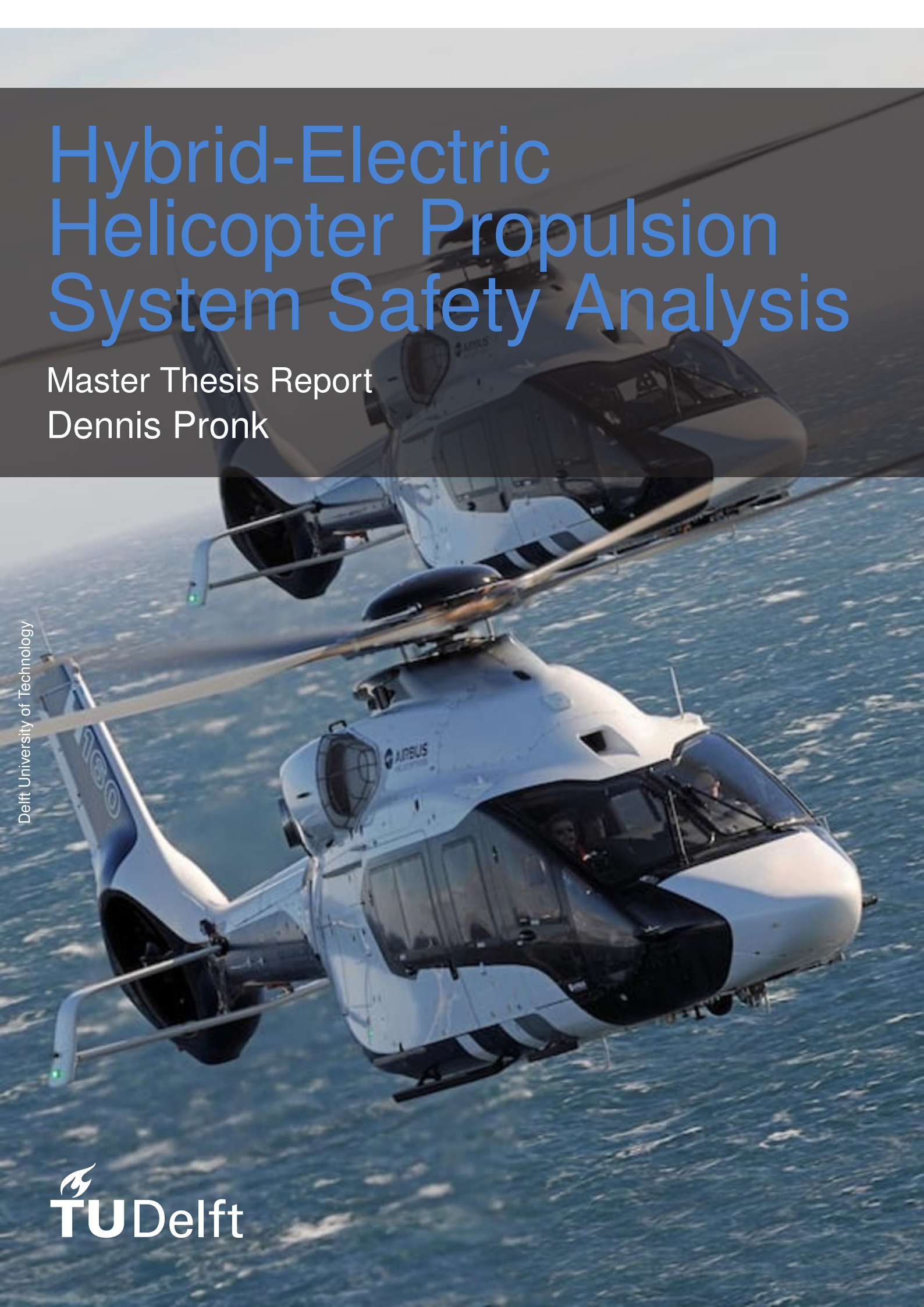
Hybrid-Electric Helicopter Propulsion System Safety Analysis

Master Thesis Report

Dennis Pronk



Delft University of Technology

TU Delft

FACULTY OF AEROSPACE ENGINEERING
FLIGHT PERFORMANCE AND PROPULSION TRACK

MASTER THESIS REPORT

2023/2024

HYBRID-ELECTRIC HELICOPTER PROPULSION SYSTEM SAFETY ANALYSIS

Author:
Dennis Pronk

Student number:
4443861

Preface

This thesis report represents the final step of my journey as a student in Delft. Even though the road taken differed substantially from the one envisioned when I first arrived in Delft, I would not trade it for any other. Even though I already had to leave the faculty of Aerospace Engineering after the first Bachelor year, I was always confident that I would be leaving Delft only after attaining a Master's Degree at the faculty of Aerospace Engineering. I am thankful to my parents for sharing this belief during all my study years.

After spending years learning the ins and outs of Aerospace Engineering I was glad that I could combine my love for aircraft with a growing feeling of responsibility to help the world combat the destructive effects of climate change. Being able to contribute in some way to technical advancements that might help the aviation industry become more sustainable was an amazing opportunity and I hope that there will be more in the future.

I want to thank everyone who helped me grow as an engineer and a person over these past 9 years. I want to thank Professor Fabrizio Oliviero for making sure my tendency to do more practical research did not come at the cost of the academic targets. I also want to thank Zeynep Kocobas and Antoine Rabourdin of Airbus Helicopters for the good care during my time at the company, without you I would not have been able to conduct the research. Specific thanks to my best friend Servaas, for being my brother for all these years and for always offering advice during my hardships during the thesis.

Abstract

As industries are trying to decrease their carbon footprint, new technologies are being implemented. This is also the case for the helicopter industry. Similarly to the automotive industry, the helicopter industry is looking to implement hybrid-electric propulsion. To support this, a lot of research has been conducted into the performance of the different hybrid-electric propulsion systems architectures. However, no effort has been made to map the effects these architectures have on the safety of the helicopter. Since safety is an important aspect of helicopter design, being able to grasp the effect of specific architectural choices early in the development process could provide a major benefit in terms of development time. This knowledge gap led to the research goal addressed with this study: *How is the risk analysis for helicopters affected by hybrid-electric engine architecture?*

The safety assessment conducted during helicopter development is mandated via several industry standards, most notably SAE ARP 4754 and SAE ARP 4761. These standards were followed while performing a safety assessment for a baseline architecture provided by the thesis company. The first step was to identify the exact scope of the hybrid-electric propulsion system, explicitly determining which subsystems are considered part of the hybrid-electric propulsion system. The next step was the identification of the different functions that the system has to perform. By analyzing how these functions can fail several failure conditions could be specified. The failure conditions were then dissected until the failures could be traced to sub-system level failures. The knowledge gained from this analysis was then used to create a baseline to compare other theoretical architectures. The concepts were compared by failure rates for 5 different failure conditions, system weight, engine development requirements and system complexity.

4 main classes of hybrid-electric propulsion system architectures were studied:

- Double-shaft Parallel
- Single-shaft Parallel
- Series-Parallel
- Series

Overall, it was found that choices in hybrid-electric propulsion system architecture significantly impact the safety assessment of helicopters. From the classes mentioned above, double-shaft parallel architecture has the least disadvantages, closely followed by single-shaft parallel. Series-parallel has higher failure rates but still shows a realistic possibility of implementation. Of all the architecture classes, the series architecture shows the worst results in all comparisons, lacking realistic implementation possibilities.

By combining this study with pre-existing performance studies and the recommended study on system weight, a comprehensive overview can be created to aid helicopter architects in the early development stages.

Nomenclature

Abbreviations

Abbreviation	Definition
Al	Aluminium
APU	Auxiliary Power Unit
CAT	Catastrophic
CCA	Common Cause Analysis
CID	Current Interuption Device
CMA	Common Mode Analysis
Cu	Copper
DAL	Development Assurance Level
DD	Dependence Diagram
DU	Drive Unit; electro-motor + motor control unit
EASA	European Union Aviation Safety Agency
EES	Electrical Energy Storage (battery system)
EM	E-Motor
EPS	Electric Propulsion System
EPU	Electric Propulsion Unit
FAA	Federal Aviation Administration
FC	Failure Condition
FDAL	Functional Development Assurance Level
FHA	Functional Hazard Assessment
FMEA	Failure Modes and Effects Analysis
FMES	Failure Modes and Effect Summary
FR	Failure Rate
FTA	Fault Tree Analyses
GEN	Generator
GTE	Gas Turbine Engine
H/C	Helicopter
HAZ	Hazardous
HEPS / EHPS	Hybrid-Electric Propulsion System / Electric-Hybrid Propulsion System
HUMS	Health and Usage Monitoring System
HV	High Voltage
IDAL	Item Development Assurance Level
MA	Markov Analysis
MAJ	Major
MGB	Main Gearbox
MIN	Minor
MTBF	Mean Time Between Failures
NPRD	Non-electronic Product Reliability Database
NSE	No Safety Effect
OEI	One Engine Inoperative
PCM	Phase-Change Materials
PE	Polyethylene
PP	Polypropylene
PRA	Particular Risk Analysis
PSSA	Preliminary System Safety Assessment

Abbreviation	Definition
PTC	Positive Temperature Coefficient
RGB	Reduction Gearbox
SAE ARP	Society of Automotive Engineers Aerospace Recommended Practice
SEI	Solid-Electrolyte Interface
SFHA	System Functional Safety Assessment
SoC	State of Charge
SoH	State of Health
SR	Specific Risk
SSA	System Safety Assessment
UE	Undesired Effect
US	United States
ZSA	Zonal Safety Analysis

Symbols

Symbol	Definition	Unit
F(A $\rightarrow$ B)	Conversion Factor from Environment A to Environment B	-
f(z)	Probability of z	-/ Flight Hour
P(X)	Probability of X	-/ Flight Hour
z	Standardized Normal Variate	-
μ_x	Strength Mean	N/mm^2
μ_y	Stress Mean	N/mm^2
σ_x^2	Strength Variance	-
σ_y^2	Stress Variance	-

Contents

List of Figures

List of Tables

1

Introduction

In this introduction, the outline of the whole thesis will be presented. It discusses the problem definition and the research questions, it also outlines the scope of the research. Finally, it gives an overview of the report structure.

1.1. Hybrid-Electric Propulsion Systems

As the Aerospace industry is looking for ways to decrease its carbon emissions, new technologies are being developed. One of the major problems with aircraft emissions is that they are directly released into the atmosphere. A major effort is pushing for the reduction of fossil fuel usage. This has sparked the development of electrical engines as a replacement for the traditional internal combustion engine. The main advantage of electrical engines in terms of emissions is that it has no direct emissions during flight. Currently, the available technology for electrical engines and batteries is not sufficient in terms of power-to-weight ratio to be viable for usage in aircraft and helicopters. However, an intermediate step is now being developed, Hybrid-Electric Propulsion Systems (HEPS). The general definition of a HEPS is a propulsion system which integrates an electrical engine with a traditional internal combustion engine to reduce the fuel usage of an aircraft or helicopter. There are multiple methods by which this integration can be performed. One method is combining a gas turbine with an electrical engine that draws power from a lithium battery. Another method is to have the electrical engine draw power from a hydrogen fuel cell. The scope of this thesis is limited to only include the combination of a gas turbine engine with an electrical engine, powered by a lithium battery. The reason for this is the reference case at the thesis company contains this type of electrical power generation.

The maturity of this HEPS technology is substantial in the car industry, but in the aerospace industry, it remains largely untested. Currently, HEPS technology is being developed for both aircraft and helicopters with the aim of reducing fossil fuel usage. However, one cannot simply take a HEPS from a car and implement it into a helicopter. A quick look at the operating conditions of a helicopter quickly reveals that a lot of different technical considerations have to be made for safe operations. For example, the vibrations caused by the interaction of different aerodynamic, elastic and structural forces in an electrical engine fitted on a helicopter are very different from the vibrations experienced by an electrical engine in a (hybrid-)electric car.

Conventional helicopter drivetrains consist of one or two gas turbine engines coupled to a main gearbox with driveshafts, where the main gearbox is then connected to the main and tail rotors also via driveshafts. Substantial research has already been conducted regarding the theoretical performance of different HEPS architectures [1] [2]. Every research paper on this subject defines the engine architecture categories differently. This leads to some commonly described configurations which can be broken down on multiple levels. The highest classification level that can distinguish the different architectures is the following:

- Coupled architectures

- Uncoupled architectures

Here coupled architectures refer to HEPS where the "conventional" (gas turbine) engine and the electrical propulsion both power the main rotor and/or tail rotor, delivering a combined total power. An uncoupled architecture is where the two propulsion types are completely separated, e.g. a gas turbine driving only the main rotor and electrical propulsion only driving the tail rotor.

When looking deeper into coupled HEPS architectures multiple different types can be distinguished:

- Parallel (Single-shaft / Double-shaft)
- Series
- Series-parallel

The parallel architecture type has two separate "lines" of power, e.g. a gas turbine feeding into the main gearbox and a separate electrical engine powered by a battery also feeding into the main gearbox, where the power is then combined and delivered to the main and tail rotors. Two sub-types can be identified, the single- and double-shaft sub-types. For the single-shaft sub-type, the gas turbine engine and the electrical engine deliver power to the main gearbox via the same driveshaft, hence the term "single shaft". For the double-shaft sub-type, the gas turbine engine and electrical engine have separate driveshafts to deliver power to the main gearbox.
The series architecture type has a single "line" of power. A gas turbine engine is used to generate mechanical power, this mechanical power is converted into electrical power by a generator. This electrical power is then stored in a battery, this battery then powers an electrical engine. The electrical engine then delivers mechanical power to the main gearbox which transfers the power to the main and tail rotors.
The series-parallel architecture, as the name indicates, is an intermediate of the parallel and series architecture types. Similarly to the parallel architecture type it has two separate "lines of power with a separate gas turbine engine and electrical engine. However, the main gearbox also delivers power to a generator, generating electrical energy which is stored in the battery powering the electrical engine.
All of the researched HEPS architectures in this study have been classified on these two classification levels, with the additional breakdown of parallel architectures into single- and double-shaft types.

1.2. Safety

One of the most important fields in helicopter development is safety. In helicopter safety, there are three levels of protection [3]. The first level is the helicopter certification process, which is aimed at delivering a helicopter with a basic design that will not fail within certain constraints [4] [5]. The pilot certification process is also at the first level and works similarly. It should deliver pilots who should be able to fly safely within certain parameters [6]. The second level is a backup for the first level, in the case where for any reason the first level fails. This second level can be achieved with redundancy within aircraft systems and functionalities. If this is not possible, HUMS (Health and Usage Monitoring Systems) can be used to monitor critical systems and identify operational hazards in time. The last level of protection is aimed at the passengers. Should both the first and second levels fail to enable the helicopter to perform its mission safely, the third level should protect from fatalities for its passengers. An example of third-level safety implementations is crash survival features.

