirements are dependant on software. This is a field of study the students in this bachelor group has little knowledge of. This also applies to other parts of the satellite. Collaboration with the rest of the HYPSO-team is therefore crucial for getting the FMECAs as accurate as possible.

3.1 Methods

This section contains a general, short description of the methods and tools used in the process of performing the FMECAs.

3.1.1 Literature Search

A systematic method for searching literature helps increase the efficiency of the process and the credibility of the sources used. In this project, a semi-systematic approach could be used. Defining certain keywords and search engines limits the searching process. A searching plan can then be developed, and the literature search part of the assignment can this way get a finite ending date. In addition, when the approach is semi-systematic, information can later be supplied by searching later, and not according to the plan if needed[24].

3.1.2 Document review

The HYPSO team uses a cloud storage, Google drive, to store engineering documents of the satellite, flowcharts, mission analysis reports, and other relevant information. The volume of documents are relatively large. Every member of the team stores their work on this drive. It is therefore important to have a plan when searching for relevant information, to ensure we are not wasting time or using outdated information. This can be done through getting recommendations for what documents are the most relevant, and using key words to search for documents.

3.1.3 Workshops

Workshops are effective ways to utilize the participants expertise. Delegating work according to field of study, and getting people to work in teams help increase productivity. The key to getting a good workshop, is to distribute the time teaching and the time working correctly. The time teaching should be as little as possible, without this causing the participants to not understand the task given. The main focus should be working and finding solutions. [1]

3.1.4 Qualitative Interviews

A great tool for gathering information quickly are qualitative interviews. In an interview you can single out only the information that you want to know. There are however **weaknesses** to this method. The **credibility** of the information varies with the person interviewed and how many objects that are interviewed. Many objects often makes the interview quantitative. Interviews can also be biased, depending on the subject of the interviews.

There are several types of interviews. **Structured interviews** have predetermined questions, and a strict script. **Unstructured interviews** are often unprepared, and the conversation runs freely. **Semi-structured interviews** have some elements from both the previous types. Some key points are prepared in advance, but the conversation will often run freely[5].

In this assignment, where system knowledge is key, semi-structured interviews are the most appropriate way. The bachelor group can prepare the most questions in advance. However, since the tone of the interview is open, the object can point out things that the bachelor group may have overlooked or interpreted wrong due to lack of understanding.

3.2 Methodology

This section contains a detailed, step by step description of how the bachelor group solved each project goal.

3.2.1 Project goal 1: Situational analysis of the HYPSO teams current level of risk assessment.

Understanding the early risk assessments and to what extent risk had been considered in the HYPSO project was a key to get started with FMECA preparations. To find answers, we reviewed important documents on the HYPSO drive, as well as conducting semi-structured interviews with several candidates. We could only find one document, that had some level of general risk assessment. The document was:

- Mission analysis report MAR 001.

Semi-structured interviews were also conducted with several members of the HYPSO team. After the interview process, we had all the information necessary to write a situational analysis. The analysis focused on the current situation of risk assessments in the project and competence in the field at the time of the groups involvement. From interviews we also found out what was wanted from us, in terms of solving the problem at hand.

3.2.2 Project goal 2: Create a Simple Technical Description of The HYPSO Satellite

In order to give an technical description of the satellite, we took advantage of the provided documents from the cloud storage through document review. System Design Report[29] and Mechanical Design Report[19] contained some drawings and descriptions. We also utilized information from the satellite bus manufacturer, NanoAvionic's, website. In addition to this, we gathered the remaining necessary information through semi-structured interviews and conversations with members the HYPSO-team.

3.2.3 Project goal 3: Identify Suitable Standards for Conducting FMECA in This Specific Project

To identify suitable standards we used literature search. Documents from ESA accessed through the HYPSO Drive was used, but also Google search and a select few tech reports were used to localize standards. We were able to locate and read through six to eight different standards. By this point in the project we learned that standardization within a project is more important than what standards that were used. We therefore ended up choosing and mixing information from different standards, tailoring a standardized approach, useful for the HYPSO satellite.

A limitation in the early phase of the project was some standards being locked behind payment.

Standards reviewed are listed in Chapter 2.3.1.

3.2.4 Project goal 4: Defining Steps and Success Factors

1. ***Describe the steps in a FMECA according to said standard***
2. ***Define success factors for implementing FMECA in a project***

1. As pointed out in the last subsection we didn't stick to one standard, but gathered and used information from several. In order to describe the steps in the FMECA, we used the general description, chapter 2.5 as base, and made modifications more suited for the HYPSO project. These modifications were done based on variants found in standards, advising from experienced people and own ideas.
2. Through reading and advising we came across several success factors. There are success factors included in standards, articles and tech reports of FMECA. We also got some advises based on experience from people interviewed.

3.2.5 Project goal 5: Plan and Conduct FMECA

This delivery goal was really a product of the previous goals. A lot of the planning consisted of getting to know the project, understanding the engineering of the satellite, and identifying or creating useful standardized approaches for conducting the FMECA. We had to figure out the purpose of FMECA in this specific project, what people were available and how to build up the workshop. By looking into standards, applicable literature and information from conversations, we got an idea what people to include in the workshop in order to cover the required spread in competence. The situational analysis helped determine the participants in the workshop.

Another big part of conducting the FMECAs was to plan and prepare the practical aspect of the workshops. How many people attending, how to distribute the workload, and so on. To practise and test this situation, the bachelor group did two test runs of a FMECA workshop internally, using a fire alarm system as an example. This turned out to be very useful, making the group more prepared for the actual workshop.

3.2.6 Project goal 6: Choose 5 Critical Failure Modes on the HYPSO Satellite and Discuss Possible Mitigation of Risk

For choosing the most critical component, we used an **analytic approach**. Each failure mode in the FMECA was assigned a risk priority number(RPN). This is common in some variants of FMECA, and is used as a way to highlight critical components. **The failure modes we chose to single out as critical were the ones with a RPN 09 and above.** This was a number we felt represented a high rate of occurrence, and severity. To get certain points of mitigating risk, we had unstructured interviews with the relevant people, according to field of study.

3.3 Credibility of methods and methodology

This section discusses the credibility of the methods used, and the approach used to get reliable information.

To ensure the credibility of the theory used, we limited our document review and literature search to reliable sources. Exceptions were made in some situations, whereas the group had to do open Google searches. This is due to the fact that some information concerning relevant space technology can be difficult to find in the library. However, some reliable information is obtainable from sources like NASA and Avionics. The bachelor group tried mainly to use these.

Another part of the credibility issue is the information specifically used in the FMECA. Failure modes, causes and effects are found by fellow students, and may be flawed information. However, students in this project are studying for a MSc or PhD, and are competent in their field of study. It is also the best information we can get, due to limited public information concerning failure causes for spacecrafts. Some information about reliability of Cubesats were obtained though a ESA workshop in Belgium, where a co student were in attending, but it turned out to have little or no relevance for the HYPSO satellite.

Another credibility issue is surrounding the tests done on different components of the satellite. Space environment can be hard to recreate, and this effects test results. However, the HYPSO team had a radiation resilience test done in Denmark, which the group has used to highlight the risk of one of the failure modes discussed in section 5.6. This was considered a thorough test. However, the results should be considered closely, as the radiation intensity in space is hard to estimate, due to its variation.

Chapter 4

Situational Analysis

This chapter contains the results of project goal one and two.

This chapter contains a situational analysis of the HYPSO-team. A situational analysis is a description of the current state of the problem that is to be solved.

The purpose of the situational analysis is to better understand what HYPSO-team have already done in terms of risk assessments, and their needs in order to reach the mission success criteria. Another important purpose of this analysis is to collect necessary background material in order to build and facilitate a FMECA on the HYPSO satellite, including a technical description of the satellite.

Our goals with this analysis are:

1. Understand how the HYPSO-team is organized. More specifically, we want to figure out who is in charge of different areas and what field specific competence exists within the team.
2. Figure out what risk assessments that have been done.
3. Get an overview over how far the project has come. When is the launch/deadline date and what is the current phase of the project.
4. Collect enough background material necessary to prepare and perform a FMECA.

This contains a technical description of the satellite and mission success criteria.

5. What type of FMECA could benefit the project, and what does the leadership want concerning FMECA.

4.1 Organization

This section describes how the HYPSO project and team is organized, what the current phase of the project is and our role and purpose in this project.

4.1.1 Project Organization

The HYPSO team is going to deliver a satellite to AMOS, with hyper spectral imaging functions and plan to build several satellites in the course of a couple of years. The HYPSO-team consists of mainly master students and PhD candidates, as well as 3 different bachelor groups. The project leader, Evenlyn Honorè-Livermore, is writing a PhD thesis. **Evelyn engaged the bachelor group, as a measure to highlight and mitigate risk in the HYPSO-project.**

The HYPSO-team is fairly unstable. This is due to most of the members of the team writing their finishing thesis, and will graduate in the summer. New members will then be recruited, making change in personnel common.