The introduction of new technologies into the aerospace industry thus prompts the need for a new set of regulations specifically aimed at HEPS. Currently, these are yet to be fully developed, due to the technology being new to the aerospace industry. However, progress is being made at the certification organisations. An example of this is the EASA special condition for HEPS [7] which aims to provide certification requirements for these HEPS. Even though the specific safety standards are yet to be completed it is still possible to investigate the safety implications of introducing electrical systems such as high-voltage batteries and electrical engines in helicopters by using the classic EASA CS-27 or EASA CS-29 standards. These standards provide the overall certification requirements for all helicopters. To perform the safety assessment required by these standards two other standards are used, namely SAE ARP 4754B and SAE ARP 4761A, both of which were revised to their current version during the

execution of this study. There are three critically important terms in safety, these are probability, severity and risk. Probability describes the frequency with which an event occurs, this can either be expressed numerically in failures per flight hour or qualitatively with terms such as "probable" and "improbable". Severity describes how dangerous the failure event is to the health of the helicopter and its passengers. Risk combines probability and severity into a single definition, generally classified as "acceptable risk" or "unacceptable risk".

Some research has been conducted into the safety of high-voltage batteries implemented in helicopters. Currently, the battery type which is mainly being implemented is the Lithium-ion battery, as this type is lighter and has a higher performance compared to for example Nickel-Cadmium and Lead-acid batteries [8] [9]. Just like there is no single type of HEPS, there is also a multitude of Lithium-ion batteries both already in use and development, however, this distinction is out of scope for this study due to the detailed expertise required to accurately analyse the differences between them in terms of safety. As of now, these batteries have mainly been used to power a gas-turbine Auxiliary Power Unit (APU) for engine start-up power and emergency backup power [8]. Examples of these implementations are the Boeing 787-8 Dreamliner (APU), the Lockheed Martin F-35 Lightning II (APU/back-up) and the Northrup Grumman B-2 Spirit. While Li-ion batteries have great potential in terms of performance, there is one main factor holding back its widespread implementation: safety. Li-ion battery failure is not uncommon and can lead to serious implications for the aircraft and crew.

A failure in a battery cell can render it nonfunctional, losing the ability to charge or discharge the cell. The worst-case scenario, however, is when a failure in a cell leads to the cell overheating and starting a process called "thermal runaway". Thermal runaway is an irreversible process where the cell temperature increases such that all safety barriers are lost leading to battery overheating, possibly leading to a battery fire. Such a fire can then proceed to damage other systems in the helicopter, especially since this type of fire can be particularly hard to control and extinguish. Additionally, thermal runaway also produces toxic gasses that need to be released to prevent the battery from exploding. Needless to say, this is a situation that needs to have an extremely low probability of occurring. This is not the only way a battery can fail, other possibilities are:

- Internal short-circuit
- External short-circuit
- Undervoltage - overdischarge
- Overcharging

For a full safety assessment, all possible failure modes must be investigated and reviewed. The safety assessment can significantly influence the system design. The development process is never linear and contains iteration loops that might be used multiple times. For example, if during the safety assessment, it is discovered that an additional electrical engine is required, it changes the initial design. This influences the total weight and weight distribution of the helicopter. This then triggers a new performance and stability calculation which then triggers additional changes in the design, thus leading to an additional design loop. There are multiple ways in which a system can be made safer during these iteration loops when it initially does not achieve the safety requirements mandated by SAE ARP 4754B and SAE ARP 4761A. Generally, the simplest solution is to introduce redundancy, for example, when a system contains a temperature monitoring function to be able to respond to overheating a temperature sensor can be installed. However, when analysed, it is found that the sensor is not reliable enough to fulfil the requirements. To achieve the requirement, an identical second temperature sensor can be installed, now two sensors have to fail to lead to undetected overheating. At face value this solves the problem, however, because the two sensors are identical there can be incidents which cause both sensors to fail simultaneously, negating the effect of redundancy. This is called a "common mode", and because of this, for the most critical systems, dissimilarity is required. Dissimilarity is the concept of having two parts fulfilling the same function but using different mechanisms or different technologies. Dissimilarity can even lead to requirements for the parts to originate from different production batches or to requirements for the parts to be sourced from different suppliers. Standard considered common modes:

- Shared low-voltage electric power supply systems

- Shared control/monitoring networks
- Shared fuel distribution systems
- Shared cooling systems
- Shared lubrication systems

The introduction of additional parts or systems into a helicopter also introduces additional weight and can change the location of the centre of gravity. Thus, the implementation of safety measures directly affects the performance and stability of the helicopter. However, no research is currently available on how a choice in HEPS architecture affects the safety analysis of a helicopter. Thus, it will be beneficial to have an overview of the consequences a specific HEPS architecture brings when choosing an architecture in the conceptual design phase. This could then lead to a shorter development process. The research described in this thesis report is aimed at providing such an overview.

Chapter 2 discusses the theoretical background of the research conducted in this study. Chapter 3 provides the theoretical framework for the study. Chapter 4 gives a detailed overview of the methodology that was used to perform the study. Chapter 5 gives an overview of the intermediate and final results of the study. In Chapter 6 the validation of the analysis methods is discussed. Chapter 7 provides the answers to the research questions. It also discusses the limitations of the analyses conducted and thus the results presented in the chapter before it. Finally, Chapter 8 gives a set of conclusions that were drawn from the research results. It also gives recommendations on how this research could be followed up and improved.

2

Background

This chapter is aimed at providing background information on the different HEPS architectures. It also provides background information on battery technology. Additionally, it gives an overview of the different standards that are involved with the safety analysis of helicopters.

2.1. HEPS Architectures

As was already mentioned in the previous chapter, every HEPS architecture option has its advantages and disadvantages. But this multitude of options for the propulsion both the main and tail rotor leads to 34 different HEPS. A basic overview of the different coupled HEPS architectures is given in Figure 2.1, Figure 2.2, Figure 2.3 and Figure 2.4 respectively [2].

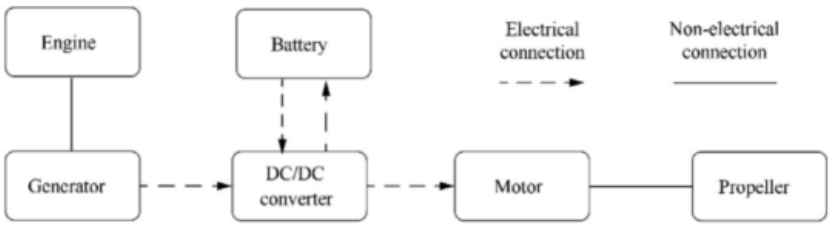


Figure 2.1: Series [2]

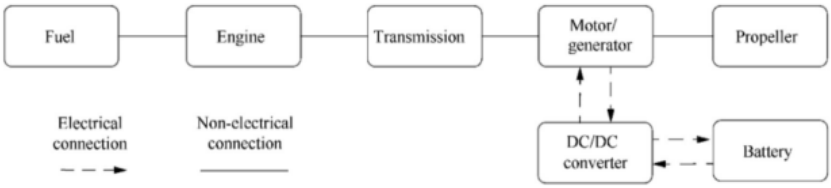


Figure 2.2: Single-shaft parallel [2] [10]

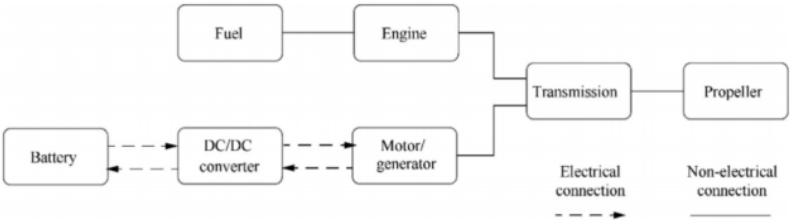


Figure 2.3: Double-shaft parallel [2]

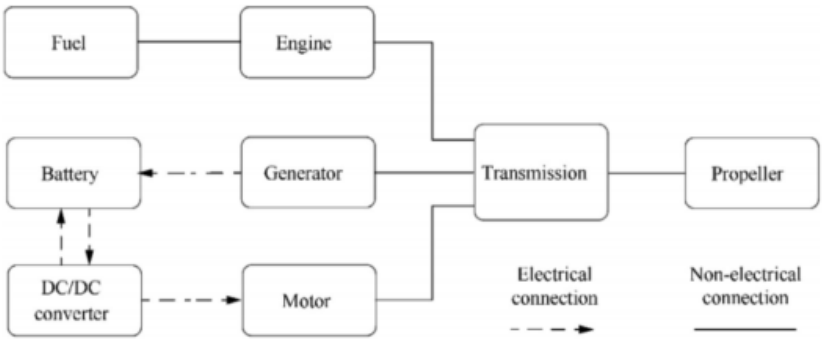


Figure 2.4: Series-parallel [2]

2.1.1. Series configuration

The series configuration as shown in Figure 2.1 has the advantage that the EM (E-Motor) can be driven by just the battery, just the GTE (Gas Turbine Engine) or both at the same time. This is caused by the decoupling of the GTE from the rotor, leading to the possibility of having the GTE run at its optimal operating condition regardless of the power requirement and thus increasing the overall efficiency of the GTE during the mission. The decoupling of the GTE also introduces more flexibility in terms of GTE placement. When the power delivered by the GTE is higher than the power required at that point of the mission the battery can be charged using a generator. And when the power delivered by the GTE is lower than the required power the battery can supply the additional required power.

A disadvantage of this system is that the mechanical energy of the GTE is always converted to electrical energy and then back to mechanical energy in the EM, this leads to a significant decrease in efficiency compared to a GTE that is coupled to the rotor running at the same optimal condition. Another disadvantage is that both the EM and the GTE need to be sized for maximum power output, leading to a high system weight for this configuration.

2.1.2. Parallel configuration

In the parallel configuration, the GTE and EM are both mechanically connected to the rotor [2]. This has some advantages when compared to the series configuration. First off, the mechanical energy is not converted before reaching the rotor, thus preventing conversion losses. A massive advantage is that both the GTE and EM can be smaller for the same performance in a series configuration. Additionally, only the GTE needs to be sized for maximum sustained power performance.

The parallel configuration can be split up per the position of the EM in the power-train architecture. If the GTE and EM are mounted on two separate drive shafts it is called a double-shaft parallel configuration (Figure 2.3). The advantage of this is that the speeds of both engines can be different than that of the propeller and that of each other.

If the GTE is connected to the EM but not directly to the rotor it is called a single-shaft parallel configuration (Figure 2.2). The GTE is linked to the EM by decoupling devices and gears. The EM is directly connected to the rotor, rigidly linking them together. The advantage of this configuration is that it has a lower mechanical complexity, which leads to a lower cost and higher maintainability.

2.1.3. Series-parallel configuration

As the name already indicates, the series-parallel configuration (Figure 2.4) is a combination of parallel and series configurations [2]. It is both the most efficient and most complex configuration. The requirement of complex clutch and gearing systems makes it the most advanced HEPS architecture, which is considered a disadvantage.

2.2. Safety Standards

To develop a new helicopter or to augment an existing design it is required to follow a specific set of certification processes. These certification processes have been standardised by a multitude of organisations, most famously the European Union Aviation Safety Authority (EASA) and the Federal Aviation Administration (FAA). These organisations have created extensive standards for design processes, system functionality and safety processes. For example, a helicopter design process usually follows the EASA CS-27 Amdt. 10 "Certification Specification for Small Rotorcraft" or CS-29 Amdt. 11 "Certification Specification for Large Rotorcraft" standard.

However, there are also standards on system, sub-system and part levels. These standards are not always produced by the FAA or EASA. An organisation which does provide a lot of these technical standards is the Engineering Society for Advancing Mobility Land Sea Air and Space (SAE). This is also the case for helicopters, which fall into the aerospace category, for which the SAE uses the denotation Aerospace Recommended Practice (ARP). One of the standards they have created is a set of guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment. The technical code for this standard is SAE ARP 4761. This standard was released in 1996 and was aimed at providing the industry with a safety assessment consisting of a Functional Hazard Assessment (FHA), Preliminary System Safety Assessment (PSSA), and System Safety Assessment (SSA).

Similarly, in 1996 a standard designated as SAE ARP 4754 was released, this standard was aimed at guiding the process of airworthiness certification for complex electronic systems in civil aviation. In 2010 a revised version of SAE ARP 4754 was released with the designation SAE ARP 4754A. The differences between these two standards have been documented [11]. First looking at the scope, SAE ARP 4754 is applicable for mainly electrical systems involved in performing aircraft functions. However, it was also used for engine systems and related equipment. With the updated version ARP 4754A, the scope has now been increased to any system that implements aircraft functions. Another major difference is that ARP 4754A also includes the service and operational phases next to the development phase.

Even though ARP 4754A and ARP 4761 were originally not designed to deal with HEPS, they are still applicable, and as such will be applied in this study. The analyses performed in this study will follow these standards when the analysis originates from the standards. However, the scope of the analyses will be limited compared to the analyses as described in the standards, as following the full scope of the standards would require too much time. In this study, the following analyses will be conducted per SAE ARP 4761:

- Functional Hazard Assessment
- Preliminary System Safety Assessment
- System Safety Assessment
- Common Cause Analyses

When looking more into the details of the differences between the two versions some parts should be specifically highlighted. The first part that should be highlighted is the guidelines for the planning of the development phase, an overview of this process is given in Figure 2.5.

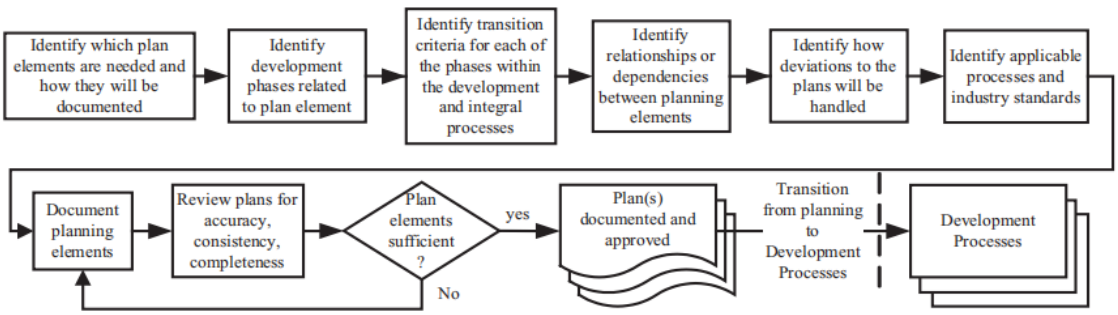


Figure 2.5: ARP 4754A planning process [11]

In ARP 4754A first, a Development Assurance Level or DAL is assigned for aircraft and systems. A DAL identifies which development objectives have to be satisfied for the functions and systems. The higher the DAL, the more extensive these objectives are. Next, it defines both Functional DAL (FDAL) and Item DAL (IDAL), after which the methodology of assigning FDAL and IDAL is given. The system DAL assignments within ARP 4754A are given in Table 2.1. In Figure 2.6 and Figure 2.7 the FDAL and IDAL assignment processes are shown respectively. These are identical in ARP 4754 and ARP 4754A.