The HYPSO team has a hierarchy based on the different fields of study involved in the engineering of the satellite. The hierarchy is branched in different categories, shown in figure 4.1

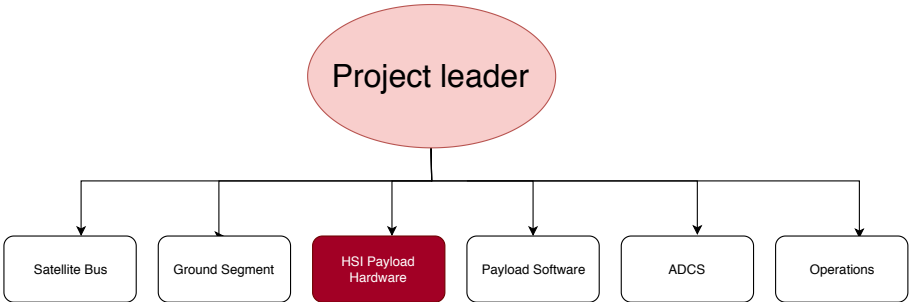


Figure 4.1: Different branches in the HYPSO project

Evelyn is also the leader of HSI payload: hardware, which is the work group the bachelor group is a part of, marked in red.

4.1.2 How Far the Project Has Come

The HYPSO project was officially started 23rd of August 2018. The initial phase mainly consisted of mission analysis, tests, and design. At the point of the groups involvement, in December 2018, most of the mechanical design for a prototype was already decided. Although several design revision was likely to happen, the bachelor group was not involved in the early design phase. On the software side, coding towards meeting mission success criteria was still active. The launch has been postponed, and is to be determined. It is assumed in mid to late 2020.

4.1.3 Competency

There is limited competence on risk management in the HYPSO-team. The project manager, Evelyn Honorè-Livermore has some experience in risk management, through previous work relations.

Other than that, the team has little to no competence in the field of risk assessment, hence the bachelor groups involvement in the project.

The different fields of study represented in the team are:

- Computer sciences;
- Cybernetics;
- Mechanical engineering;
- Material science and engineering;
- Electrical/systems engineering;
- Management.

4.1.4 The bachelor Groups Role

The bachelor group was as previously mentioned brought in to highlight and mitigate risk in the project. This will be done through conducting one or more FMECAs on the HYPSO satellite system. The FMECAs will single out critical components, and act as a overview of potential failure modes and causes.

In addition, the group is going to make a documented, step by step description of how a FMECA is prepared and done, tailored to this project. This is for enabling FMECA to be implemented in an earlier stage on the remaining satellites that will be built later on in the HYPSO project.

The bachelor groups role is rooted with the project leader, as she brought the group into the project. This is positive in the sense that the FMECA have priority high up in the hierarchy, which can potentially make planning and conducting workshops easier.

4.2 Risk Assessments

Before the group was involved in the HYPSO-project, a risk evaluation had already been done. A separate Risk work sheet was also created. These risk assessments

lacked actual content, and only contained a list of attendees. The bachelor group has no previous risk assessment to work with. However, it became clear that risk has been a topic of conversation between several participants in the HYPSO-project. Some points of risk are mentioned in different engineering documents, but with no apparent system. This means the bachelor group has to talk with individuals working with these documents, extract the information and document this. Workshops will also be used to gather and document information.

4.3 Technical Description of HYPSO

This chapter contains a limited description of the HYPSO satellite. The purpose for this description is to provide an overview in how the satellite is designed to best meet the mission success criteria(4.4), and what function each subsystem has. The functionality of the different subsystems created the base for the scope of FMECA 1.

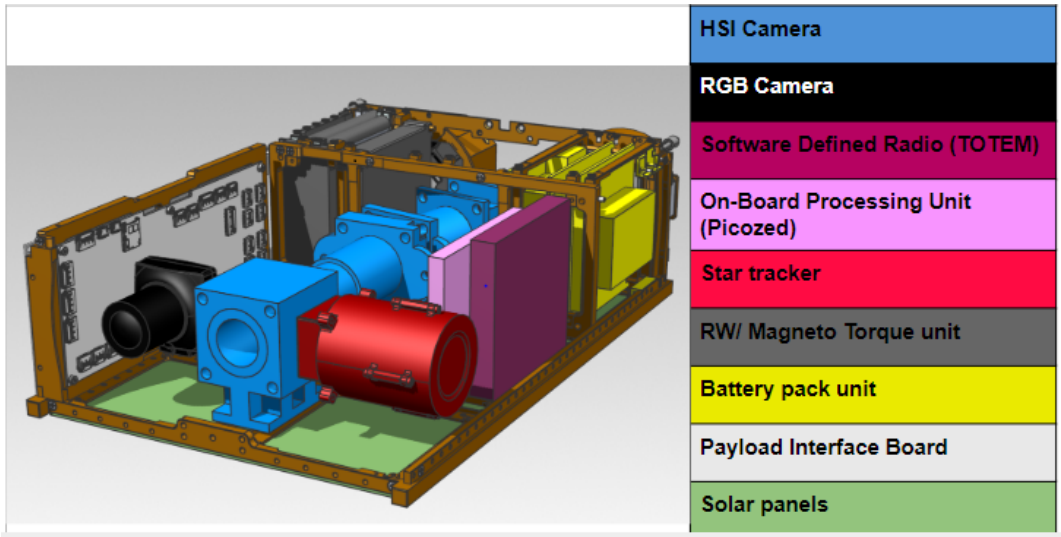


Figure 4.2: The HYPSO satellites different subsystems

4.3.1 CubeSat

The CubeSat-project started as an initiative from California Polytechnic State University and Stanford to provide affordable access to space for the university science community. This new standardized platform has fulfilled its purpose, and has lead to several space programs in different universities around the world.

In 2010 NASA announced the CubeSat Launch Initiative(CSLI) to support CubeSat developers. With this initiative NASA covers most of the cost of providing the satellites ride into space, together with their already planed launches. In exchange for the ride, NASA wants a report on the results of your CubeSat investigation [28].

HYPSO uses the format of a CubeSat. A CubeSat is defined as a nano-satellites whose designs are compliant with the CubeSat Design Specification defined by the CubeSat standard published by California Polytechnic State University in 1999. A CubeSat unit is a cube with size **10x10x10cm** and a satellite consist of 2 to 6 cubes [33]. The specific standards for the CubeSat makes it possible for companies to mass produce components, reducing the costs.

To protect the satellites during launch, it have been developed standardized dispensers. The dispenser work as a cover for the satellite, and releases it into space at appropriate time during the shootout to hit the orbit targeted [28].

The purpose with a CubeSat is [27]: "The primary mission of the CubeSat Program is to provide access to space for small payloads. The primary responsibility of companies developing 6U Dispensers is to ensure the safety of the CubeSat and protect the launch vehicle (LV), primary payload, and other CubeSats during launch."

4.3.2 HYPSO

HYPSO is the satellite SmallSat-lab is working on and follows the CubeSat Design Specification. The spacecraft consist of 6 cubes(20cmx30cmx10cm). The satellites sub assemblies is divided into two groups; Satellite bus-and payload.

Payload is defined as all equipment attached to the satellite except the equipment necessary to operate [8]. In other words, the payload is the components the HYPSO-team is developing and adapting for HYPSO satellite to meet the mission success criteria(4.4).

The bus is a pre-designed frame, with necessary components to operate in space(and meeting the criteria for space environment), made by an Lithuanian initiative called NanoAvionics. The Satellite bus contains the frame, Startracker, Rotation Wheels/Magneto Torque unit, Battery pack unit, Payload Interface Board and Solar panels.

The bus is already mechanically, electrically and functionally tested and ready for payload installation when it arrives from NanoAvionics.[6] The **bus** has a total weight of **4570g** and can fit additional up to 7500g and 4 CubeSat units in payload size.

Frame Interface

The frame interface is constructed as a 3x2x1 unit cage in aerospace Aluminum. Most of the surfaces are anodized to provide hard wearing and protection against short circuit. NanoAvionics has made the frame weight and stiffness optimized to best handle the environment the satellite meet in space. [6] The frame also helps absorbing radiation.

Startracker

The document HYPSO Design Report states that: *"A star tracker is an instrument that tracks the stars in the sky to provide positional and orientational data for the satellite. The star tracker itself is not a separate payload, but a part of the bus. However, it will need to be rigidly coupled to the HSI to ensure compliance with the directional pointing of the main payload."* [29].

The function of the Startracker is to provide angular information. This data in addition to position the GPS provides gives accurate computation of the angle of spacecraft, and gives the images a precise position [17].

ADCS

Contains magnetorquers, rotation wheels, flight controller. The function of the ADCS is to Control the spacecrafts physical motions. It orients the spacecraft towards desired altitude and actuates reaction wheels to perform a slew maneuver. Estimation of the orientation, position and velocity of spacecraft are done autonomously in the flight controller[17].

RW/Magneto Torque unit The Magneto Torque unit consist of two magnetorquer rods in X and Y direction, and one coil in z-direction. These magnet keeps track of the spacecrafts angle compared to the earth's magnetic field. The function of the magnetorquer unit is to control the rotation of the satellite and what surface the HSI camera points towards. Attitude control accuracy is +-2.5 degrees.

Power unit

The battery pack consist of 8 cells with a total energy storage of 12800 mAh/ 92Wh. The voltage supplied is 7.4V. The purpose of the power pack is to store and serve energy to the other subsystems, when its needed over the satellites lifespan.

Solar Panels

The bus is delivered with very high efficient (optimally 29%)solar panels developed for space. They are constructed with high quality materials and follows the clean room environment assembly guidelines from NASA.

The solarpanels are the energy source for the satellite during operation.

Payload Interface Board

The payload interface board is the main bus unit. The function of the board is to connect all the components together and run the software installed. The computer contains a fail-safe mode which will keep the satellite operational even after a micro controller break-down.

4.3.3 Payload

The Payload consist of HSI camera, RGB camera, Software defined Radio (TOTEM) and On-board processing unit (picozed).

Hyper spectral Imaging Camera (HSI)

The main payload of the satellite will be a pushbroom HSI. The HSI camera consists of three assembly systems: Imager, OnBoard Processing unit and Break out Board(BOB).

Imager This imager is designed to be made from COTS parts as to make construction simple, parts readily available and reduce costs. The lens assembly features an angled center section with an integrated grating. The prototype utilizes a cage system to ensure stiffness across the length of the lens assembly, and this proved important for the interface solution chosen[19]. The imager contains 3x50mm VIS-

NIR objectives to focus the light into the grating. The grating fractions the light into the camera head, creating the hyper spectral image.

The function of the imager to perform high resolution hyperspectral imaging and to store data in three dimensions (spatial x, spatial y, spectral)[17].

Figure 4.3: Early design of the HyperSpectral Imager

On Board processing unit

Payload control and data processing is managed by a computer(PicoZed) mounted on a custom carrier board. Onboard processing unit(OPU) is the interface between HSI+BoB and the spacecraft bus[17]. Data from the HSI are processed on an FPGA(gate array) on the OPU (e.g. compression, super-resolution). Data from the imager are huge files, and needs to be processed to be able to sent down to ground stations and interpreted. Successful data processing is a decisive part of mission success. In-house development of software for the PicoZed is a central part of the HYPSO-teams work [19].

Break Out Board(BOB)

The break out board is the board that is the interface between the HSI and the picozed unit.

Software Defined Radio

A software defined radio is a radio where tasks performed by hardware, such as mixing, amplifying, filtering etc, is done by software. Applying this concept to SmallSats can increase data throughput, add the possibility to perform software updates over-the-air and make it possible to reuse the hardware platform for multiple missions with different requirements. The SDR will use a separate UHF monopole antenna to not influence the main communication or data link of the spacecraft[29]. The Software defined radio is not included in the primary mission of hyperspectral imaging, and serves no function in that aspect.

RGB Camera

The USB 2 uEye LE industrial camera with a Kowa, LM6JC, 6 mm, 2/3 lens was presented as an option at the Preview Design Review(PDR), but feedback from the review team proved that more work will have to be done before a final decision of the camera specs can be made.[29]. The camera has larger FoV than HSI but lower spatial resolution[17]. The main function of the RGB camera is to provide color photography of the earth as well as georeferencing for the HSI. This makes the RGB a tertiary mission subsystem.

4.4 Mission Success Criteria

The mission success criteria are important for setting the scope of the FMECA. What is the main purpose of the satellite, and in what way does each subsystem contribute to this? The mission success criteria are parameters indicating whether or not the mission reaches a certain level of success. Setting the objective of the

FMECA based on what is required for full success can be beneficial, in terms of what functions of the different subsystem contributes to this. The mission success criteria in table 4.2 are found in the mission success requirement document on the HYPSO drive, and were set before the groups involvement in the project.[18].

ID	Full / minimum success	Functional area	Definition
MS-0-002	Minimum	Ground, orbit	Mission control shall identify, track and receive telemetry from S/C after 45 min from launcher deploymen
MS-0-003	Minimum	HSI	Shall observe Case 1 and Case 2 waters off the Norwegian of at least 70x70 km^2 area
MS-0-004	Full	HSI	Should observe Case 1 and Case 2 waters globally of at least 70x70 km^2 area
MS-0-005	Full	Orbit	Should image same target at least 3 passes per day
MS-0-006	Minimum	HSI	Shall take at least 1 raw image with less than 160 spectral bands in VIS-NIR
MS-0-007	Full	HSI	Should take at least 1 image with less than 20 spectral bands in VIS-NIR
MS-0-008	Minimum	HSI, ADCS	HSI images shall have at least 300 m spatial resolution
MS-0-009	Full	HSI, ADCS	HSI images should have at least 100 m spatial resolution
MS-0-010	Minimum	ADCS	S/C shall perform along-track slew maneuver at a angular velocity with magnitude of 0.01 deg stability over 60 s
MS-0-011	Full	ADCS	S/C should perform cross-track slew maneuver at a angular velocity with magnitude of 0.01 deg stability over 60 s
MS-0-012	Minimum	HSI, RGB , Operations	Shall downlink 1 hyperspectral images in L1A data format containing detectable optical signatures (Chl-a, CDOM etc.) to be processed on ground
MS-0-013	Minimum	HSI, RGB , Operations	Should downlink 1 operational hyperspectral images in less than 1 hr after successful onboard dimensionality reduction, classification and target detection with certainty of 10 % of positive optical signatures (Chl-a, CDOM etc.) to be ground truthed
MS-0-014	Full	Comms	Shall enable flexible mission planning & scheduling and subsystem updates through

Table 4.2: *Mission success requirements as found in mission requirement report*

4.5 What Type of FMECA to Conduct

After reviewing the lack of properly documented risk evaluations we decided, together with Evelyn, that a function FMECA could benefit the project. The FMECA would have base in a select number of the mission success criteria. The mission success criteria are good indicators of the subsystems ability to preform required

functions. However, the hardware was already designed, so some customization had to be made. This will be described more in depth in chapter 5.5.2. **The FMECA will be used to set new mission requirements**. The mission requirements are requirements set to each subsystem, and is not to be confused with the mission success criteria.

A **Hardware FMECA** on the self designed mechanical interfaces was also desired, as well as the presumed critical optical equipment. This wish was due to the importance of the components, due to their role in the primary mission, which is imaging. The decision process will be described in chapter 5. There was a wish for conducting FMECA on the break-out-board, however big design changes was still being made, and lack of time and manpower available and made us dismiss this FMECA.

Chapter 5

Results

In this chapter, the results will be presented and discussed, project goal by project goal. Some project goals already have their results presented in other chapters. For these goals only the most important findings will be listed in this chapter. We, the bachelor group, will refer to ourselves in first person to avoid confusion.

5.1 Project goal 1: Situational Analysis of the Current Level of Risk Assessment

5.1.1 Findings

- The HYPSO-project lacked properly documented risk assessment. Some documents had an aspect of risk evaluation. However, these documents had no apparent systems, and no information whether or not they were outdated;
- The HYPSO-project had come a long way in terms of design and engineering, and a prototype was almost ready to be assembled at the point of the groups involvement;
- The organization was branched into the work groups(see figure (4.1, chapter

4.1): **Satellite bus, Ground segment, HSI payload: Hardware, Payload:software, ADCS and operations**. The bachelor group was placed in the HSI:Hardware group. Evelyn, the project leader, was the head of this group as well;

- The mission success requirements are listed in chapter 4.4, table 4.2;
- We decided on conducting a function based FMECA, with a hardware structure. We also decided to conduct a more standardized hardware FMECA on the mechanical components and optics.

5.1.2 Discussion

The purpose of this goal was to get an insight in the current situation, and what needed to be done to successfully implement FMECA in the HYPSO-project. The full Situational analysis can be found in chapter 4. The section below contains a discussion on how the findings from the situational analysis determined some of the decisions we made in this assignment.

Even though the project had come a relatively long way at the point of our involvement, and a prototype was designed, the project lacked documented risk assessments for early design and engineering. We thought conducting a functional FMECA would be useful for documenting failure modes and causes. These thoughts were in line with Evelyn's wishes, and led to the scope of FMECA 1. An FMECA based on functionality would most likely uncover failure modes that were already considered. However, getting it all down in a document and actively discussing the results could lead to new ways of interpreting the flaws in the satellite.

The mission success criteria found in chapter 4.4 defined the basis of the scope for this FMECA. Evelyn wanted an FMECA that included the entire cycle from a command was sent from the ground station, until the picture arrived back to the operator, illustrated in figure 5.1. Some of the mission success criteria were as a consequence less relevant, particularly those related to launch.

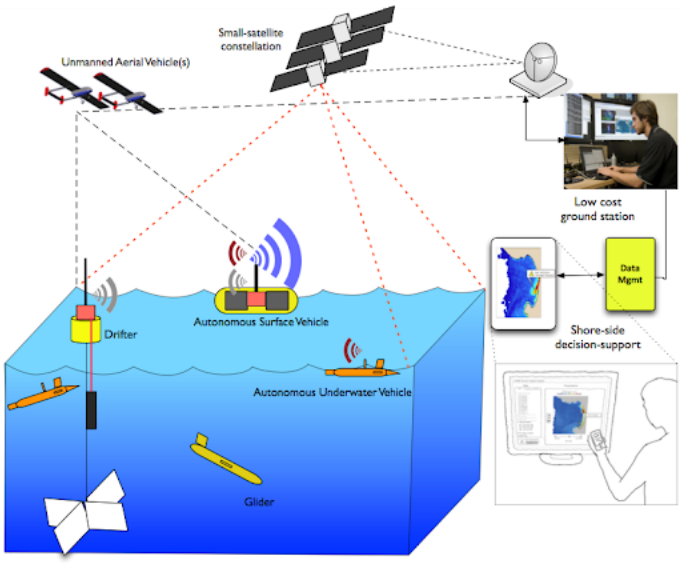


Figure 5.1: Illustration of the complex communication process in the HYPSO-project

Parts of the optical equipment and the mechanical components were designed by the HYPSO-team. These parts are critical to mission success, due to the optics capturing the light and producing the actual image. The mechanical components makes sure the components are in the right place. Considering this, we decided the second FMECA to be a hardware FMECA for these components.