Failure Condition Classification	System development Assurance level
Catastrophic	A
Hazardous/Severe Major	B
Major	C
Minor	D
No safety effect	E

Table 2.1: ARP 4754A system DAL assignment [11]

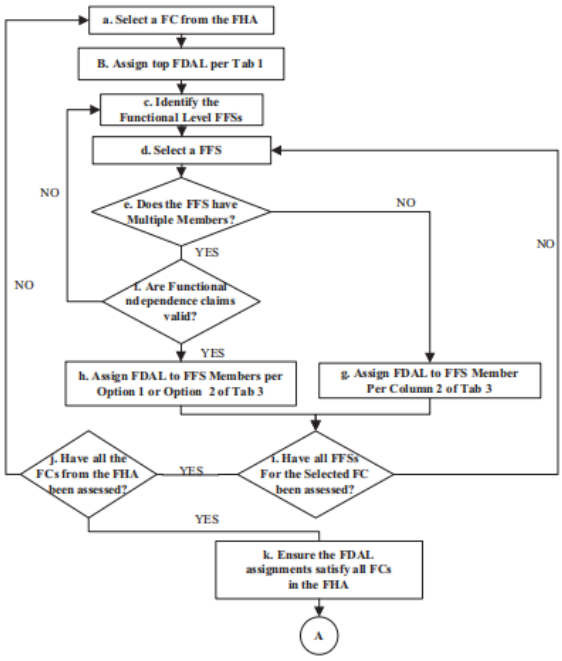


Figure 2.6: ARP 4754A system FDAL assignment [11]

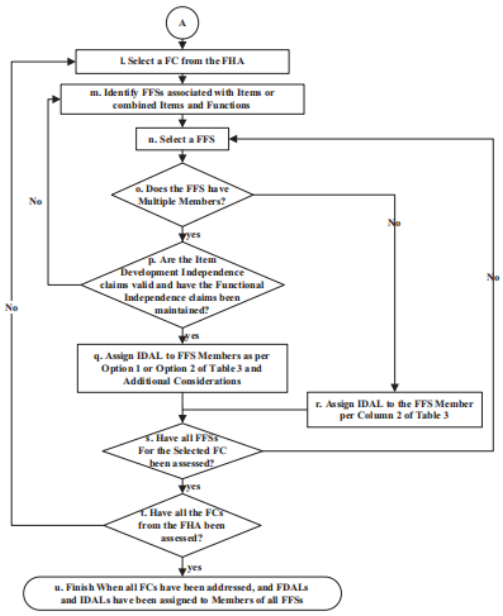


Figure 2.7: ARP 4754A system IDAL assignment [11]

To explain the process visualized in Figure 2.6, an example will be given. Step a: let us assume that there is a Failure Condition (FC) called "FC1: loss of mechanical power" in the Functional Hazard Assessment (FHA). Step b: This Failure Condition is classified as "Catastrophic" since it leads to a crash landing. In the standard, a Catastrophic event has FDAL A. Step c/d: a failure tree is created, shown in Figure 2.8. Step e: there are two basic events leading to the failure conditions, their independence needs to be verified. Step f: FDALs are assigned to the basic events, there are two options, both indicated in Figure 2.8. Step g: a Failure Condition may have multiple Functional Failure Scenarios (FFS), where the conditions differ, for example, in one scenario the failure occurs during testing above a test area whereas in the other scenario, the failure occurs during a commercial flight over a city. This might lead to different failure trees and thus a different evaluation. Step i/j/h: when all Functional Failure Scenarios for all Functional Failures are evaluated the final step is to validate them by comparing them to the FDAL assignments for the Failure Conditions in the Functional Hazard Assessment.

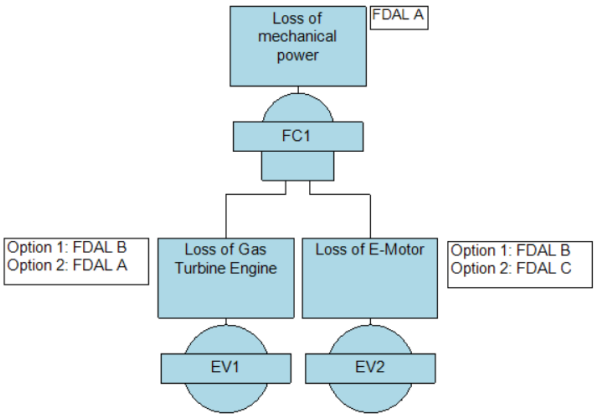


Figure 2.8: FDAL Assignment Example

2.2.1. SAE ARP 4761

In this subsection, a more detailed view of the SAE ARP 4761 standard will be presented. ARP 4761 first gives an overview of what the safety assessment process for aircraft should entail. This overview is shown in Figure 2.9. Analysing the figure from top to bottom, the first item shows the different phases of a typical development cycle. The first phase is the concept development phase, in this phase the aircraft functions. architectures and requirements are decided. The second phase is the preliminary design phase. In this phase, the aircraft functions, architectures and requirements will be divided into system functions, architectures and requirements. The third phase is the detailed design phase. In this phase, the systems will be designed in detail, already choosing the specific parts which will combine into a system. The final phase is the design validation & verification phase. In this phase tests and analyses will be conducted to ensure that the final design adheres to all the requirements set at the start of the development cycle. It works itself back up, validation first starts at the lowest level, the part level, where the requirements and functions for the specific parts will be verified and validated. If the parts adhere to the requirements the next step is to look at the system level. When all the parts are combined into the specific systems, do they still fulfil all the requirements set for the systems? If so, the analysis goes to the highest level, the aircraft level. The systems are combined and then the whole aircraft has to be able to fulfil the requirements set at the aircraft level during the concept development phase.

The second part of the figure shows all the different analyses done during each phase. At the aircraft level, Functional Hazard Analysis (FHA) and Fault Tree Analysis (FTA) are conducted. Similarly to the aircraft level, at the system level, an FHA will also be conducted. The goal of an FHA is to determine the functions, hazards, effects and classifications for either the aircraft or the aircraft systems. At the system level, the process is divided into two parts, the first part is the Preliminary System Safety Analysis or PSSA, during this part an FTA is conducted without knowing the specific parts involved. The second part is the System Safety Analysis or SSA, at this point, the specific parts are known and thus a definitive FTA can be conducted. Next to a definitive FTA, there is also a Failure Modes and Effects Analysis (FMEA). The FMEA is a bottom-up method to identify the failure modes of all items, systems and functions and to determine their effects on the higher levels. Next, single failure modes can be combined into a Failure Modes and Effect Summary (FMES) if they lead to the same failure condition. The SSA is usually based on the PSSA FTA and uses the FMES.

The last part of the figure shows the Common Cause Analysis (CCA). The CCA is an analysis aimed at supporting detailed system architecture. It evaluates the sensitivity of the overall architecture to common cause events. The CCA consists of three different analyses: particular risk analysis, common mode analysis and zonal safety analysis. The results of the CCA are fed back into the systems PSSA and SSA.

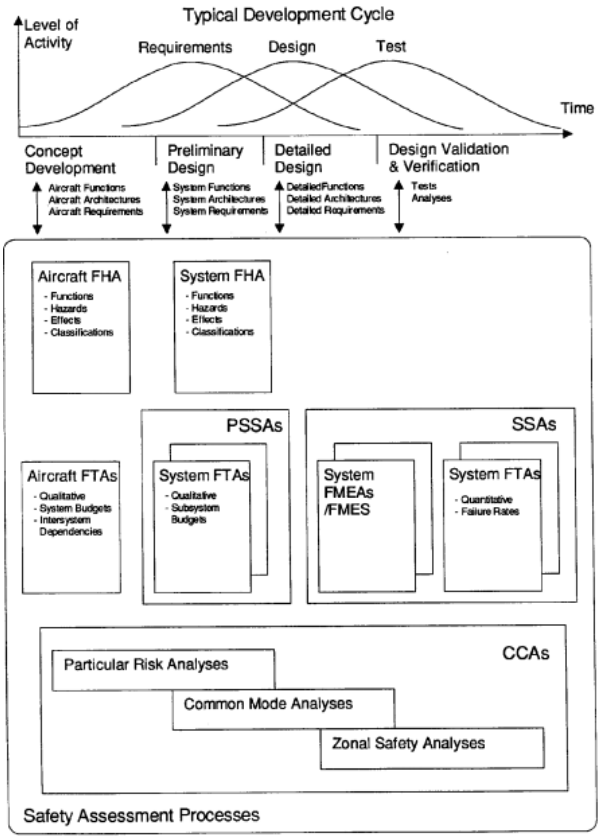


Figure 2.9: ARP 4761 safety assessment process overview [12]

During the FHA, the different system functions are identified. The goal is to identify all the failure conditions of the helicopter or system. To be able to conduct an FHA, a framework is required. This framework is given in Table 2.2. It sets a standard for the severity of a failure condition based on the probability per flight hour. For each probability, it gives a description that may be used to describe the possibility, a failure condition severity classification, a failure condition effect and a DAL. The failure condition severity in each column gives the maximum allowable severity for the failure probability.

Probability (Quantitative)		Per flight hour 1.0	1.0E-3	1.0E-5	1.0E-7	1.0E-9
Probability (Descriptive)	FAA	Probable		Improbable		Extremely Improbable
	JAA	Frequent	Reasonably Probable	Remote	Extremely Remote	Extremely Improbable
Failure Condition Severity Classification	FAA	Minor		Major	Severe Major	Catastrophic
	JAA	Minor		Major	Hazardous	Catastrophic
Failure Condition Effect	FAA & JAA	- slight reduction in safety margins - slight increase in crew workload - some inconvenience to occupants		- significant reduction in safety margins or functional capabilities - significant increase in crew workload or in conditions impairing crew efficiency - some discomfort to occupants	- large reduction in safety margins or functional capabilities - higher workload or physical distress such that the crew could not be relied upon to perform tasks accurately or completely - adverse effects upon occupants	- all failure conditions which prevent continued safe flight and landing
Development Assurance Level	ARP 4754	Level D		Level C	Level B	Level A

Note: A "No Safety Effect" Development Assurance Level E exists which may span any probability range.

Table 2.2: ARP 4761 failure condition severity[12]

The PSSA completes the failure conditions list as generated in the FHA and the corresponding safety requirements. It includes methodology on the requirements for various identified hazards, both qualitative and quantitative. The factors contributing to failure may be identified with FTA, Dependence Diagram (DD) or Markov Analysis (MA).

The SSA aims to validate the failure condition list generated in the PSSA. Thus, the SSA is an evaluation of the implemented system to check compliance with safety requirements. The following information can be included in the SSA process documentation:

- List of previously agreed upon external event probabilities
- System description
- List of failure conditions (FHA, PSSA)
- Failure condition classification (FHA, PSSA)
- Qualitative analyses for failure conditions (FTA, DD, FMES)
- Quantitative analyses for failure conditions (FTA, DD, MA, FMES, etc.)
- Common Cause Analyses
- Safety-related tasks and intervals (FTA, DD, MA, FMES, etc.)
- Development Assurance Levels for hardware and software (PSSA)
- Verification that safety requirements from the PSSA are incorporated into the design and/or testing process
- The results of the non-analytic verification process (i.e., test, demonstration and inspection activities)

The CCA is used to identify specific dependencies or to provide the means to verify function independence. Individual failure modes or external events leading to a major severity or worse failure condition can be identified using the CCA. It is performed during the SSA to validate the independence of systems or items as stated in the PSSA. The CCA consists of three different analyses. These are aimed at identifying individual failure modes or external events that can lead to the most severe failure conditions. Each of the three analyses uses a different approach to evaluate possible common modes.

The first analysis of the CCA is the Particular Risk Analysis (PRA). This analysis identifies events or external influences which can impair failure independence. The aim is to eliminate the threats or to show the risks to be acceptable. Typical risks at a minimum include:

- Fire
- High energy devices
- Leaking fluids
- Hail/ice/snow
- Bird strike
- Tread separation from tire
- Wheel rim release
- Lightning
- High-intensity radiated fields
- Failing shafts

The second analysis of the CCA is the Common Mode Analysis (CMA). This analysis is used to verify the independence of events identified in the FTA in the implementation. Any effects that can eliminate independence should be included. Common mode faults include:

- Hardware error
- Software error
- Production/repair flaw
- Situation-related stress
- Installation error
- Requirements error
- Environmental factors
- Cascading faults
- Common external source faults

In [13] a CMA for an electric power system is provided. Part of the CMA is the CMA checklist, it first gives multiple types of common cause types and then corresponding cause sources. It also then lists the specific failures/errors from a specific source. An example of this can be seen in Table 2.3, where the common cause sources and failures for the design common cause design type are given.

Common cause type	Common cause sources	Common cause failures/errors
Design	The same software	The software common cause failure of LCGU, RGCU, and AGCU
	GCU	The failure of multiple power supply channels caused by a single control unit
	Layout and installation of equipment and wires	The common cause failure of left/right/emergency AC channels
		The common cause failure of left/right DC channels and ETRU power supply channels
	Common connector	The failure of multiple power supply channels caused by that of a single connector
	Common grounding point	The failure of multiple power supply channels caused by that of a single grounding point

Table 2.3: CMA checklist example [13]

The third analysis of the CCA is the Zonal Safety Analysis (ZSA). Each zone of the aircraft should be analysed with a ZSA. It aims at ensuring compliance with safety requirements for the equipment installation. The applicable safety requirements are:

- Basic installation
- Interference between systems
- Maintenance errors

The ZSA first divides the aircraft into zones which are then analysed separately. An example of this is given in Figure 2.10. For every zone, the equipment and components are identified. Then, the potential issues are identified.

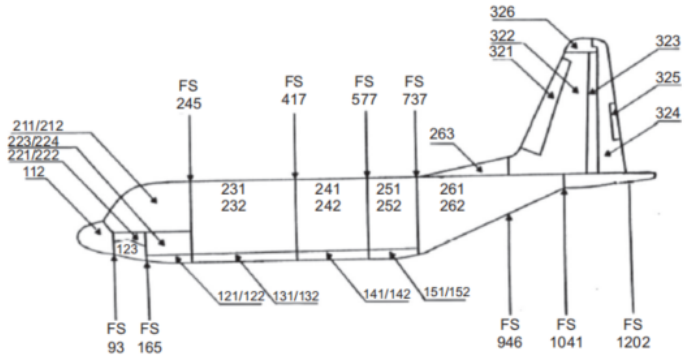


Figure 2.10: ZSA zone division [13]

2.2.2. SAE ARP 4754A

In this subsection, a more detailed view of the SAE ARP 4754A standard will be presented. In Figure 2.11 the interaction between the safety process and the development process is shown. On the top row, it can be seen that each phase has a corresponding section in the standard. In general, the figure shows how the process starts at the aircraft level, and then goes down to the system level. After the system level, it goes to the item level, which leads to software and hardware design. Now, the process goes from the item level back to the system level and aircraft level afterwards. For each level, there is a preliminary safety assessment on the left-hand side which is then verified on the right-hand side of

the figure. While going down, a functionality allocation is further specified. However, while going up, functionalities are integrated again.

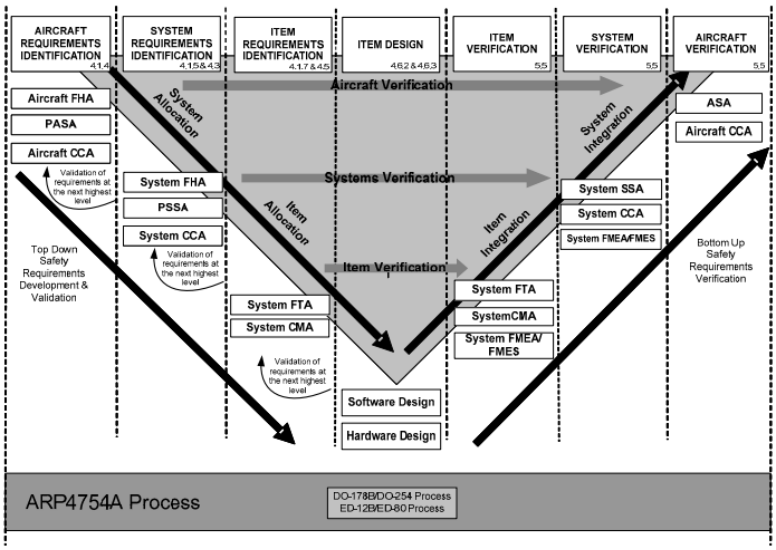


Figure 2.11: ARP 4754A process [14]

In Figure 2.12 it is shown how the different processes with the safety assessment process interact with each other. It also states the respective paragraphs of the standard describing the processes.

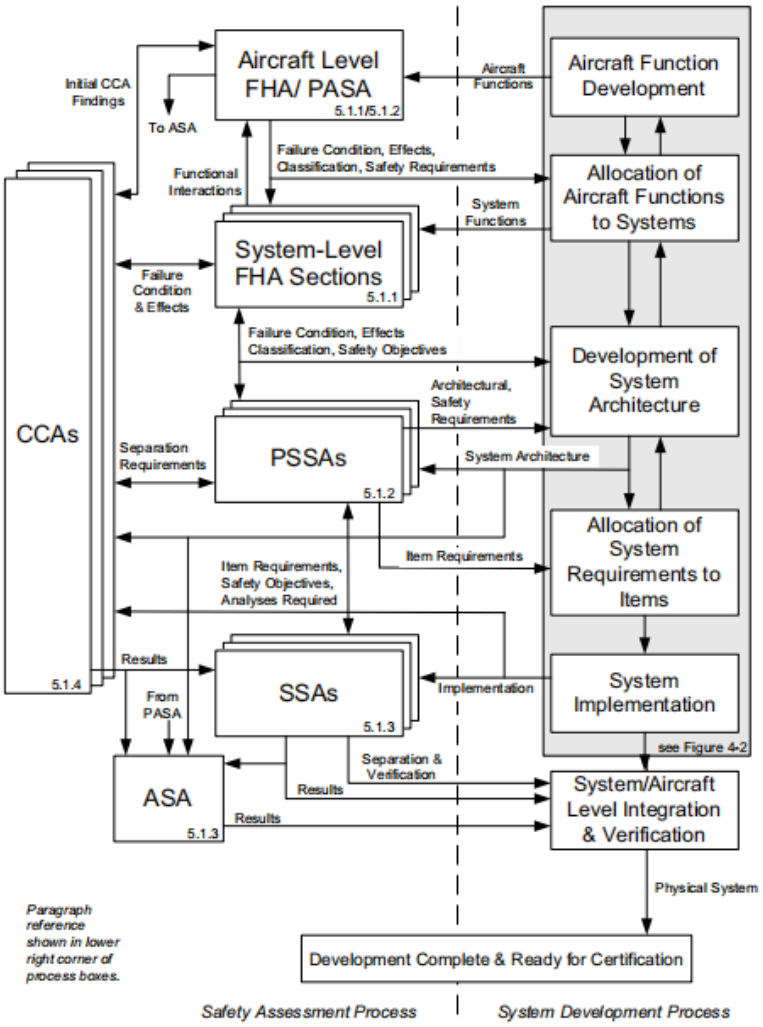


Figure 2.12: ARP 4754A process interaction[14]

To be able to assign FDAL's the aircraft functions need to be defined and assigned to a specific aircraft system. Even though there are no specific recommendations on how to decide on a functional grouping of systems, the grouping of systems can be optimised in each case. The full details of the system implementation are not required to create these groupings, but they may be heavily affected by implementation constraints, failure effects and life-cycle support. After a function has been assigned to a specific system, it will be further linked to specific items. It should be noted that allocating system and item functions is not a linear process but an iterative process. As the requirements and parts specifications become more detailed, other systems and items will be affected. The process is only completed when all the requirements are met in the final architecture. Some typical aircraft functions:

- Aircraft aspects of air traffic control
- Automatic flight control
- Cargo handling
- Collision avoidance
- Communication
- Engine control
- Environmental control
- Flight control
- Ground deceleration
- Ground steering
- Guidance

- Navigation
- Passenger safety

When looking at engine development, a different set of functions arises:

- Aircraft communication
- Engine health monitoring
- Modulate thrust
- Passenger safety
- Thrust reverser control

Similarly, when applying the standard for propeller development, yet another set of functions applies:

- Modulate pitch of the blade
- Modulate speed
- Passenger safety

After the function allocation is finished at the item level and the requirements have been, the verification process starts. This starts by integrating items within the same system and checking whether the requirements are still being met. More and more items are integrated until all the items within a single system have been integrated and verified. The next step is to then start integrating the systems. After each integration step, the requirements have to be verified. The safety assessment process is finished if all the systems have been integrated into the complete aircraft-level functionalities and verified to fulfil the set requirements.

The development assurance levels or DALs indicate the level of tenacity required for mitigating safety risks for a specific function. The greater the severity of a possible error, the higher the DAL. Each DAL is specified in ARP 4754A. The DAL of a function/item depends on the failure condition, as can be seen in Table 2.4. The failure condition represents the severity of the effects caused by a specific error. ARP 4754A provides assignment principles for each failure condition, specifying what DAL should follow from a failure condition and under which circumstances. The failure conditions listed from most severe to least severe:

- Catastrophic
- Hazardous / Severe Major
- Major
- Minor
- No Safety Effect (NSE)

TOP-LEVEL FAILURE CONDITION CLASSIFICATION	DEVELOPMENT ASSURANCE LEVEL		
	FUNCTIONAL FAILURE SETS WITH A SINGLE MEMBER	FUNCTIONAL FAILURE SETS WITH MULTIPLE MEMBERS	
		OPTION 1	OPTION 2
Column 1	Column 2	Column 3	Column 4
Catastrophic	FDAL A	FDAL A for one Member, additional Member(s) contributing to the top-level Failure Condition at the level associated with the most severe individual effects of an error in their development process for all applicable top-level Failure Conditions (but no lower than level C for the additional Members).	FDAL B for two of the Members leading to top-level Failure Condition. The other Member(s) at the level associated with the most severe individual effects of an error in their development process for all applicable top-level Failure Conditions (but no lower than level C for the additional Member(s)).
Hazardous/ Severe Major	FDAL B	FDAL B for one Member, additional Member(s) contributing to the top-level Failure Condition at the level associated with the most severe individual effects of an error in their development process for all applicable top-level Failure Conditions (but no lower than level D for the additional Members).	FDAL C for two of the Members leading to top-level Failure Condition. The other Members at the level associated with the most severe individual effects of an error in their development process for all applicable top-level Failure Conditions (but no lower than level D for the additional Members).
Major	FDAL C	FDAL C for one Member, additional Member(s) contributing to the top-level Failure Condition at the level associated with the most severe individual effects of an error in their development process for all applicable top-level Failure Conditions.	FDAL D for two of the Members leading to top-level Failure Condition. The other Members at the level associated with the most severe individual effects of an error in their development process for all applicable top-level Failure Conditions.
Minor	FDAL D	FDAL D for one Member, additional Member(s) contributing to the top-level Failure Condition at the level associated with the most severe individual effects of an error in their development process for all applicable top-level Failure Conditions.	
No Safety Effect	FDAL E	FDAL E	

Table 2.4: ARP 4754A DAL assignment by failure condition (figure adapted from [14])

Something that is also described in ARP 4754A are the types of requirements that can be encountered during the development process, these are listed below. Most of these requirements are self-explanatory, however the ones which are not will be explained. The interface requirements describe the interconnections between different systems and items, it also contains the complete behaviour of the signals exchanged between the systems. Derived requirements are requirements which arise from previously made design choices. In the next iterative loop, these design choices will be set as requirements. As these requirements are a result of the design process they are called derived requirements.

- Safety requirements
- Functional requirements
- Customer requirements
- Operational requirements
- Performance requirements
- Physical and installation requirements
- Maintainability requirements
- Interface requirements
- Additional certification requirements
- Derived requirements

2.3. Subsystem failures

2.3.1. Battery

Thermal runaway is a major safety concern for battery systems. Figure 2.13 gives an example of a Li battery subjected to increased temperatures.

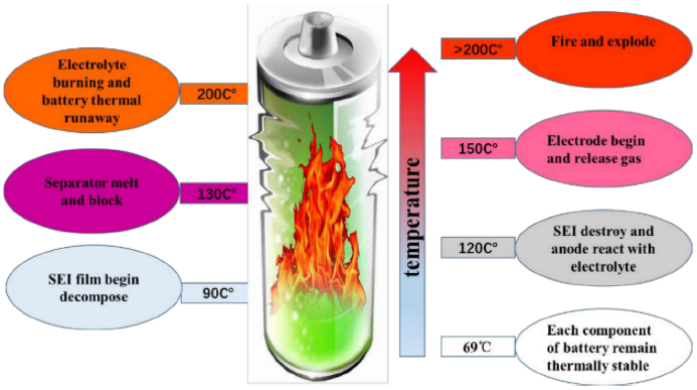


Figure 2.13: Lithium Cobalt Oxide cell subjected to temperature increases [15]

A rising temperature in the battery can cause the Solid-Electrolyte Interface (SEI) film to degenerate. The SEI film prevents the anode from reacting with electrolytes. When thermal runaway is mitigated before the loss of the SEI film, then a loss of functionality can be avoided, however, should the event progress past this stage, then a complete loss of functionality is unavoidable. The main mitigation method for the prevention of SEI loss is to increase the quality standards for batteries. For mitigating the gas production in the cell, a solution would be the use of cell-venting mechanisms. These mechanisms release the gasses produced within a cell into the surroundings in a controlled manner. This way, a full thermal runaway can be prevented. Once thermal runaway occurs, the only mitigation left is to keep the resulting fire contained. This is something that is already implemented for GTE in rotorcraft by using firewalls. A firewall is a set of walls around a specific system which insulates it from the rest of the aircraft. This ensures that a fire is contained within the firewall, resulting in the loss of only a single system. The impact of a fire event on safety completely depends on the architecture of the HEPS system. For example, if the EM is used as a backup within a parallel architecture and there is a failure in the GTE, then a loss of the EM would be critical. If the GTE does not fail, failure of the EM would not lead to a catastrophic event. However, if a series configuration is used where the battery is the main supply of power the impact is different. Then, a failure in the battery will result in an inability to perform the mission and lead to an emergency landing. The effect of the described loss of functionality of the EM is similar in the case of a loss of power.

To be able to mitigate the risk of a cell ending in thermal runaway, it must be understood what causes a cell to fail in the first place. There are both internal and external failures that can lead to the battery overheating and possibly initiating a thermal runaway [16].

External short circuit

An external short circuit is when the output terminals of a Li-ion cell are bridged by a conductor [9]. This is usually classified as a low-resistance failure. When a battery pack is fully charged, a short circuit can lead to a peak short circuit current of more than 25 times the hourly current potential. At the same time, the voltage drops [16]. At worst, this can lead to cell venting or a cell rupture. This, in turn, can start a chain reaction due to the produced heat. Stacks of battery cells are especially vulnerable to this type of failure as vibrations can cause wire connections to break [15]. As helicopters deal with a lot of vibrations, this might be a specifically important risk.

Internal short circuit

Internal short circuit is similar to the external short circuit, except that it occurs within the cell itself. It still leads to an increase in local temperature, if this increase is high enough, it will lead to cell damage. There are four different scenarios which can cause an internal short circuit [9]:

- Between both current collectors
- Between Cu current collector and the positive electrode
- Between Al current collector and negative electrode
- Between both electrodes

In turn, each of these four scenarios can be caused by a variety of reasons:

- Metallic contaminants
- Separator failure
- Dendrite growth
- Mechanical abuse
- Lithium plating
- Improper charging protocols
- Charging outside-rated temperature

Cell overcharge
Typically, a Li-ion cell is considered fully charged at roughly 4.20V. When this limit is exceeded, reactions in the cell are started which can lead to thermal runaway [9]:

- Li-ions are depleted from the positive electrode
- Cell impedance increases, electrolyte decomposes, leading to heat generation
- Exothermic reaction between delithiated positive electrode and electrolyte
- Cell separator degrades, leading to additional heat generation

This failure usually occurs due to a failure in the battery management system, which is supposed to limit the maximum charge and monitor the SoC (State of Charge) [15].

Cell overdischarge
Li-ion cells typically cannot be discharged to 0V and usually rely on a cut-off scheme. This cut-off value is usually between 2.0 and 3.0V. Overdischarging can cause oxidation on the negative electrode, reducing future performance [9] [15]. If overdischarging occurs frequently, dendrite growth may start to occur, which can eventually lead to an internal short circuit.

Low-temperature charging
Li-ion transport through the SEI layer is limited in low temperatures [9]. When charged in this environment it can result in lithium plating at the SEI layer, this can again lead to dendrite growth, which can lead to internal short circuit.

High-temperature storage and charging
High-temperature storage and charging can lead to different failures [9]:

- SEI layer breakdown, in the worst case resulting in thermal runaway
- Electrolyte vaporization, leading to an increased internal pressure
- State of charge, a charged cell can lead to electrolyte oxidation, further increasing the internal temperature

2.3.2. Protection Functions

Several safety measures have been implemented to mitigate the most common battery failure modes, some of which are described in Section 2.3.1. Multiple measures can be taken to improve battery safety. These protection methods can be categorized by the level of implementation, either cell level or system level.

First, multiple protection functions are possible at the cell level. A shutdown separator can be used to stop the transport of ions between the electrodes and shut down micro-pores in the case of overcharging or misuse in high-temperature situations, preventing short circuit currents. Another safety method is called "shutdown additives", these additives shut down the reactions in a cell permanently. A frequently used protection function is the usage of safety vents. In case of overpressure caused by the release

of gasses in the cell, this pressure is released from the cell through the safety vents. Another simple mechanical protection function is a thermal fuse. A thermal fuse simply melts when a current exceeding normal operations passes through it, severing the connection in case of a short circuit. Another method of breaking the circuit is the PTC (Positive Temperature Coefficient) device. The material in the PTC device increases the cell resistance with an increase in temperature, separating the circuit after a certain threshold. By increasing the cell resistance it limits the current in the cell and thus its ability to generate heat. CID (Current Interrupt Device) is often used as a protection function, it also functions by breaking the cell circuit when unfavourable situations arise within the battery cell (overcharge, short-circuit, over-temperature). New protection functions on the cell level like local water-in-salt are being researched but so far it has not led to new major implementations in commercial batteries.