When setting the project goal, we created a list with everything we needed to know from the situational analysis, ensuring we got the necessary information. As we worked at the SmallSat-lab, doing spontaneous and unstructured interviews was a practical way to obtain information. **In hindsight**, more structured interviews with a better documentation could have made the process a bit more efficient, in terms of getting duplicate information from different people. However, using unstructured interviews led the conversation to be open, and gave an overall better insight in the project. This way, we even got extra information we didn't think of asking for.

5.2 Project goal 2: Create a Simple Technical Description of the HYPSO Satellite

5.2.1 Findings

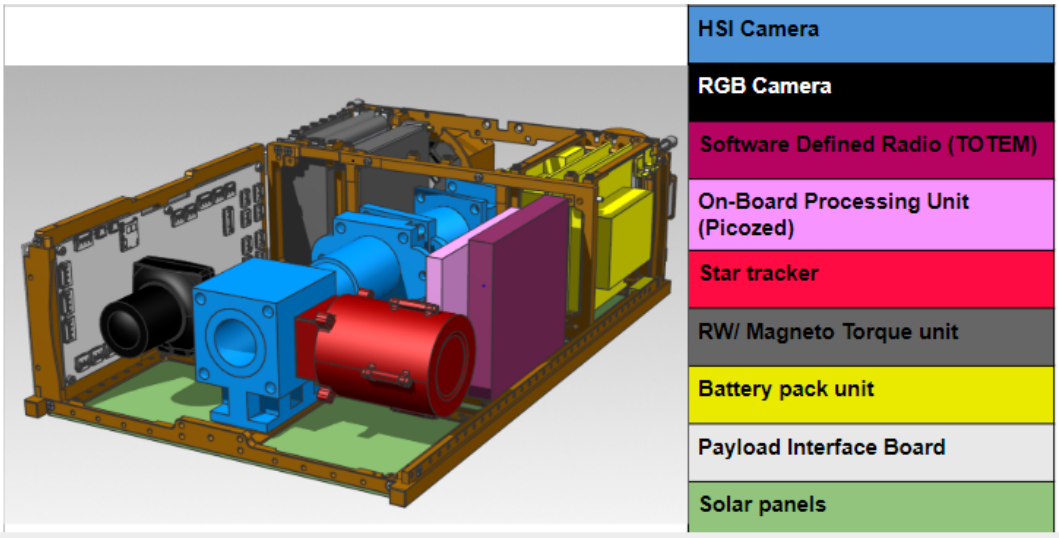


Figure 5.2: The HYPSO satellites different subsystems

See chapter 4.3.2 for detailed description and purposes of each subsystem.

5.2.2 Discussion

Setting the scope is one of the most important parts of the FMECA preparation. To do this effectively, we needed a sufficient understanding of how the satellite is assembled and how it functions. The technical description played an important part in understanding which components or subsystems are essential for reaching mission success.

When creating the technical description, we got to interact with other members of the HYPSO-team. Getting a better understanding of the project, the team members and their thoughts about the satellite's subsystems and components, were useful for planning the FMECAs in terms of who to include in the workshops.

A key enlightenment from this project goal was that we were absolutely dependant on the other members of the HYPSO team in order to conduct the FMECAs. The HYPSO satellite system is complex, and their expertise is essential for ensuring the quality of the FMECA.

Due to a planned document review, getting the information needed to make the technical description was fairly efficient. Some documents contained a lot of the design information. We also knew what members of the HYPSO team to interview due to a good insight in the project structure found in project goal 1.

5.3 Project goal 3: Identify Suitable Standards for Conducting FMECA in this Specific Project

5.3.1 Findings

The standards we found most relevant in this particular project are:

- MIL-STD-1629A, (1980) "Procedures for performing a failure mode and effect analysis";
- ECSS-Q-30-02C(2009) "Space product assurance – Dependability, FME(C)A";
- TOR-2009(8591)-13 "Space Vehicle Failure Modes, Effects, and Criticality Analysis (FMECA) Guide ".

5.3.2 Discussion

As mentioned in 2.3.1, we experienced that it is more important that the procedure of FMECA is standardized rather than following one specific standard. This is somehow mirrored in the established standards, such that they describe more what an FMECA should contain and less what to do step by step. This makes each

standard more or less similar, varying in the description in how to apply to different technical areas, and different processes.

In the results of this project goal we included TOR-2009(8591)-13. This is not an standard, but more a guide how to apply FMECA to space vehicles. The guide takes base in several different standards, among them MIL-STD-1629A. This tech report turned out to be very applicable to our situation, covering more guiding in Software/Hardware interface than the other standards. This is a big part of the satellite systems. The guide also included examples of conduction of different types of FMECAs in systems similar to HYPSO. With reliable references and sources, we consider this document as a solid base.

A **limitation** in this project goal was that some standards are locked by payment. This made the searching process a bit more elaborate.

5.4 Project goal 4: Defining Steps and Success factors

1. ***Describe the steps in a FMECA according to said standard***

5.4.1 Findings

As described in detail in Chapter 2.5 General method, a general FMECA consist of three phases: Preparation, workshop and review.

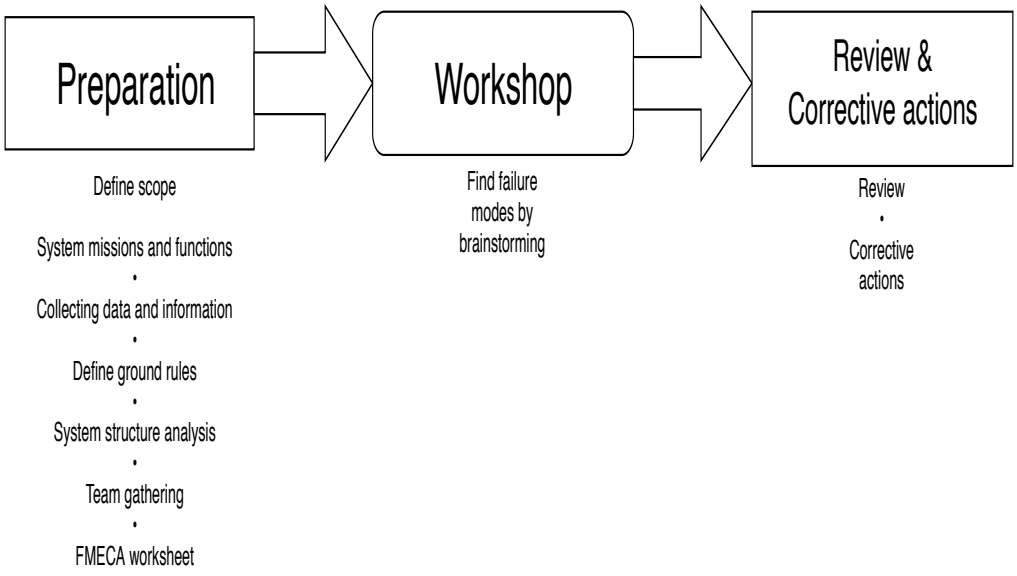


Figure 5.3: General FMECA method

Based on the general process described in chapter 2.5 and the situational analysis, our planned approaches turned out:

Function FMECA

Preparation:

(a) Take base in the project targets/ mission success criteria. Rank each subsystem after their importance in the mission and decide which ones to include in the scope. Use mission success criteria to define the function of every subsystem included in the scope.

(b) Make sure people from each subgroup of the project is included in addition to representatives from the leadership.

(c) Define the RPN scales, concepts, operational phases to include in the scope, design of spreadsheet and time frame of the workshop. The preparation is perhaps the most important step of the entire analysis, and makes sure you get the results you are after.

Workshop and review

(d) Use enough time to explain the purpose of this analysis, and thorough define the concepts of failure mode, cause, effect and RPN. However,

remember it is a workshop, not a lecture.

(e) Start with a limited brainstorming session, listing as many failure modes as possible. We used 10min pr subsystem. An other approach could be 10 min per mission success criteria, though this tends to be less structured.

(f) Sort all failure modes, and discuss criticality and risk mitigating countermeasures. Complete current failure mode before moving over to the next.

In the second FMECA, we used the same base but customized it for a **Hardware approach**:

Preparation

(a) List every component in selected subsystems in a spreadsheet. Detail level is placed as low as possible without any design changes scheduled.

(b) Engage people with the relevant competence. Decide what function each component has.

(c) Include every single phase of the operation during the whole lifespan of the satellite. Consider entire life cycle, i.e, launch, operation, all the way to ended mission.

Workshop and review

(d) List every failure mode possible. Link failure modes directly to the function of component.

(e) Organize and review them component by component. Consider doing this more than once, ensuring the information in the document is as accurate as possible.

Based on our experience from the first two FMECAs, modifications to the approaches were made. The customized approaches are the standardized methods we recommend for the following HYPSO satellites and is attached to the report. See attachment 3 and 4.