On the second level, the battery system level has some very different protection functions. These are usually aimed at mitigating external impacts, the spreading of thermal runaway and sudden energy discharge. Think of temperature sensors combined with system regulators or battery pack exhaust vents. Insulation between the battery and the rest of the vehicle is also a common strategy, for this aim firewalls and fire retardant compounds can be used. Even though there are already a lot of improvements in terms of battery safety, there are still a lot of improvements to be done and a lot of safety measures are currently under development or the subject of research.

2.3.3. Monitoring Functions

At first sight, it seems like thermal runaway failures occur instantly. However, some parameters already show abnormal behaviour and/or values before a failure occurs. Tracking these abnormalities provides the possibility of preventing catastrophic failure from occurring or spreading. This could be done by providing monitoring functions. These monitoring functions will then provide warnings in case of abnormalities. These warnings could then be separated into three different categories of warnings (Figure 2.14):

- Long-term warnings
- Medium-term warnings
- Short-term warnings

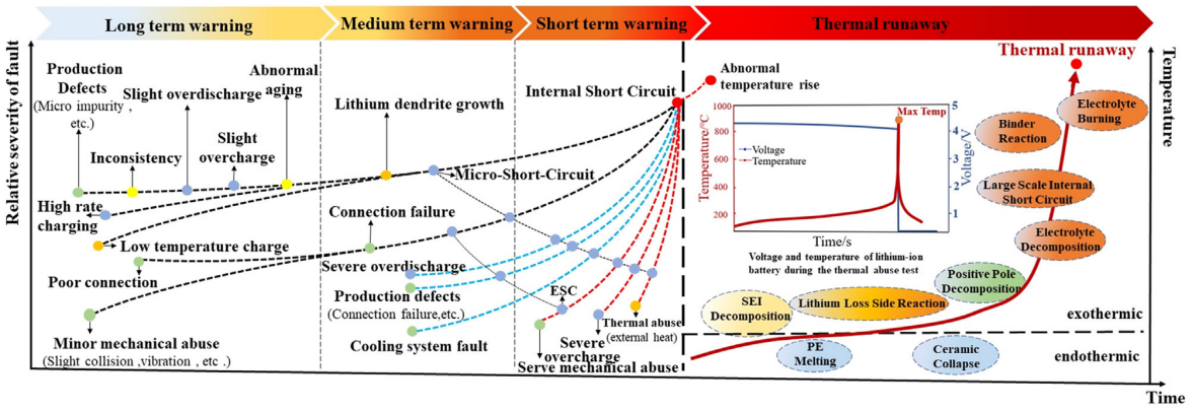


Figure 2.14: Graded warning diagram of thermal runaway of a lithium-ion battery [17]

Minor abnormalities that occur should lead to long-term warnings. Minor abnormalities can lead to major abnormalities. For example, low-temperature charging or high-rate charging can lead to Lithium dendrite growth. There can also be a multi-step process of minor abnormalities leading to a major abnormality. For example, production defects can lead to inconsistencies in battery performance, leading to slight over-discharge and/or slight overcharge, which both then attribute to abnormal ageing, which can cause Lithium dendrite growth. This also goes to show that different processes of minor abnormalities can lead to similar major abnormalities.

Medium-term warnings signify failures which are not immediately impacting battery safety. However, if left untreated they could evolve into failures which acutely impact the safety of the battery. For example, severe overdischarging could eventually lead to an internal short circuit. More examples can be found in Figure 2.14. These failures should be monitored and treated to prevent further damage from occurring.

Short-term warnings give alerts about major failures that immediately damage the vehicle and could lead to casualties within minutes. However, when such a warning is issued there is still sufficient escape time for the occupants. In the case of helicopters, that would mean that the helicopter still has enough time to perform an emergency landing and for the occupants to leave the helicopter safely. This is where the classification of short-term warning will need to be different from the original paper, as the paper is aimed at electric vehicles in general, which usually denotes electric cars.

SoH (State of Health) monitoring can be used to provide a long-term warning as it collects data from the battery to estimate the remaining useful life. However, which parameters are monitored exactly is up to the battery supplier. Mid-term warnings are relayed hours before an actual failure occurs. One of the methods most commonly used is real-time battery temperature modelling to predict when internal battery failure will occur. Phenomena that would lead to a short-term warning include the release of gasses from the battery or a sudden increase in voltage or temperature. In total, there are a lot of different parameters that could be measured with a multitude of methods leading to the different types of warnings. The parameters that are commonly monitored are temperature, voltage and current.

2.3.4. E-Motors

Electrical engines, or E-motors, have multiple failure cases of interest. The first failure case is over-torque, this can be caused by the release of more electrical energy than requested by the flight control system. This can damage the main gearbox by causing torque mismatching. Overspeed is when the electrical engine operates at a higher rotation speed than intended. When the electrical engine surpasses the maximum design rotation speed it can cause a rotor burst. A rotor burst is when the magnetic part of the electrical engine breaks apart, and due to the energy the part has it is then called high-energy debris. This debris can then cause significant damage to neighbouring systems in the helicopter.

Protection Functions

Multiple protection functions can be implemented to limit the effect of electrical motor failures. Damage caused by over-torque can be prevented by including a shear neck in the drive shaft. A share-neck is an intended weak spot in the driveshaft that breaks at a specific torque level. This causes a loss of power from the engine for the rest of the flight but prevents a loss of the main gearbox, which would be catastrophic. Another protection method is the inclusion of a clutch, which can automatically disengage the engine from the main gearbox without causing permanent damage. In the case of high-energy debris, a casing can be installed around the electrical engine to prevent the debris from reaching other systems on the helicopter. Another way to protect against overspeed is to sever the electrical connection between the electrical engine and the battery, leading to a loss of power and thus stopping the generation of mechanical power.

Monitoring Functions

Similarly to the battery monitoring functions, the electrical engine also generally includes multiple monitoring functions. The most commonly monitored variables are:

- Temperature
- Rotation speed
- Torque
- Electrical current
- Voltage

2.3.5. Main Gearbox

The main gearbox has two failure cases, the first case is the inability to deliver power to the main and tail rotor, while still allowing the rotors to turn and thus allowing for auto-rotation. In the second case, there

is a blockage in the main gearbox, preventing the main rotor from turning and causing a catastrophic situation, leading to the loss of the helicopter. There are also aggravating conditions possible for the main gearbox, such as the loss of lubrication, which does not immediately lead to a loss of the gearbox, but does severely impact the wear of the gearbox.

Protection Functions
As mentioned in the section on electrical engines, the inclusion of shear necks and clutches can prevent blockage of the main gearbox. There are no additional protection functions for this in the main gearbox itself. For the loss of lubrication, additional reservoirs are commonly included in the main gearbox lubrication system to extend the availability of lubrication in case of a leakage.

Monitoring Functions
Several variables are monitored in the gearbox to monitor the health of the system. In the lubrication system, magnetic chip detectors filter magnetic chips from the lubrication system to prevent further damage from being caused by the chips. These chips can indicate damage to the gear system and will thus lead to a warning being sent to the avionics system. Another variable that is monitored is fluid levels, to directly monitor the availability of lubrication oil in the main gearbox and thus warn the pilot in case of a leakage.

2.3.6. Gas Turbine Engine

Similarly to the electrical engine, one main failure of the gas turbine engine is overspeed. Another main failure is overheating. Since the combustion process generates a lot of thermal energy the cooling systems must function properly. If the gas turbine engine overheats it could lead to lower engine efficiency and engine fires.

Protection Functions
As with the overspeed protection in the electrical engine, the power source can be cut from the engine. For a gas turbine engine, this translates to closing the fuel valve to stop fuel from entering the gas turbine engine and thus shutting it down. The same action can be taken for overheating to let the engine cool down. In case of an engine fire, a fire suppression system is activated to extinguish the fire.

Monitoring Functions
Commonly monitored variables in a gas turbine engine are:

- Rotation speed
- Torque
- Temperature

3

Research Framework

In this chapter, firstly, the knowledge gap for Hybrid-Electric Propulsion System (HEPS) safety that prompted this research is given. Secondly, it provides the main research question and the subquestions that were used to answer the main research question. Thirdly, the scope of the research is provided. Finally, an overview of the research steps is given.

3.1. Research Motivation

In Chapter 2 a lot of information is provided on the current challenges for Hybrid-Electric Propulsion technology and on the current safety standards involved in the helicopter development process. It also gave a first view into the knowledge gap that this research aimed at solving. Namely, providing an overview of the safety effects that a specific choice of HEPS architecture brings. During the first stage of the development, the conceptual design phase, the propulsion system architecture is decided. However, at that stage, the impact of that choice on the ability to fulfil the safety requirements is still unknown. It is thus not uncommon for a major redesign to be prompted later in the development process due to the inability to fulfil the safety requirements with the initially chosen architecture. This could be prevented if these safety effects can already be estimated during the propulsion system architecture selection in the conceptual design phase. Importantly, this study is not aimed at studying the possible advantages or disadvantages of HEPS compared to a conventional propulsion system. It is aimed at studying the possible advantages and disadvantages of the different HEPS architecture types compared to each other.

From this the main research question that this thesis aims to answer follows:

How is the risk analysis for helicopters affected by hybrid-electric architecture?

To tackle this research question it was broken down into a set of subquestions:

- How is the safety analysis for helicopters performed?
  - What type of risk assessment is done at the aircraft/function/system level?
  - How is it ensured that the failure rate estimates are conservative?
- What are the most critical (sub-)systems with respect to safety for helicopters?
  - What functions should a HEPS perform?
  - How can part/system/function redundancy be achieved in HEPS?
  - What are the most critical common modes?
- What are the most frequent failures in hybrid-electric drive-trains??
  - What are the most frequent failures in helicopter GTEs?

  - What are the most frequent failures in EMs?
  - What are the most frequent failures in battery systems?
- How do the different HEPS architecture types affect the safety analyses?
  - How does the parallel architecture type affect the safety analysis?
  - How does the series-parallel architecture type affect the safety analysis?
  - How does the series architecture type affect the safety analysis?
- How does the number of engines affect the safety analysis?

3.2. Research Boundary

To be able to perform proper research, it is important to set clear boundaries to limit the research scope. The first boundary set relates to the helicopter that would be considered, for the study, only a helicopter with a twin-engine architecture was considered. Specifically, the helicopter has (at least) one GTE and an Electric Propulsion Unit (EPU) consisting of (at least) one electrical motor and one battery. The thesis company provided a reference case with these specifications, thus enabling studying this architecture type in detail. This boundary was also set to limit the amount of possible engine architectures. For example, theoretically, it would be possible to have a helicopter with as many gas turbine engines, electrical motors and batteries, leading to almost endless possibilities. And since conventional helicopters have only one or two gas turbine engines, it makes sense to limit the amount of separate engines considered in this study.

The second boundary is to limit the amount of systems taken into account during the study. During the study only the propulsion system will be taken into account. This includes every system from the energy storage to, but not including, the main and tail rotors. To clarify, this includes the following systems:

- Electrical Energy Storage (EES)
- Drive Unit (E-Motor + Motor Control Unit)
- Main Gearbox (MGB)
- Gas Turbine Engine (fuel system excluded)

The third boundary is the scope of the comparison. The comparison is limited to a predetermined set of failure conditions and a low-fidelity weight estimation that follows from each architecture. The mission used for the baseline architecture will not change for the other concepts. Thus, the specific performance or fuel efficiency of the different concepts is considered out of scope. This includes the additional energy that would be required to fulfil the mission following increased system weight. The reasoning for this boundary with several sub-parts is that there are a lot of possible failure conditions, which might not be critical for the system design, thus it makes sense to only consider a few that have a high impact on the system design. Regarding the weight estimation, a low-fidelity estimation gives an idea of the system weight advantages and disadvantages of each concept. However, for a high-fidelity weight estimation, a whole separate study could be performed due to the amount of detailed knowledge on each of the subsystems that would be required. The omission of increased system weight impact is because an increased weight would lead to increased performance requirements, which in turn would increase the weight again, leading to an iterative design loop, which would distract from the main objective without adding any major benefit to the results.

The fourth boundary concerns the technology present in each of the subsystems. The technology standard provided in the baseline concept will not change in any of the concepts, even though some concepts might require specific adjustments to some subsystems. As the technology is still heavily in development, data on technology developed by different manufacturers is heavily protected and thus generally unavailable. Thus the data used for the baseline architecture will also be used for the theoretical architecture.

3.3. Safety Process Plan

The following steps of the safety analysis were performed during the research:

1. Baseline System Identification
2. HEPS System FHA
3. HEPS PSSA
4. Subsystem PSSA (EES/DU/MGB/GTE)
5. Subsystem SSA (EES/DU/MGB/GTE)
6. HEPS CCA (CMA)

These steps together form the baseline for the comparative analysis. The theoretical background of steps 2 till 6 is provided in Chapter 2. The exact methodology that was followed will be explained in Chapter 4. After creating the baseline the next step was to identify a set of theoretical architectures. For these theoretical architectures, the FTAs were adjusted accordingly to fit the corresponding architecture. Finally, the following aspects were compared for all of the architectures:

- Top-level failure rates
- Subsystem failure rate allocation
- FDAL allocation (GTE / EPS)
- HEPS estimated weight

4

Methodology

This chapter describes in detail the steps conducted to get the final results of the study. The overview of these steps was already given in Chapter 3. The research method is a reference-based study. The first part of the study (4.1-4.6) aimed at performing the safety assessment per the standards mentioned in Chapter 2 for a reference case provided by the thesis company. The second part of the study aims to research the differences in safety assessment for the different Hybrid-Electric Propulsion System architectures.

4.1. Baseline Architecture Identification

Before the safety assessment can be started properly it is important to have a clear view of the rotorcraft or system being evaluated. First, the decision is made on which subsystems are considered part of the HEPS. As each project and company uses different definitions it is important to define this. Subsystems that could be included are:

- Gas Turbine Engine
- Electrical Motor
- Motor Control Unit (Inverter)
- Transmission Systems
- Rotors
- Fuel Systems
- Battery Systems
- Energy Distribution Systems

Secondly, it is important to classify the HEPS using the classifications given in Section 2.1. As each class has its distinctive features, every architecture should be identifiable. This is important as no additional theoretical concepts with the same architecture as the baseline have to be created to compare the different architecture classes.

4.2. HEPS Function Identification

The first step during the safety assessment of a helicopter is normally a rotorcraft-level Functional Hazard Assessment (FHA). However, since the scope of the research is limited to the HEPS this level is skipped and a System FHA (SFHA) is conducted for the HEPS. For the SFHA the first step is to identify the main functions that the system has to perform. For the HEPS these are functions such as providing mechanical power. These main functions can then be further broken down into more specific sub-functions, e.g.:

- F1: Provide mechanical power to MGB
  - F1.1 Provide mechanical power to MGB with only GTE

- F1.2 Provide mechanical power to MGB with only EPS
- F1.3 Provide mechanical power to MGB with both GTE and EPS (GTE 100% power + EPS 100% power)
- F1.3 Provide mechanical power to MGB with both GTE and EPS (GTE 50% power + EPS 100% power)

After completing the function list the corresponding functional failures are identified. A Functional Failure (FF) or failure scenario describes a specific situation with a specific loss of functionality. An example is given in Table 4.1.

Function	***To provide mechanical power to main and tail rotor***	
Reference	F1	F1
Sub-reference	F1.3	F1.3
Functional Failure Reference	FF.005	FF.006
Functional Failure	Full loss of hybrid power, autorotation possible	Full loss of hybrid power, no autorotation possible
Effect on other subsystems and on H/C (worst case)	Emergency landing using autorotation	Loss of H/C
FF severity	CAT	CAT
FC ref	FC.EHPS.003	FC.EHPS.003

Table 4.1: SFHA example

The functional failures are linked to a Failure Condition (FC). These FCs group the different functional failures by failure effect on the rotorcraft. In this example, the full loss of hybrid power. Next, the FCs have to be classified with a corresponding severity, as can be seen in Figure 4.1. The severity indicates the expected damage to the vehicle and its occupants when the FC occurs. Another indication is also attached to the FC, a failure rate. This failure rate is the maximum probability for the FC to occur per flight hour. In Figure 4.2 it is shown what failure rate corresponds to each severity.
Another type of failure included in the SFHA is the Specific Risk (SR). An SR is a failure which occurs due to external factors or other systems while affecting a specific area of the rotorcraft or multiple systems simultaneously. Examples of an SR are bird strikes, fuel leakages and fires.

Failure Condition Severity Classification	FAA	Minor	Major	Severe Major	Catastrophic
	JAA	Minor	Major	Hazardous	Catastrophic
Failure Condition Effect	FAA & JAA	- slight reduction in safety margins - slight increase in crew workload - some inconvenience to occupants	- significant reduction in safety margins or functional capabilities - significant increase in crew workload or in conditions impairing crew efficiency - some discomfort to occupants	- large reduction in safety margins or functional capabilities - higher workload or physical distress such that the crew could not be relied upon to perform tasks accurately or completely - adverse effects upon occupants	- all failure conditions which prevent continued safe flight and landing

Figure 4.1: Coupling FCs to Severity [12]

In conclusion, the output of the HEPS SFHA is an overview of all functional failures, failure scenarios and specific risks. These are all grouped into failure conditions and then coupled with a severity classification and a corresponding failure rate. Additionally, the assumptions that are made in the SFHA are also summarized.

Probability (Quantitative)	Per flight hour					
	1.0	1.0E-3		1.0E-5	1.0E-7	1.0E-9
Probability (Descriptive)	FAA	Probable		Improbable		Extremely Improbable
	JAA	Frequent	Reasonably Probable	Remote	Extremely Remote	Extremely Improbable
Failure Condition Severity Classification	FAA	Minor		Major	Severe Major	Catastrophic
	JAA	Minor		Major	Hazardous	Catastrophic

Figure 4.2: Coupling Severity to Failure Rate [12]

4.3. HEPS Failure Tree Identification

After the identification of the HEPS functions and their classification into Failure Conditions, the Failure Conditions have to be dissected. By dissecting the Failure Conditions the origins of the failure can be traced back to the (sub-)system or item level. This analysis is called the HEPS Preliminary System Safety Assessment (PSSA). The output of the HEPS SFHA is used as an input for this step. The PSSA aims to dissect the failure conditions into sub-system failures. Thus, attributing specific failures to specific sub-systems. This is done by performing a Failure Tree Analysis (FTA). In Figure 4.4 an example of a failure tree is shown. At the top of the failure tree is a failure condition, and at the bottom are the subsystem-level failures. Boolean logic combines the bottom-level failures into the top-level failure condition. All of the failure trees in this study were created using Isograph Fault Tree+ software.

There are three possible types of gates present in failure trees in this study (Figure 4.3):

- OR-gates: the occurrence of any of the lower conditions leads to this failure;
- AND-gates: the simultaneous occurrence of all the lower conditions leads to this failure;
- VOTE-gates: the simultaneous occurrence of at least a specific amount of the lower conditions leads to this failure.

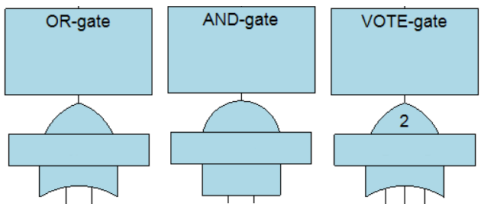


Figure 4.3: Gate Visualization

Figure 4.4 provides an example of a failure tree containing both AND-gates and an OR-gate. The creation of a failure tree starts with the top event, usually a Failure Condition (FC). The next step is to list what causes this top event to occur. For example, the top-level event can be "loss of directional control", this could have multiple causes, such as "loss of tail rotor power" or "loss of tail control system". In the failure tree, this would be visualized as an OR-gate leading to these two lower-level events. By continuing to find the causes of the lowest-level events, the failure tree is expanded until the desired level of detail is achieved. This level of detail could be the failure of a subsystem such as "loss of motor control unit" or the failure of a specific item such as "loss of temperature sensor". A failure tree is in essence no different from a logic tree or a decision tree. In the HEPS PSSA, a top-down approach is used to allocate failure rates to the subsystem failures. Specifically, the top-level failure rate is cascaded equally downwards to the sub-system-level failures.

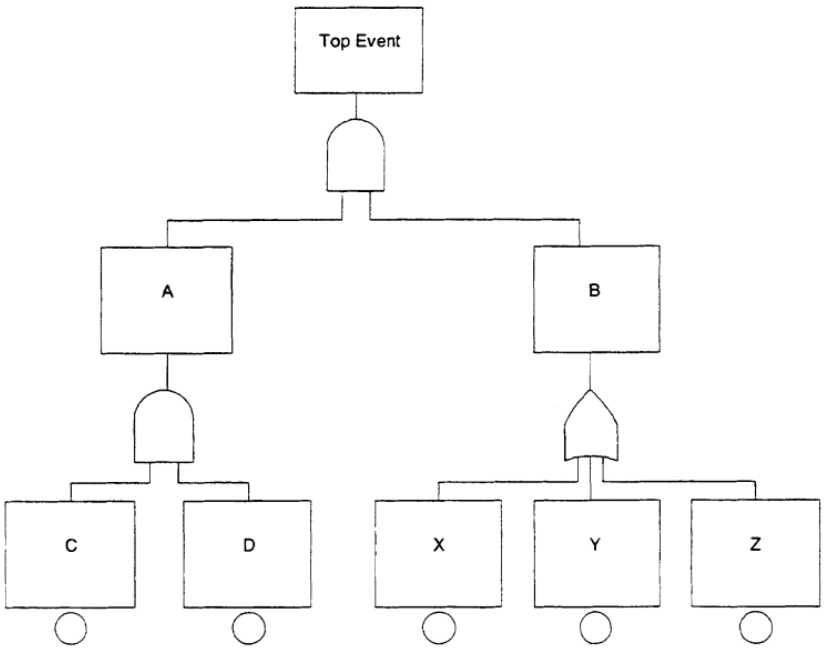


Figure 4.4: Example FTA [12]

For example, take for the top event a failure condition where the complete rotorcraft is lost. The top event is then classified in terms of severity such as Catastrophic, which is usually abbreviated to "CAT". This classification, in turn, would require a probability lower than 1E-9. Now, following boolean logic [18], the maximum allowed probability for intermediate events A and B can be calculated, where the top event is denoted with T:

$$P(T) = P(A) \cdot P(B) = 1E\text{-}9 \tag{4.1}$$

Distributing the allowed failure rate equally leads to:

$$P(A) = P(B) = \sqrt{P(T)} = \sqrt{1E\text{-}9} \approx 3E\text{-}5 \tag{4.2}$$

This has to be repeated to arrive at the failure rates for basic events C and D:

$$P(C) = P(D) = \sqrt{P(A)} = \sqrt{3E\text{-}5} \approx 5E\text{-}3 \tag{4.3}$$

To arrive at the failure rates for basic events X, Y and Z a different calculation must be applied since there is an OR gate:

$$P(B) = P(X) + P(Y) + P(Z) \approx 3E\text{-}5 \tag{4.4}$$

Distributing the failure rate equally between basic events X, Y and Z:

$$P(X) = P(Y) = P(Z) \rightarrow 3P(X) \approx 3E\text{-}5 \rightarrow P(X) \approx 1E\text{-}5 \tag{4.5}$$

In Figure 4.5 the final result is given. The position of a basic event in the tree and the gates that lead to it have a major impact on the top-down allocated failure rate.

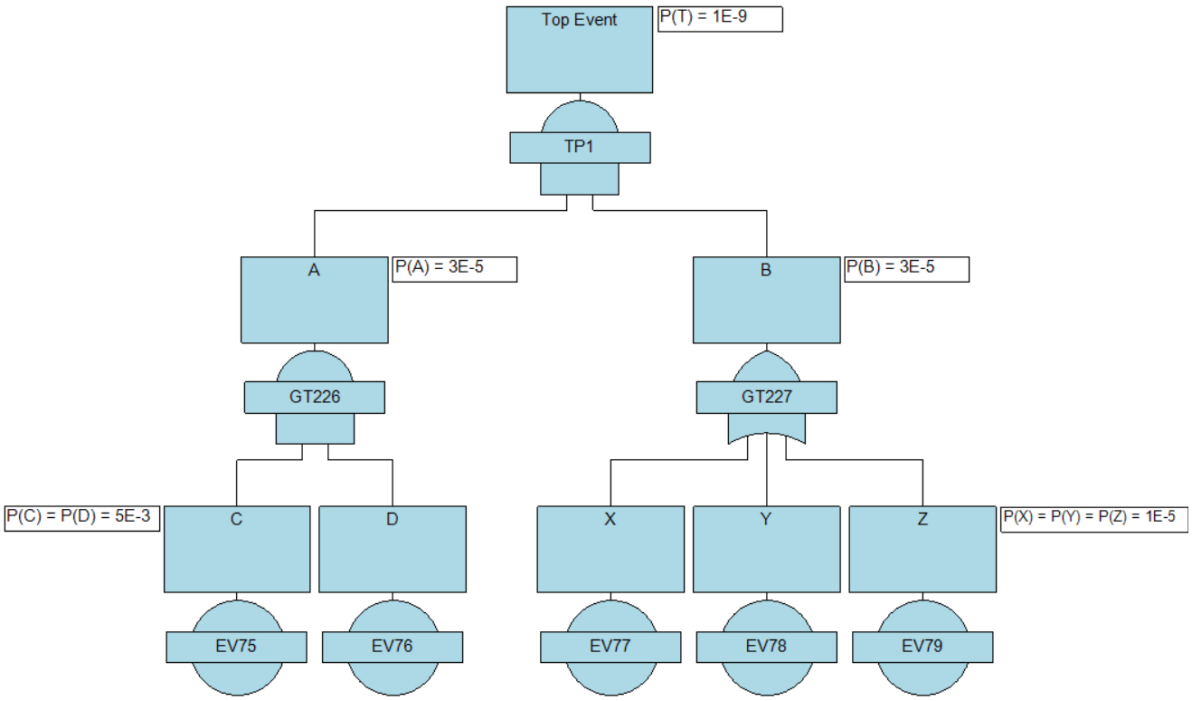


Figure 4.5: Example Failure Tree Result

The output of the HEPS PSSA is a list of subsystem failures with their corresponding allocated failure rates. The same basic event may be present in multiple failure trees, in that case, the lowest allowable failure rate will be taken, selecting the most stringent case.

4.4. Subsystem PSSA (EES/DU/MGB/GTE)

After completing the HEPS PSSA it is time to go down one level to the sub-system level. The subsystem failures are attributed to the different subsystems, using them as failure conditions for the subsystems, as can be seen in Figure 4.6, where basic event C from Figure 4.5 has now become a subsystem-level failure condition. The severity and failure rates that were cascaded down in the HEPS PSSA will be copied to these failure conditions. The same procedure will be repeated, dissecting the subsystem failure conditions into basic events, indicating specific failures in the subsystems. Additional subsystem-level failure conditions may be found, which will then be dissected accordingly into basic events. The output of the subsystem PSSA is a set of failure trees, when combined with the HEPS PSSA, the two levels describe the failure propagation from specific subsystem failures to HEPS-level failures. When a subsystem-level failure condition does not originate from a HEPS-level basic event, it is not attached to a HEPS-level failure tree. It is individually classified with a severity and failure rate on the subsystem level, taking into account how it might influence the level above it.