5.4.2 Discussion

The target for our first FMECA was to identify and highlight potential failure modes. This was supposed to be a function FMECA at a high detail level, which is an approach usually used in the early stage of a design process. What we did wrong was we started creating a hardware hierarchy, finding each subsystem's function and operational mode. The problem with this was that each subsystem had several different functions in different situations and phases, making the FMECA hard to structurize. After a couple of meetings decided to structurize based on the mission success criteria, limiting the scope to the main subsystems and operational phases.

Because the subsystems were already designed we chose to keep the hardware hierarchy in the FMECA structure. This was necessary to be able to sort the failure modes on the different subsystems, giving the wanted result of the analysis, and the complexity of the system.

We chose to be specific in our approach when it came to gathering the team in the first FMECA. Due to the high level of detail and the project wide scope, representatives from every branch of project were necessary. In this project where the project leader is engaged more or less in the every section of the project, it is very beneficial, if not crucial to include the leadership in the FMECA.

In this situation the necessary ground rules of the analysis was the RPN scales, the layout of the FMECA worksheet and the definitions of the concepts. We assumed basic ground rules of FMECA, such as **"all failure modes is reviewed as that is the only failure"** and similar rules, are followed. The framework in the first FMECA had to include other detail from the scope such as phases analyzed and time frame of the satellite (e.g the whole life span, or just the first year).

We chose to merge **workshop and review** because the brainstorming team and review team was the same. Based on advising from people with experience we chose to add a more detailed description of the workshop than the general

description. This were steps we found necessary to achieve desirable results from the workshop. These details helped to better guide the brainstorming and adapting the approach to the structure chosen.

The **modified standardized approach**(attachment 3) has a similar skeleton. This document is meant as a guide to the coming participants of the HYPSO-team, giving them a document containing the most important factors for implementing FMECA in design. We chose to add more explanations to each step based on our experience, to help the coming HYPSO-team learn from our review.

The main modifications in the preparation phase were to determine and use the purpose of the FMECA more in the preparation, added some specific details about information we found necessary conducting the workshop.

In the workshop and review phase we added some extra steps. It turned out that it was challenging making everyone reviewing the worksheet the same way. This created the need for quality check and follow up. The number of failure modes got high, most of them not critical. We chose therefor to include a critical RPN limit to channelize the resources toward the more critical components. These modifications are further discussed under Discussions 5.5.2.

The second **FMECA, Hardware approach**, were more similar to a traditional hardware approach. A standardized digital worksheet was used, and steps made directly after mentioned standards. Because of this, and the fact that the review team in this analysis had some experience from the first workshop, we left out some steps and went earlier to the conduction.

In the **final standardized approach**(attachment 4) we included some more steps and explanations. The reason for this is that the analysis should be easier to apply without experience from earlier FMECA. This also helps the approach being more standardized, and easier to repeat later.

2. ***Define success factors for implementing FMECA in HYPSO project***

5.4.3 Findings

Success factors may variate from situation to situation, here are the success factors we experienced as most valuable listed, a more detailed list can be found in chapter 2.4:

- Understanding the fundamentals and procedures of FMECA, including the concepts and definitions;
  - Prioritize thorough explanation in the initial phase of the workshop.
- Selecting the right FMECA projects;
  - Right detail level.
- Preparation steps for each FMECA project;
  - Well defined RPN scale;
  - Include the right people in the workshop;
  - Solid structure of the FMECA.
- Applying lessons learned and quality objectives;
  - Test run/experience.
- Qualified facilitation;
  - Control over basic principles in how to conduct FMECA;
  - Flexibility of the management, adapt to the participants of the workshop;
  - Quality check;
  - Follow up during and after the review;
- Implementing an effective company-wide FMECA process.
  - Engagement of leadership.

5.4.4 Discussion

Something that became clear in the beginning of the first workshop was that **Understanding the fundamentals and procedures of FMECA, including the concepts and definitions** is important. FMECA is usually

performed in teams, and reviewed by other people. Different understanding of concepts will yield very different results and interpretations, making the FMECA confusing, rather than helpful. We spent a lot of time introducing the concepts and process of FMECA in the beginning of the first workshop. This information was also available on paper during the workshop. We consider this time well spent since it saved a lot of time and questions later in the workshop. This allowed the participants to work more independently and efficient.

When it comes to **Selecting the right FMECA projects**, we experienced that in order to obtain the best possible result, using the right level of detail is very important. A detail level too high or too low will quickly decrease the quality. In FMECA 1 we potentially set the detail level slightly too low, making the workshop more comprehensive than expected.

Preparation steps for each FMECA project. Well defined RPN scale turned out to be decisive to the quality of the result. Dividing the scale into imprecise section could in worst case scenario have resulted in just 1 and 2. Another important factor was to pick the right team. Fields where knowledge were missing was skipped and resumed at a later time, when the right people were available. Too many people will cause chaos end reduce productivity. In addition to the importance of right defined RPN scale and team assembled, good understanding and a solid reason for the structure of the FMECA. We received several questions how the structure of the FMECA was decided. For example the information that the base of FMECA 1 were mission success criteria was important brainstorm to organize the failure modes.

Conducting and leading an FMECA for the first time felt partial stressful and disorganized. Doing a test run and **Applying lessons learned** prepared us for basic startup problems and helped us avoid these in the workshop.

Qualified facilitation turned out to be more important than expected. Being aware of basic FMECA principles such as considering one single mode isolated at a time, or decide effects both on main functions and on other units

increases efficiency of the process. Adjusting question and scope after group size had a big impact on the result. Asking the right questions, limit the discussion when it was derailed, and pushing it in more quiet setting were crucial to maintain good progress. **Quality check** was also a factor that turned out to be useful. In some situations, some individuals misunderstood the RPN scales, plotting number in different way than the rest, resulting in incomparable numbers. Regular quality check caught these mistakes and we were able to correct them before they led to greater consequences. Another important task for the facilitator is to follow up the review all the way through the project. People forget to complete their part and needs to be reminded now and then to avoid to stop.

Implementing an effective company-wide FMECA process, or in this situation project-wide was necessary due to the project-wide scope in the first FMECA. A function FMECA relies on knowledge from all professions connected to the functions analyzed. Another decisive factor was that engagement from the leadership. People are busy, and some pressure from authorities is necessary to get all people involved prioritize the workshops and reviews.

5.5 Project goal 5: Plan and Conduct FMECA

5.5.1 Findings

The results of our FMECA is attached.

- Attachment nr.1: FMECA 1: Functional;
- Attachment nr.2: FMECA 2: Hardware and optics.

We defined a Risk priority number of 9 and above to be **critcal**

5.5.2 Discussion

FMECA 1: Function approach

The first FMECA was the **Function FMECA**. A function FMECA is usually performed before the hardware system is decided. This is to document and highlight risks in the concept, and avoid bringing these failures into the design. In our case the hardware was designed before we got included in the project. After discussing with advisor and the leadership, we agreed that it still could be beneficial to run a function FMECA on this project. The reasons for this was that there could be basic failure modes overlooked earlier in the project. Developing and testing a function FMECA on HYPSO could benefit later versions of the satellites(HYPSO-2 and so on). In addition, a single document to look up failure modes and causes would be beneficial HYPSO-team.

Since it was too late to perform a pure function FMECA, due to the projects progress, we decided doing a combination of function and Hardware approach. Using mission success criteria defined by the HYPSO-team as base(see chapter 4.4, table 4.2), we connected the subsystems and their functions together. This way, the functions would be the main focus of the analysis, but the hardware structure would also be included. In addition we found the hardware divided system easier to structure compared to the functional system of HYPSO on this level of complexity.

The purpose of the analysis would be figuring out what subsystems could prevent achieving mission success. This was an approach that fit the project well. **The mission success criteria are direct parameters indicating whether mission success is met or not.** By using these criteria as base, we had the FMECA mainly focusing on function, while simultaneously including mission success in the analysis. This ensured the FMECA being directly relevant for the primary mission. The primary mission, or the HSI-mission, is the source of the mission success criteria.

This structure makes the FMECA more complex than a basic function FMECA. More complex in the way that we had to consider a way to divide in to hardware com-

ponents while functionality was the main focus. However, we could justify choosing this combination with more potential benefit for HYPSO. Later versions of HYPSO is recommended to follow more or less the same hardware structure, making this approach a potential standard for this project.

Determining how to divide the entire satellite system into analyzable subsystems with the scope we chose turned out to be difficult. We had to consider both functionality and hardware hierarchy. A basic understanding of the satellite was acquired in the technical description. Using this knowledge, we created a suggestion physical hierarchy diagram, found in figure 5.4.

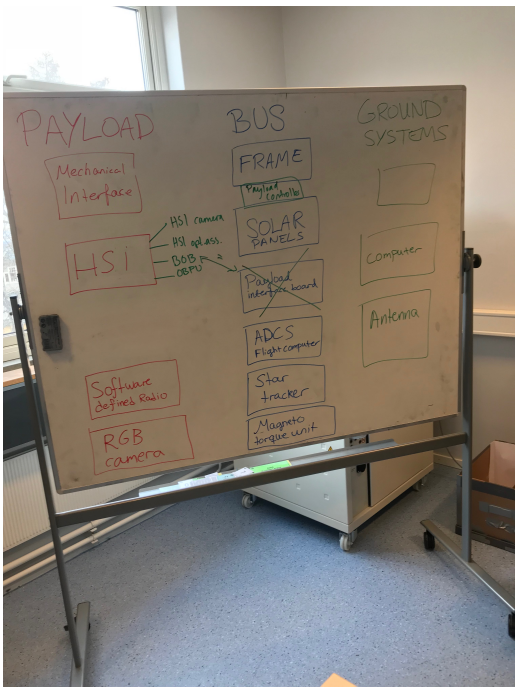


Figure 5.4: First suggestion of physical hierarchy diagram

This figure was flawed on several different levels. Firstly, it gave no real indication of what levels the subsystems were in relation to each other. Secondly, after some review, some of the subsystems listed in figure 5.4 had nothing to do with the mission success criteria. With this knowledge, we created another physical hierarchy diagram.

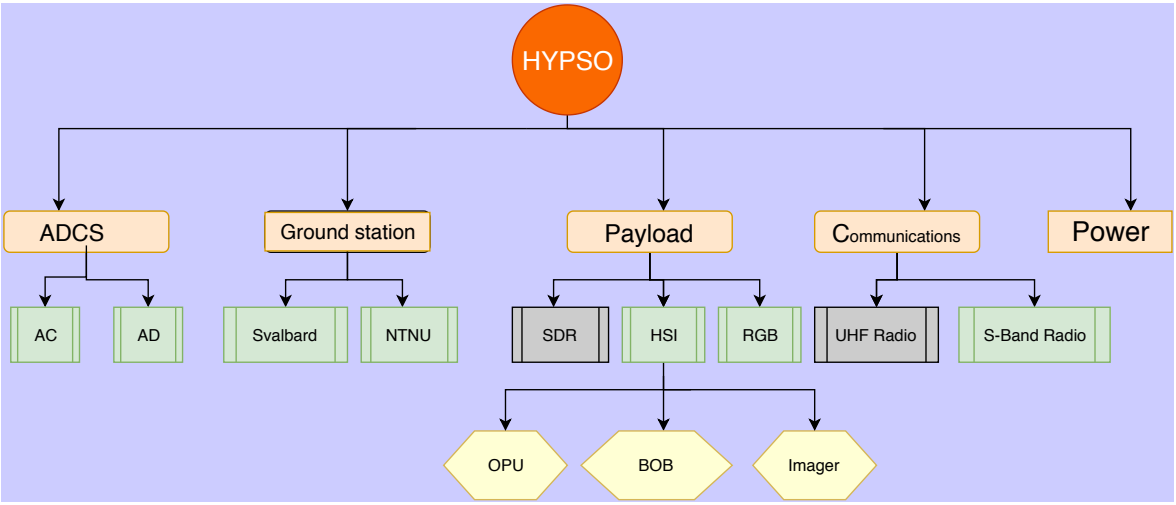


Figure 5.5: Physical hierarchy diagram used in FMECA 1

This division was detailed on important subsystems for the mission success criteria, and a less detailed on less important subsystems. **In retrospect, we could have used a more functionality based division.** This could have been beneficial, due to most of the failure modes being software related. However, the physical hierarchy worked well, when the ground rules had been determined in terms of how to organize the failure modes in worksheet. All the failure modes related to one component were gathered in the same tab. Doing it this way turned out to be more work, but the analysis document was more systematic, which means more user friendly.

When we defined the Risk priority number(RPN) scale we also used mission success criteria as base. To ensure that the scale was not to wide, we used a 1-5 scale, instead of a typical 1-10 scale. Most of the severity and occurrence numbers came from individual opinions provided by members of the HYPSO-team. 1 to 5 is wide enough to separate the failure modes without losing precision. Having a wider scale wouldn't benefit the RPN when they are not empiric. Total failure and full success was the natural endpoints in consequence scale, dividing each step with reduction in mission success.

If a hardware failure occurs on a satellite after launch, there is physically nothing

you can do to repair it. Some exceptions do exist, where hardware failures can be fixed with a software reset. However, this is uncommon. Because of the limitations in fixing hardware failures, the **detectability parameter** in the RPN formula loses some of its purpose. We considered the parameter to give a false sense of security. Critical failure modes with a high rate of detectability, which would have a low detectability number, could contribute to critical failure modes to get a lower RPN than other failure modes with a low rate of detectability. Because of this, we chose to **exclude the detectability parameter completely**, as we felt this better visualized the actual risk in the satellite system.

We also discussed using **quantitative parameters** on the probability scale(percentages). The issue stating quantitative reasoning with numbers, is that it may lead to wrong interpretations. It could seem that we had done actual tests, or had numbers with backing from other tests, which we didn't have in most cases. Occurrence and severity scale used in FMECA 1 can be found in table 5.4 and 5.2

Severity Number	**Severty Class**	**Severity Description**
1	Negligible	Operating conditions are such that personnel error, environment, design deficiencies, subsystem or component failure or procedural deficiencies will result in no effect on the systems function
2	Marginal	Failure may commonly cause minor effect on the systems function.
3	Considerable	Failure may in some cases cause functions to stop system from fulfilling mission success requirements
4	Critical	Failure causes serious absence of required functions. Most mission success requirements will not be met.
5	Catastrophic	System ceases to function, no mission success requirements can be met

Table 5.2: *Severity scale used in FMECA 1*

Occurrence Number	**Occurrence Class**	**Occurrence Description**
1	Improbable	So unlikely that occurrence is negligible
2	Remote	Occurrence possible but unlikely
3	Occasional	Likely to occur at some point in lifetime
4	Probable	Will occur several times in lifetime
5	Frequent	Likely to occur often

Table 5.4: *Probability scale used in FMECA 1 and 2*

Planning the workshop for the function FMECA took time. We tried several test runs, and what we decided on can be found in chapter 5.4, as this is part of the answer to project goal 4.

The **first workshop** had nine participants, which was a preferable size. Enough to get discussion, but not enough to lose control. All the fields of study were represented, except communication. This was not ideal. We started by introducing the concepts of FMECA, and followed up with defining the scope based on mission success criteria.

We did a brainstorming session, linking functions to subsystems, and failure modes according to the functions. The failure modes and functions were put directly into the premade worksheet, divided by hardware hierarchy. This was very efficient, and the workshop team started to work independently after a few examples. The participants sat down in pairs, and took one subsystem each(excluding communications). This led to the volume of failure modes being found to be relatively large. Some corrections had to be done, to ensure that the information in the

worksheet followed the same structure. The workshop lasted for three hours, and the worksheet was still missing effects, RPN and counter measures.

Most of the failure modes linked to the mission success criteria we set were software based. To ensure we got the best information possible, we planned our next workshop to be the second part of a software code review meeting. These meetings were weekly, and had 5-10 participants. We used two software meetings to finish the FMECA. The first meeting we did one subsystem, the HyperSpectral Imager(HSI), in collaboration, and gave each participant a subsystem to finish by the next meeting. This worked well, and the results of the FMECA were discussed and reviewed in the next meeting. The primary focus was peer-reviewing the RPN, which is an important output of the analysis. Some adjustments were made. The FMECA was done from our part, and we recommended the participants to use this worksheet as a risk documentation, and actively use it later in the project, as the worksheet is continuously available on the HYPSO drive.

One of the subsystems, the Software Defined Radio(SDR), didn't fit into our scope of analysis, which made us cut the subsystem from the analysis. This is due to the Software defined radio being used for a secondary mission(not HSI-mission), and not being related to the mission success criteria at all. The only way the SDR could affect the satellites ability to take picture is if it hogs all the power, which is a highly unlikely scenario, almost negligible. This was one of the failure modes in the power subsystem.

The finished FMECA is indicating what subsystems are critical. This will be used when mission requirements are redefined. Critical failure modes will be considered in the design review. However, this will happen after the bachelor group has ended its involvement in the project.

One of the **Weaknesses** in conducting the FMECA the way we did, was the complexity of having both a hardware structure, and a functional approach. This lead to some extra work discussing which failure modes belong in what subsystem. However the FMECA is user friendly and organized, which is ultimately the most

important. Another weakness in the approach is that a lot of the software failure modes were determined as a homework by one participant of the FMECA. This means that some of the subsystems failure modes and effects are not peer-reviewed. Some failure modes may lack information other participants could offer.

All of the RPN numbers were prioritized for peer-reviewing with the rest of the HYPSO-team, due to the importance of the RPN. This was necessary due to time limitation.

FMECA 2: Mechanical Interfaces and Optics

The **Hardware FMECA** we did was more similar to a regular standardized FMECA, making the planing and conducting more straight forward. This meant that we could rely heavily on the **standards** chosen in project goal 3. We used these standards to create a new worksheet, in which we listed all the components, down to every bolt. Some components we looked at as a whole, for example the 50mm VIS-NIR objectives. The camera head was also looked at as a single component. This was done to limit the workload to a realistic level. The objectives and camera head contain numerous small components, and if one is replaced the whole component has to be redesigned.

The base of the analysis was the self made mechanical interfaces for the camera, as well as the optical components. For this to be a beneficial FMECA, we also included all the premade parts directly interfacing with the self made components.The bolts used on these parts were included as well. The premade parts are made by NanoAvionics, and are designed and tested for space. A component list can be found in the FMECA, see attachment 2.