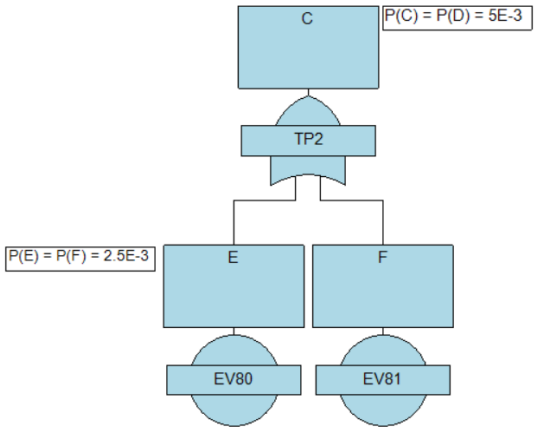


Figure 4.6: Example Subsystem Failure tree

4.5. Subsystem SSA (EES/DU/MGB/GTE)

Now that the structure of the failure propagation is known, an estimation can be made for the failure rates of the subsystem basic events. This is done using empirical data, from similar systems used on different rotorcraft or from systems in an empirical database. The database used in this study is the Non-electronic Product Reliability Database, commonly known as the NPRD. The NPRD contains empirical data on a wide range of equipment implemented in aerial, naval and ground-based environments. Figure 4.7 gives an sample of this. The database has different categories it can be filtered on:

- ID: item-specific identification number
- Description: type of item
- Source reference: dataset reference, amount of recorded failures, total time passed during data acquirement
- Environment: type of environment in which the equipment data was acquired Table 4.2
- Quality: quality specification; military or civilian
- Failure rate: failure rate per million flight hours [-/1E6 hr]

NPRD | Top 1000 parts

ID	Description	Source reference	Environment	Quality	Failure data type	Failure rate
	Overheat Sensor					
NPRD167396	Overheat Sensor		AC	Military	FAILURERATE	0,17414
NPRD167397	Overheat Sensor	800109-000 N=0 HRS=5.347E+05	AC	Military	FAILURERATE	1,870194
NPRD167398	Overheat Sensor	800110-000 N=0 HRS=5.7485E+05	AC	Military	FAILURERATE	1,739578

Figure 4.7: NPRD sample

As can be seen in Table 4.2, the NPRD contains equipment used in a variety of environments. When selecting equipment to represent the subsystems in the SSA, equipment used in the "ARW" environment is selected whenever possible. If this is not possible, it is preferred to select airborne equipment. The last option is to select any equipment present in the database. To make the failure rate selection as conservative as possible, the highest failure rate is selected out of a set of similar equipment. The performance of equipment is tied heavily to the operating environment. Thus, when non-ARW equipment is selected, a correction has to be conducted to the failure rate. This correction is prescribed in a US military handbook [19] and shown in Table 4.3. However, since this table was created for the MTBF (Mean Time Between Failures), which is the inverse of the failure rate, the reference failure rate is to be divided by the conversion factor instead of multiplied. For example, if equipment with the environment "Ground Benign" is selected it is converted to the "Aircraft Rotary Wing" environment as shown in Equation 4.6

$$P(A_{RW}) = \frac{P(G_B)}{F(G_B \rightarrow A_{RW})} = \frac{P(G_B)}{0.1} \tag{4.6}$$

Environment	Symbol	Nominal Environmental Conditions
Ground, Benign	G_B	Non-mobile, temperature and humidity-controlled environments
Space, Flight	S_F	Earth orbital. Approaches Ground Benign conditions. Vehicle neither under powered flight nor in atmospheric reentry.
Ground, Fixed	G_F	Conditions less than ideal include installation in permanent racks with adequate cooling air and possible installation in unheated buildings.
Ground, Mobile	G_M	Conditions are more severe mostly for vibration and shock. Equipment installed on wheeled or tracked vehicles.
Naval, Sheltered	N_S	Sheltered or below-deck conditions on surface ships and submarines.
Naval, Unsheltered	N_U	Unprotected surface ship-borne equipment exposed to weather conditions and salt water.
Airborne, Inhabited, Cargo	A_{IC}	Typical conditions in cargo compartments occupied by aircrew without environmental extremes of pressure, temperature, shock and vibration.
Airborne, Inhabited, Fighter	A_{IF}	Same as AIC but installed on high-performance aircraft such as fighters and interceptors.
Airborne, Uninhabited, Cargo	A_{UC}	Uncontrolled areas with environmental extremes of pressure, temperature and shock.
Airborne, Uninhabited, Fighter	A_{UF}	Same as AUC but installed on high-performance aircraft such as fighters and interceptors.
Airborne, Rotary Winged	A_{RW}	Equipment installed on helicopters, internally and externally.

Table 4.2: NPRD equipment environments as described in MIL-HDBK-217F [20]

From Environment \ To Environment	G_B	G_F	G_M	N_S	N_U	A_{IC}	A_{IF}	A_{UC}	A_{UF}	A_{RW}	S_F
G_B	X	0.5	0.2	0.3	0.1	0.3	0.2	0.1	0.1	0.1	1.2
G_F	1.9	X	0.4	0.6	0.3	0.6	0.4	0.2	0.1	0.2	2.2
G_M	4.6	2.5	X	1.4	0.7	1.4	0.9	0.6	0.3	0.5	5.4
N_S	3.3	1.8	0.7	X	0.5	1.0	0.7	0.4	0.2	0.3	3.8
N_U	7.2	3.9	1.6	2.2	X	2.2	1.4	0.9	0.5	0.7	8.3
A_{IC}	3.3	1.8	0.7	1.0	0.5	X	0.7	0.4	0.2	0.3	3.9
A_{IF}	5.0	2.7	1.1	1.5	0.7	1.5	X	0.6	0.4	0.5	5.8
A_{UC}	8.2	4.4	1.8	2.5	1.2	2.5	1.6	X	0.6	0.8	9.5
A_{UF}	14.1	7.6	3.1	4.4	2.0	4.2	2.8	1.7	X	1.4	16.4
A_{RW}	10.2	5.5	2.2	3.2	1.4	3.1	2.1	1.3	0.7	X	11.9
S_F	0.9	0.5	0.2	0.3	0.1	0.3	0.2	0.1	0.1	0.1	X

Table 4.3: NPRD environment conversion factors in MTBF

There was no failure rate data for mechanical parts such as input drive shafts and gearboxes available at the thesis company. However, an estimation can be made by statistical calculation using normal

distributions (Figure 4.8). For this, an internally available tool was used. Setting the stress variance to a value of 10% and the strength variance of 1% ensures a conservative estimation following industry standards. Generally, during the design of these parts, a safety factor of 1.8 is used, meaning that the mean strength is 1.8 times higher than the mean stress. This leads to a probability of around 1E-15. The calculation is conducted using Equation 4.7 and Equation 4.8. In this study, the mechanical failure rates have been set to 1E-7 or 1E-11 to show that even with those failure rates the requirements can be fulfilled.

$$z = \frac{|\mu_y - \mu_x|}{\sqrt{{\sigma_x}^2 - {\sigma_y}^2}} \tag{4.7}$$

Where:

- μ_y and μ_x = stress and strength means, respectively
- σ_x^2 and σ_y^2 = strength and stress variance, respectively
- z = standardized normal variate

$$f(z) = \frac{1}{2\pi} e^{\frac{-z^2}{2}} \tag{4.8}$$

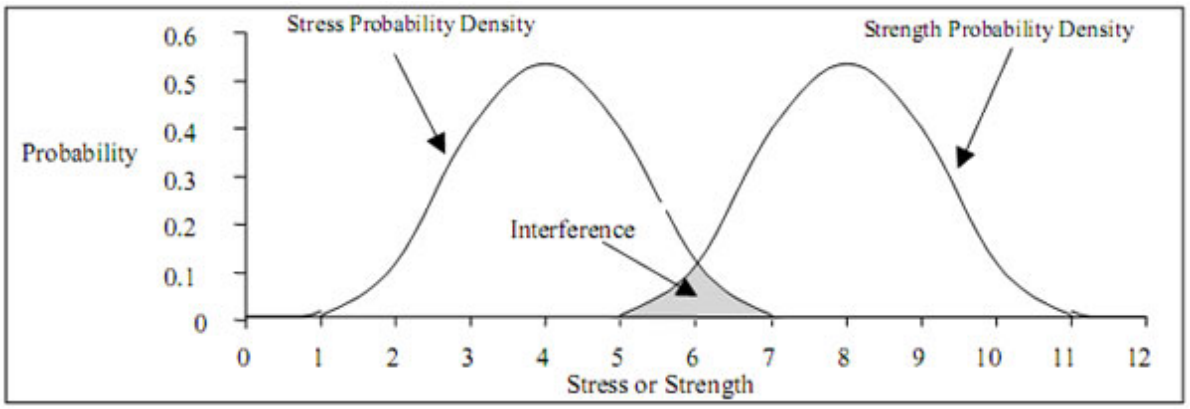


Figure 4.8: Mechanical part failure rate estimation

When each basic event has been attributed with a failure rate, the top-level failure rate can be calculated, which in this study is done automatically by the Isograph Failure Tree+ software. The calculated failure rate is then compared to the target failure rate for the failure conditions set in the subsystem PSSA. If the calculated failure rate is lower, it achieves the target and is thus substantiated. However, if the calculated failure rate exceeds the target, the failure tree has to be adjusted until it achieves the set target. This can be done by introducing redundancy, as explained in Chapter 1.

The output of the subsystem SSA is a set of validated subsystem-level failure trees representing the failure conditions originating from the HEPS PSSA. Every basic event is thus represented by a failure rate, reference equipment, the failure rate target from the PSSA and an FDAL.

4.6. HEPS CCA (CMA)

The Common Cause Analysis (CCA) is a part of the safety analysis that does not have a specific place in the linear progression between the FHA and SSA, as seen in Figure 2.12. As inputs, it uses the results generated in the FHA, PSSA and SSA. Normally the CCA has three parts; the Common Mode Analysis (CMA), the Particular Risk Analysis (PRA) and the Zonal Safety Analysis (ZSA). In this thesis, only the CMA was conducted. For HEPS architecture to impact the ZSA, a detailed placement of the subsystems is required, or the system placement has to vary majorly from its reference location. Since

neither of these requirements was fulfilled, the ZSA was not conducted. For the PRA, the Particular Risks have to be identified, which was done during the HEPS PSSA and subsystem PSSA. However, the identified risks were not majorly influenced by possible changes in the HEPS architecture and a full PRA was left out of scope.

The CMA consists of two activities. The first activity is the creation of a questionnaire (Figure 4.4). Here the "commodities" which might be shared by multiple systems, subsystems or items are identified. For each, it is then determined if there are failures that would negate the independence in the design of the system. Additionally, an example is provided for each of these common failures. The second activity is the questionnaire evaluation. The HEPS system and its subsystems are checked for common failures described in the questionnaires. Any identified common modes that have already been mitigated are documented while unmitigated common modes must be addressed, prompting a (sub-)system redesign.

Common Mode Types	Common Modes Sub-types	Examples of Common Mode Sources	Examples of Common Mode Failures/Errors
CONCEPT AND DESIGN	DESIGN ARCHITECTURE	Common discharge header	Common discharge failure
		Common external sources (ventilation, electrical power, ...)	Failure of common sources (ventilation, electrical power, ...)
		Equipment Protections	Designer failure to predict an event, ...
		Operating Characteristics (normally running, standby, ...)	...
		Others	...

Table 4.4: CMA questionnaire example

4.7. Theoretical Concepts

After the completion of the reference case safety analysis, there is now a baseline to compare other possible HEPS architectures. The first step is to create a set of theoretical concepts. The minimal requirement is that each architecture category described in Section 2.1 is represented in at least one concept. Another important requirement is that all of the concepts are technically feasible, at least theoretically. To ensure this, experts are consulted on the technical feasibility of the concepts. Next, the amount of GTEs, E-motors, and batteries is allowed to vary. Generators, which are not separately present in the reference case can be added. Also, the transmission system may be adjusted to meet the technical feasibility requirement.

4.8. Comparative Analysis

The final part of the thesis research is the comparative analysis. In this part, the baseline created by the reference case is used to perform a safety analysis for the theoretical concepts selected in the previous step. To compare the results, a common framework needs to be present. The first part of this framework is the selection of failure conditions. The baseline and the theoretical concepts should be evaluated for the same failure conditions for a reasonable comparison. The second step is subsystem standardization or building block creation. As all FCs are analysed by an FTA, the failure trees must remain legible. To ensure this, basic building blocks can be created that represent subsystem failures such as "loss of alert data transmission from GTE". These building blocks will remain constant in every FTA, while there may be multiple similar blocks present in a single FTA. Now all concepts can be represented by failure trees in a standardized manner.

For all failure trees, a top-down and a bottom-up approach will be taken for failure rate calculations. The top-down approach is first used to create the failure tree, similar to a PSSA. It also provides a failure rate allowance for all the basic events in the failure tree using boolean logic. The assumption for this boolean logic is that all basic events leading to the same gate have an equal failure rate. As the top-down approach is only aimed at providing an initial estimation, it does not matter that this assumption is not realistic. It is, however, standard practice in the industry to perform the first estimation in this manner. The bottom-up approach is aimed at providing a more realistic failure rate for each basic event. During this approach, all of the basic events are given a more realistic failure rate originating either from test

data provided by the thesis company or from the NPRD database. After filling in the new failure rates, the Isograph Reliability Workbench software calculates the failure rate for the failure condition at the top of the failure tree. If this failure rate is lower than the target, the failure tree and thus the system design are validated. If the failure rate is higher than the target, normally, the system design has to be adapted and the failure rate has to be recalculated, until the failure rate is lower than the failure rate target. In this study, the concept will not be replaced by an adapted version if it does not achieve its target. However, an adapted version of the concept may be added to showcase how such a system redesign would work.

With both approaches, a PSSA and an SSA are represented in the comparative analysis. With the top-down approach, every basic event is coupled with a Functional Development Assurance Level (FDAL). It starts with attributing a severity and failure rate to an FC [12]. Then an FDAL can be allocated to the FC, as shown in Table 4.5. However, an FDAL has specific rules on how it can be cascaded downwards in a failure tree. An FDAL is not directly tied to the probability of failure, but it is a qualitative evaluation, with each level having specific development requirements. Since the FDAL directly correlates to the development rigour of a system, and thus development time and costs, it is generally beneficial if the FDAL can be reduced. Another problem with high FDAL is that off-the-shelf technology is not always able to prove it meets FDAL C or FDAL B due to strict standards. When there is an AND-gate in the failure tree the FDAL can be reduced in different manners [14], in Table 4.6 it is shown how an FDAL can be reduced, visualized in Figure 4.9.

Severity Classification	Minor	Major	Hazardous	Catastrophic
Probability (Quantitative)	1E-03	1E-05	1E-07	1E-09
Development Assurance Level	Level D	Level C	Level B	Level A

Table 4.5: FDAL allocation as described in SAE ARP4761

Functional Failure DAL	**Option 1**	**Option 2**
FDAL A	1x FDAL A, rest FDAL C+	2x FDAL B, rest C+
FDAL B	1x FDAL B, rest FDAL D+	2x FDAL C, rest D+
FDAL C	1x FDAL C	2x FDAL D
FDAL D	1x FDAL D	

Table 4.6: FDAL reduction options [14]

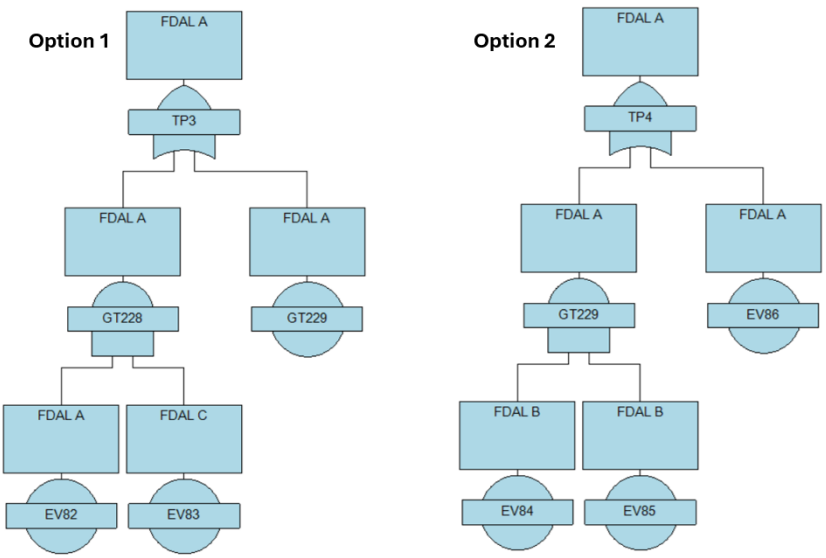


Figure 4.9: FDAL reduction example

Additionally, an analysis is conducted where one of the basic events has an unknown failure rate. This simulates the situation in which all failure rates are known except for one basic event. By taking the target FC failure rate and all of the known failure rates for the other basic events the "left-over" failure rate for the unknown basic event can be calculated. If the "left-over" failure rate is negative it indicates that the system can't achieve the target failure rate for the top-level failure condition with the current system design. This might also be true if the "left-over" failure rate is unrealistically small. If the "left-over" failure rate is a realistic positive number it indicates that the system design might be sufficient, however, no final conclusion can be drawn. An example is given in Figure 4.10. In this example, it is shown how the "left-over" failure rate is calculated.