The RPN scale had to be modified, as the base of the analysis no longer was the mission success criteria. The new parameter for setting the RPN scale was **Whether or not the camera was able to capture a picture with readable data.** This lead to the severity scale from the function FMECA being unusable. The new severity scale was found in consultation with the participants of the Hardware

FMECA, and can be found in table 5.6. The occurrence scale from FMECA 1 was reused, as this still was applicable.(table 5.4)

Severity Number	**Severity Class**	**Severity Description**
1	Negligible	Missing information in image is negligible
2	Marginal	Image missing some data points
3	Considerable	Image missing information
4	Critical	Irregular image. Image not usable
5	Catastrophic	No image

Table 5.6: *Severity scale used in FMECA 2*

Conducting the hardware FMECA was a more standardized approach than the functional. The component list needed a bit of updating, particularly bolts, so the first workshop started with this. After this, we followed an approach similar to the one in chapter 2.5. First associating functions to components, and failure modes thereafter. The participants in the workshop had developed most of the designs we were analyzing, and had some failure modes and causes ready before the workshop started. This, in combination with them being involved in the function FMECA as well, lead to this being an efficient process. The entire FMECA was done over two workshops, lasting approximately three hours each.

One of the **limitations** in this approach is that we had to do the FMECA before the prototype was shock tested. This lead to the RPN assigned shock related failure modes not being as accurate as they could have been.

In addition, lack of interdisciplinary competence and experience perhaps had a negative impact, increasing the possibility of inadequate results.

The objectives and the camera head was looked at as one single component. This means some potential failures on a more detailed level are non present in the analysis. However, limiting the detail level on the selected components was considered beneficial, due to the complexity of the components, and the lack of knowledge surrounding these.

One of the **Strengths** that stands out is that the FMECA team purely consisting of engineering students who made a large portion of the components analyzed. This leads to their knowledge of the components function and flaws being sublime. The objectives were also radiation and vacuum tested, so reliable Risk priority numbers were provided.

5.6 Project goal 6: Choose 5 Critical Failure Modes on the HYPSO Satellite and Discuss Possible Mitigation of Risk

5.6.1 Findings

RPN	**Failure mode nr.**	**FMECA**	**Failure mode**
15	ME35	Hardware	50mm VIS-NIR objectives does not collect enough light because breaks due to shock
15	ME36	Hardware	50mm VIS-NIR front objective does not collect enough light because it darkens due to radiation
10	ME37	Hardware	50mm VIS-NIR front objectives does not collect enough light due to substance condensation
9	A5	Function	OPU fails due to software crash
16	L4	Function	The ground station receives noisy signal due to the antenna not pointing correctly or interference

Table 5.8: *Failure modes chosen for highlighting risk and FMECAs versatility*

5.6.2 Discussion

When choosing the failure modes to discuss in this project goal, we opted to go for a combination of the most critical failure modes, and failure modes that are fairly typical for both hardware and function based FMECAs. This was done highlight

the FMECA tools versatility. FMECA is useful for both hardware and software, as long as it is structured and prepared in the right way.

As shown in table 5.8, the 50mm VIS-NIR objectives are critical components, having the failure modes with the highest Risk priority number in the hardware FMECA.(2.1). The software crash is a failure mode on the critical limit, but is fairly representative for several failure modes in the function FMECA, in terms of effect and counter measure, and was therefor included in this chapter.

50mm VIS-NIR Objectives does not Collect Enough Light because it Breaks due to Shock

There are three 50mm VIS-NIR objectives in the Hyper Spectral Imager, HSI. The objectives focuses the light in a certain way into a grating, which fractions the light. This creates the hyper spectral image(see figure 1.1. for visualization)

The shock referred to in this failure modes is the environment the objectives are subject to during launch. The launch is a critical phase for all space objects, and the HYPSO-1 satellite is no exception. The satellite is going to be sent up on a carriage, a rocket that launches multiple space objects at once. This means that in addition to the standard launch shock, there is also a risk of hitting other satellites being launched on the same rocket. This can be fairly critical, and if the outer objective breaks as a result of one of these factors, the satellite could not reach mission success at any level, due to imaging being impossible(4.4).

A countermeasure for this would could be testing the objectives for the expected launch conditions, and include a safety factor accordingly. Another, and perhaps better solution would be to introduce a dampener system on the entire platform the objectives lay on. The dampener system would absorb most of the blow, leaving the objectives undamaged. This is a countermeasure that the mechanical team is considering implementing at this time. Shock testing is also planned in 2019/2020, and will determine if the dampener system is needed.

50mm VIS-NIR Front Objective does not Collect Enough Light Because it Darkens due to Radiation

This failure mode is quite special, because the probability of occurrence is 100%. The outer lens on the objective will darken due to radiation, and degrade over time(2.7.2). This will effect what light passes through the objectives. This failure mode increases in severity over time, with a average severity estimated as 3(5.6). This number is determined from the radiation resilience test done by members of the HYPSO team in Denmark.[21] The test results showed how an objective identical to the ones used in the Hyper spectral Imager reacted to the expected radiation. The darkening of the glass will vary with how much radiation it actually will be subject of, with an estimated minimum of 10%[21]. The credibility of the test numbers is not completely reliable, as the radiation envoirement in space is hard to estimate and recreate. The number can be false, but we went with the best estimate we had.

50mm VIS-NIR Front Objectives does Not Collect Enough Light due to Substance Condensation

Another big issue in space is substance condensation as a result of outgassing(chapter 2.7.1) Outgassing refers gas particles trapped inside the macrostructure of the material precipitating and condensing on to other parts of the satellite, in this case the outer lens. This can reduce the qualities of the images.

A solution to this problem is to only use spacecraft approved materials, which can be found in an open NASA database, containing outgassing rates[7].

The HYPSO satellite has some components of outgassing prone materials. This is due to cost and weight. Swapping these materials for more outgassing resistant materials will be considered on one of the next design reviews.

Onboard Processing Unit Fails due to Software Crash

The onboard processing unit controls the payload and processes the data from the Hyper Spectral Imager. A failure mode listed in the function FMECA is that the onboard processing unit fails to reboot due to a software crash. We chose this failure mode, as it was one of the more critical software related failure modes, with a good solution. If the OPU fails to reboot due to a software crash, there could be several different reasons. Firstly, the reason could be untested software that enters a wrong state which causes a crash. This is highly unlikely, as the software will be tested before launch.

Another failure cause could be a "heisenbug". A heisenbug is simply a bug that changes behavior when one starts observing it. This is hard to countermeasure, as it is a general failure, and not a specific failure cause.

The OPU being fed erroneous parameters could also lead to a software crash. However, this would be a fault from another subsystem, and is excluded from the analysis, due to the limitations of FMECA(2.5).

One of the more complex causes that could lead to this failure mode is alpha rays flipping bits. This is called a soft error in computer science, and could change the data from a 0 to 1, or the other way around, causing software crashes[20].

A simple solution to all these causes would be implementing a Watchdog. A watchdog is an electronic timer used to detect and counter malfunctions in software. The watchdog does this through sending a timeout signal, so if the computer enters a malfunctioned state, the watchdog will time out the computer and reset it to a safe mode, or simply reset the software. A watchdog is installed in the satellite bus, but not on the payload. This is a potential fix that might be entered at some point in the HYPSO project.

Watchdogs are used in some unmanned spacecrafts to prevent irreversible failures.

The Ground Station Receives Noisy Signal due to the Antenna Not Pointing Correctly or Interference

Another important step for fulfilling the mission success criteria is getting the images back down to the ground station. This function is crucial for completing downlinking of images. This failure mode had the highest overall RPN in the entire project.

Interference from other signal in the atmosphere or due to radiation from space is likely to happen and makes the pictures hard to read. Unfavorable angle between the pointing direction of the antenna and the satellite will also weaken the signal received. A solution to this failure could simply be using another ground station with better angle to the satellite in that exact moment. This however, takes considerable coordination, and may be unrealistic. Investing in a second antenna or a larger one could also help solve this problem.

To **complete** this goal, we had to rely on workshops and reviews with members of the HYPSO team. The workshop process was efficient, due to test runs that had been performed. Implementing the success factors found in project goal 4 also contributed to the process being efficient.

Something that could **improve** this result is getting the findings **peer-reviewed** by an external resource, to quality ensure, and identify potential overlooks.

Chapter 6

Conclusion

The problem definition of this project is to highlight critical failure modes on the HYPSO satellite through FMECA, and to suggest a standardized customized FMECA approach for the HYPSO satellites.

Project goal 1 and 2: To uncover what needed to be done in order to solve the problem, we conducted a situational analysis of the HYPSO project. This included a technical description of the satellite. The situational analysis reviled a lack of risk management. The risks had only been considered individually by the subgroups during the project. At the time we were included in the project, a function approach is usually too late. However, we found a broad function FMECA, containing every subsystem most beneficial, in terms of creating documentation and quality checking design. We also decided to conduct a more specific hardware FMECA on mechanical components and optical parts. This was due to the primary mission of the satellite being imaging.

Project goal 3: In order for the HYPSO project to utilize this risk management the best way, a standardized approach is proven necessary. We found that which standard being used is less relevant, as long as the approach is standardized within the organization.

Project goal 4: We **developed two tailored approaches** for this project.

The steps are described and modified specific to this project through the situational analysis and experiences from the FMECA. However, they are still general enough to adapt to different subsystem, teams and satellites. With this project we have provided the HYPSO project with a solid base for further risk management, both for this satellite and for coming HYPSO satellites.

Success factors provide a good foundation to implement these tailored approaches. Based on theory and experience from conducting the FMECAs, we have integrated what we consider the most important success factors in our approaches.

Project goal 5: During the two FMECAs, more than 230 (142 FMECA 1 and 92 in FMECA 2) failure modes were found. This created a good overview and highlighted potential elements of risk. Most failure modes were already known and had a low risk priority number(RPN). However, 32 failure modes had a critical high number (9 or more). The result of the FMECA was useful for the HYPSO-team, and will be used to determine new mission requirements.

Project goal 6: One of the findings was that the outer objective in the Hyper Spectral Imager was singled out as a highly critical component. Failure modes included darkening of the lens due to radiation, breaking of the objective due to shock from launch, and outgassing. These could be prevented by shielding, dampener systems and using space grade materials respectively.

We also, for example, found that a software problem in the Onboard Processing Unit could be tackled by a watchdog. The failure modes with the highest risk priority number were in the ground station subsystem. Interference or bad pointing of the antenna could lead to the ground station receiving noisy signals. A possible solution could include investing in a larger antenna, or using a different ground station.

Chapter 7

List of attachments

7.1 FMECA 1 Functional

7.2 FMECA 2 Hardware and optics

7.3 Suggested functional FMECA approach

7.4 Suggested Hardware FMECA approach

7.5 Stakeholder analysis

7.6 Popular science article

Bibliography

[1] Conducting a workshop — main section — community tool box. https://ctb.ku.edu/en/table-of-contents/structure/training-and-technical-assistance/workshops/main. (Accessed on 04/29/2019).

[2] Design fmea, process fmea, concept fmea - fmeca types. http://www.fmea-fmeca.com/types-of-fmea.html. (Accessed on 05/13/2019).

[3] Design fmea, process fmea, concept fmea - fmeca types. http://www.fmea-fmeca.com/types-of-fmea.html. (Accessed on 04/08/2019).

[4] Different methods of risk analysis. https://www.brighthubpm.com/risk-management/110911-methods-of-risk-analysis/. (Accessed on 04/19/2019).

[5] interviews - research-methodology. https://research-methodology.net/research-methods/qualitative-research/interviews/. (Accessed on 04/29/2019).

[6] Nanoavionics 6u satellite bus m6p — nanoavionics. https://n-avionics.com/platforms/6u-cubesat-bus-m6p/. (Accessed on 02/02/2019).

[7] Outgassing data for selecting spacecraft materials system. https://outgassing.nasa.gov/. (Accessed on 05/15/2019).

[8] Payload — definition of payload. htyear={},note={(Accessedon04tps://www.merriam-webster.com/dictionary/payload}, month = ,/02/2019).

[9] Watchdog timer. https://os.mbed.com/cookbook/WatchDog-Timer. (Accessed on 05/15/2019).

[10] What is fmea and how is it different from hazard analysis? – softcomply. https://softcomply.com/what-is-fmea-and-how-is-it-different-from-hazard-analysis/. (Accessed on 04/19/2019).

[11] Why your it project may be riskier than you think. https://hbr.org/2011/09/why-your-it-project-may-be-riskier-than-you-think. (Accessed on 04/19/2019).

[12] How to increase cubesat reliability. Technical report, ESA Academy, 01 2019.

[13] AMOS. About ntnu amos. https://www.ntnu.edu/amos/about-amos. (Accessed on 02/06/2019).

[14] J. Blanquart. Hardware software interaction analysis: Practical case and lessons learnt. Technical report, ESA SP-532, 06 2003.

[15] Carl Carlson. Six essential factors for fmea success. Accendo Reliability, 2018.

[16] Roland J. Duphily. Space vehicle failure modes, effects, and criticality analysis (fmeca) guide. Technical report, US Air Force Space Command, 06 2009.

[17] Mariusz Groette. Personal conversation - skype. 3/25, 2019.

[18] Mariusz Grøtte. Hypso-mrd-001 mission requirements document. unpublished, 2017.

[19] Tord Kaasa Hansen. Mechanical and thermal integration of an hsi payload in a 6u cubesat. unpublished, 2017.

[20] T Heijmen. Radiation-induced soft errors in digital circuits. Technical report, 2002.

[21] Marie Henriksen and Vebjørn Kristvik. Radiation resilience test. Technical report, 2019. Test report.

[22] Per I.Bye. *Vedlikehold og driftssikkerhet*. NTNU, MTP, 1 edition, 2009.

[23] Marvin L. Roush John X. Wang. *What every engineer should know about risk engineering and management*. Marcel Dekker, inc., 2000.

[24] Peter Stray Joergensen Lotte Rienecker. *Den Gode Oppgaven*. Fagbokforlaget Vigmostad Bjoerke AS, 2 edition, 2013.

[25] Mary Ann Lundteigen. Fmeca. NTNU.

[26] Arnljot Hoyland Marvin Rausand. *System Reliability Theory Models, Statistical Methods, and Applications*. John Wiley Sons, 1 edition, 2004.

[27] Arash Mehrparvar. CubeSat Design Specification. Technical report, California Polytechnic State University, 03 2017.

[28] NASA. Cubesat 101. 2017.

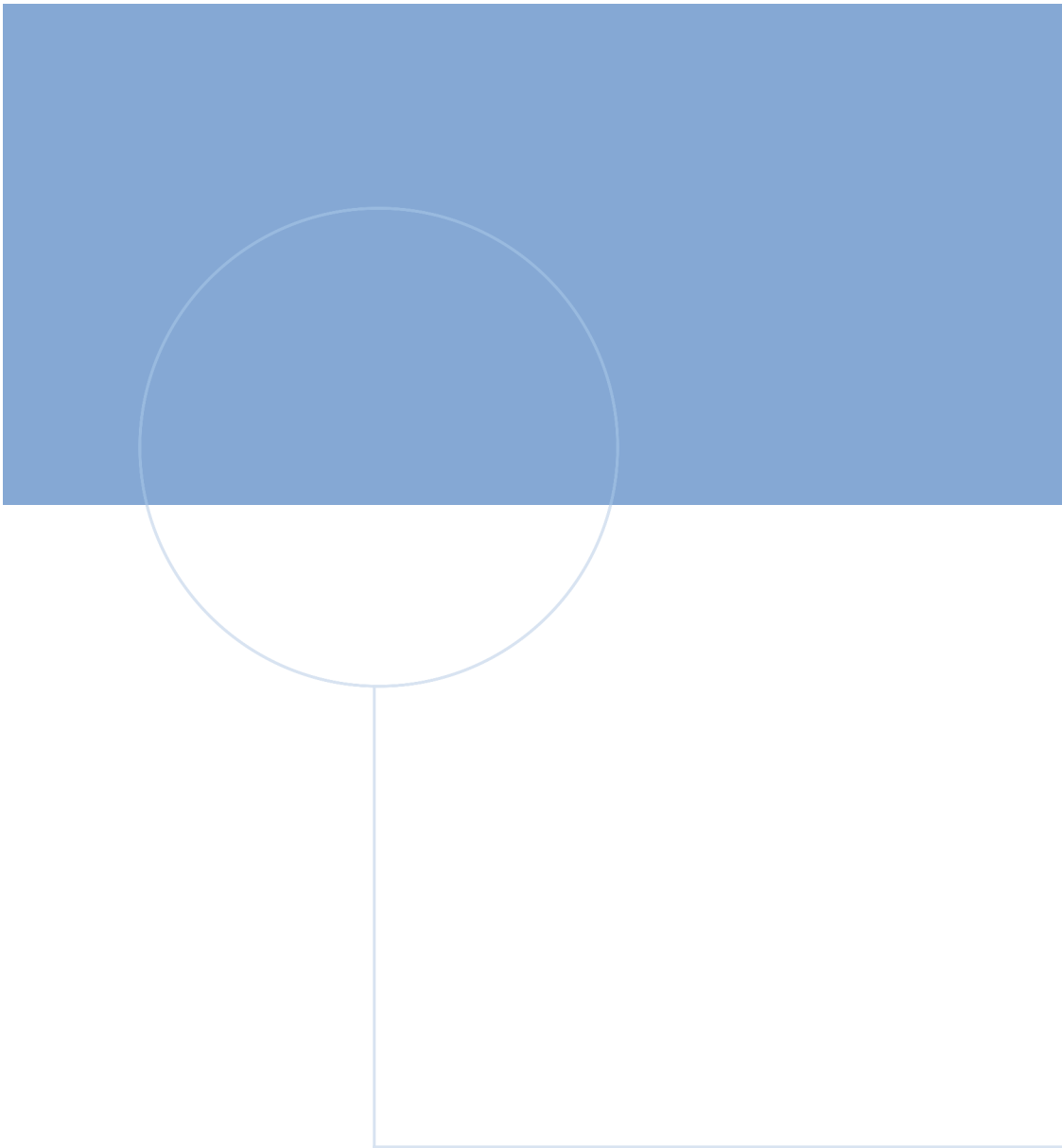
[29] HYPSO project team. Hypso-dr-001-a system design report. 2017.

[30] Marvin Rausand. *Risk Assessment: Theory, Methods, and Applications*. John Wiley Sons, 1 edition, 2013.

[31] Florian Solzbacher. Personal conversation. 1/15, 2019.

[32] Diomidis H. Stamatis. 10 essentials for high performance quality in the 21st century. Technical report, 12 2011.

[33] Roger Walker. Review objectives for esa iod cubesat projects. 2016.



NTNU

Kunnskap for en bedre verden