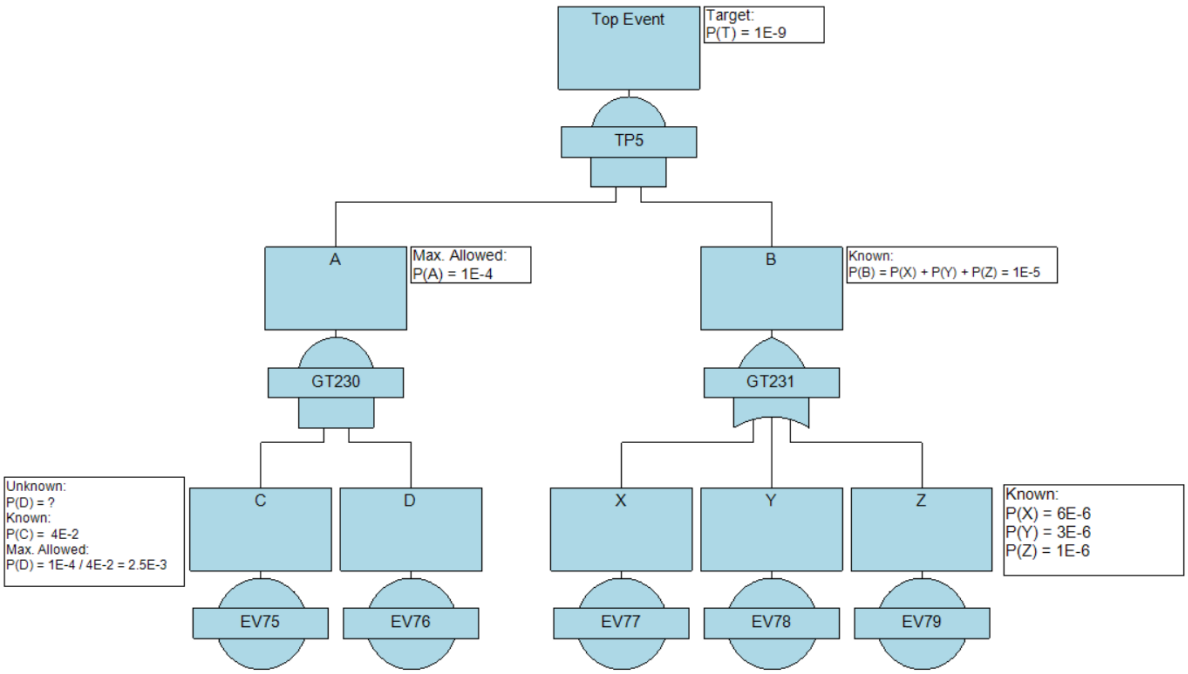


Figure 4.10: Failure rate unknown example

Lastly, a low-fidelity weight comparison is conducted. For this weight comparison, the weight for every major item present in the different concepts is accounted for. This is done by using empirical data provided by the thesis company and publicly available weight and performance data. Varying relations between maximum power output and power density will be taken into account for the GTE, batteries, E-motors and generators. This weight comparison aims to give an idea of how the different HEPS architecture types affect the HEPS weight.

5
Results

In this chapter, the results of the research activities presented in the previous chapter will be presented. They will be presented in the same order as the methodology in Chapter 4.

5.1. Baseline Architecture Identification

In Figure 5.1 an overview of the baseline architecture used to perform the safety analysis is provided. This figure also indicates all systems deemed part of the Hybrid-Electric Propulsion System (HEPS), except for the main and tail rotors, which are visualized to show how the HEPS is connected to both rotors. It is important to mention that the tail has an additional gearbox since it operates at a different rotation speed than the main rotor. All black-coloured connections are mechanical connections while the red-coloured connections are electrical connections. The sub-systems that are considered part of the HEPS:

- MGB: Main Gearbox
- GTE: Gas Turbine Engine (without fuel system)
- EPS: Electric Propulsion System, consisting of:
  - RGB = Reduction Gearbox
  - DU = Drive Unit (E-Motor + Motor Control Unit)
  - EES = Electric Energy Storage (Battery System)

This architecture is classified as a double-shaft parallel HEPS. Both sides of the propulsion system are connected separately into the MGB, where the mechanical power of both systems is combined before they are transferred to the main and tail rotors. Both DUs are combined in an RGB because the rotation speed of the E-Motors exceeds the operational limits of the MGB, it is necessary to reduce the rotation speed before transferring the mechanical power to the MGB, hence the name Reduction Gearbox. If there is only a single DU this reduction can be done at the MGB input stage after adapting the MGB. Both DUs are powered by a high-voltage battery (EES), and each EES is only connected to a single DU, thus leading to two separate power networks to the EPS. Both driveshafts connecting the engines to the MGB connect to a freewheel at the MGB to prevent blockage of the MGB. Blockage is when the rotor cannot move due to the MGB being stuck in a fixed position, leading to a catastrophic crash. For the same reason, both DU-RGB driveshafts are fitted with a "shear-neck", a mechanical device that destroys the mechanical connection when operational limits are exceeded.

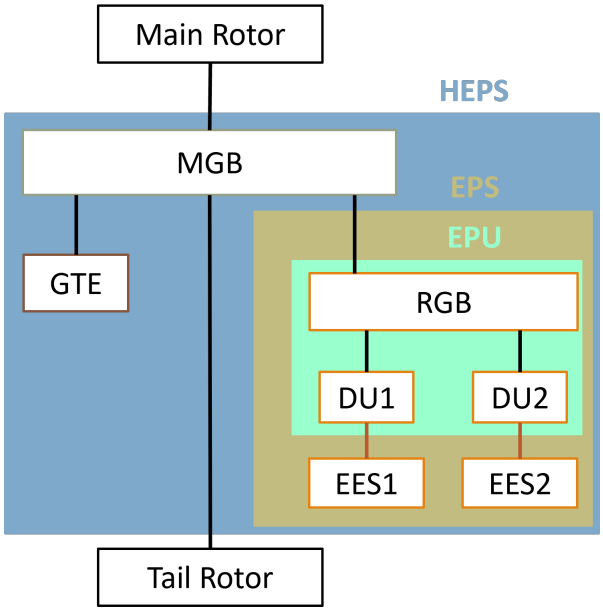


Figure 5.1: HEPS definition

5.2. HEPS System Functional Hazard Analysis

The functions that the HEPS or EHPS (Electric-Hybrid Propulsion System) must perform are listed below. The initial function list was created using the propulsion system Functional Hazard Assessments (FHAs) of other helicopters at the thesis company as a foundation. Next, the list of functions was discussed with system designers and safety experts at the thesis company to come to the final list presented below. Which functions are included in the FHA depends on which systems are considered in the FHA. To give an equal overview of the functions of the Gas Turbine Engine (GTE) and Electric Propulsion System (EPS) sides, for the System Functional Hazard Analysis (SFHA) the fuel system, both storage and distribution, was considered. Assumptions used in defining the function list are mentioned below the function explanation.

Function list:

F1 Provide mechanical power to MGB
- F1.1 Provide mechanical power to MGB with only GTE
- F1.2 Provide mechanical power to MGB with only EPS
- F1.3 Provide mechanical power to MGB with both GTE and EPS (hybrid mode)

F2 To store energy used for propulsion
- F2.1 Store electrical energy for EPS from on-ground charging
- F2.2 Store electrical energy for EPS from in-flight charging
- F2.3 Store chemical energy for GTE

F3 To distribute energy to propulsion systems
- F3.1 Distribute electrical energy for EPS
- F3.2 Distribute chemical energy for GTE

F4 To provide EHPS (Electric-Hybrid Propulsion System) controls and monitoring
- F4.1 To provide parameters for flight monitoring
- F4.2 To provide alerts to the flight crew
- F4.3 To provide Start and Stop controls
- F4.4 To provide engine cross-talk

F5 Protect Helicopter (H/C) and EHPS
- F5.1 Protect EHPS against overtorque
- F5.2 Protect EHPS against overspeed
- F5.3 Protect EHPS against internal short-circuit
- F5.4 Protect EHPS against external short-circuit

- F5.5 Protect EHPS against overvoltage
- F5.6 Protects H/C against fire
- F5.7 Protect H/C against high-energy debris

F6 Emergency engine shut-off

- F6.1 Emergency shut-off of GTE
- F6.2 Emergency shut-off of EPS

Function 1 is split into three sub-functions, representing three different scenarios. Function 1.1 represents a situation where the EPS does not contribute mechanical power while the GTE is on its maximum power setting. Inversely, in function 1.2 the GTE does not contribute any mechanical power while the EPS is on its maximum power setting. In function 1.3, the GTE and EPS contribute mechanical power, thus achieving a hybrid power mode.
Function 2 is also split into three sub-functions. Function 2.1 is defined as charging the batteries in between missions, whereas function 2.2 is defined as in-flight charging, also known as the generator function. Function 2.3 is storing the fuel for the GTE.
Function 3 is a standard function, split into two sub-functions. Function 3.1 is defined as distributing the electrical energy from the Electrical Energy System (EES) to the DU. Function 3.2 describes the fuel distribution system, which ensures fuel flow to the GTE.
Function 4 combines the control and monitoring functions, which could also be assessed separately. The parameters in function 4.1 are variables such as altitude and flight speed. The alerts in function 4.2 are meant to warn the pilots of dangerous situations or non-functioning systems. Function 4.3 points to the controls necessary to start up and shut down the engines. Function 4.4 mentions engine cross-talk, which comes down to torque and rpm matching between the different engines.
Function 5 contains all the protection functions. Functions 5.1 and 5.2 protect the EHPS against over-torque and overspeed respectively, which can occur in the GTE and EM. Functions 5.3 and 5.4 protect the EHPS against short-circuits. Functions 5.6 and 5.7 are protection functions present in more systems than just the HEPS and are aimed at protecting the helicopter against threats coming from the HEPS, whereas the other sub-functions aim at protecting the HEPS against threats originating from within.
Function 6 contains the emergency engine shut-off functions for the GTE and EPS. Which differs from function 4.3, by having the specification of an emergency environment.

Auto-rotation is an operating mode where the MGB does not transfer any mechanical power to the main rotor, but the rotor is allowed to rotate freely. It extracts energy from the airflow around it while in descent so that a flare-up is possible just before landing to soften the impact. A forced landing is an abrupt landing operating in case of an emergency.

From the defined functions, a list of functional failures/failure scenarios was created, covering the possible effects of the functions not operating as intended. The complete FHA worksheets can be found in Appendix A. Each of these functional failures is then grouped into a failure condition. These Failure Conditions (FCs) will be used as the starting points for the HEPS Preliminary System Safety Assessment (PSSA). In Table 5.1 an overview of the FCs and their corresponding severity and failure rate is provided. No Safety Effect (NSE) is a severity classification where the FC does not affect the safety of the helicopter, thus it also does not have a failure rate attached to it. FC.EHPS.001 refers to "OEI" which stands for One Engine Inoperative, indicating that at least half of the maximum power is available. In the architecture of the reference helicopter, FC.EHPS.001 is the situation where the EPS is not delivering any mechanical power to the main gearbox. Since the GTE supplies more than half of the mechanical power during normal operation, we can consider this situation "OEI". Inversely, in FC.EHPS.002, when the GTE is not delivering mechanical power to the main gearbox, less than half the nominal power is available, leading to a more severe failure effect than FC.EHPS.001. This is why these Failure Conditions have different severities and failure rate targets attributed to them.

FC ref	FC	Severity	Failure Rate
FC.EHPS.001	Partial loss of EHPS mechanical power (OEI rating)	MAJ	1.00E-05
FC.EHPS.002	Partial loss of EHPS mechanical power	HAZ	1.00E-07
FC.EHPS.003	Full loss of EHPS mechanical power	CAT	1.00E-09
FC.EHPS.004	No start of mission	NSE	-
FC.EHPS.005	Loss of in-flight charging	MAJ	1.00E-05
FC.EHPS.006	Impaired engine control	HAZ	1.00E-07
FC.EHPS.007	Uncontained fire	CAT	1.00E-09
FC.EHPS.008	High energy debris	CAT	1.00E-09
FC.EHPS.009	Degraded flight safety	MAJ	1.00E-05
FC.EHPS.010	Compromised flight safety	HAZ	1.00E-07
FC.EHPS.011	Contained thermal runaway	MAJ	1.00E-05

Table 5.1: FHA Failure Conditions

5.3. HEPS Preliminary System Safety Assessment (PSSA)

Initially, it was planned that all Failure Conditions (FCs) identified in the System Functional Hazard Assessment (SFHA) would be analyzed with a Failure Tree Analysis (FTA) in the HEPS PSSA. However, it was quickly discovered that not all of these Failure Conditions were usable for an FTA. The first reason for Failure Conditions to be excluded is when they have the severity classification "NSE", which stands for "No Safety Effect", as the term indicates, the failure condition has no effect on the safety of the helicopter and its passengers, thus there is no reason to analyze the Failure Condition further, this is standard industry practice.

The second reason for excluding Failure Conditions in the HEPS PSSA is that the FCs might be better suited to be analyzed using a Zonal Safety Analysis (ZSA) or Particular Risk Assessment (PRA). When a Failure Condition heavily depends on the specific placement of systems in the helicopter, it is better to analyze the Failure Condition in a Zonal Safety Assessment, as the name indicates, the ZSA is a spatial safety assessment, aimed at finding the failures relating basic installation, system interference and maintenance errors. FC.EHPS.011 was excluded since its installation has a major impact on the safety effect of a contained thermal runaway. With a contained thermal runaway no fire can spread to other systems, however, there are still gasses that need to be expelled from the battery system. Normally, this would be done by connecting a venting system to the outside of the helicopter. But, if this is not installed properly, it could affect the safety of the helicopter and its passengers.

Similarly, a Failure Condition can be more suited to analyze in a Particular Risk Assessment (PRA). A PRA is aimed at identifying failures that might occur due to events in other systems or from outside the helicopter. For example, FC.EHPS.007 is better suited for a PRA since an uncontained fire will not only affect the system where the fire originates but also the systems around it. For a similar reason FC.EHPS.008 was excluded from the FTA. High-energy debris released in one system can have detrimental effects on the surrounding systems, thus every system has to be evaluated specifically for this risk and this should be done in a PRA.

Lastly, there can be a changed perception of a Failure Condition that leads to it being excluded from further analyses. This is what happened to FC.EHPS.005. After the initial literature review, it looked like the loss of in-flight charging might have an impact in terms of safety. However, after reviewing the mission envisioned for the reference helicopter, it became clear that the loss of in-flight charging was not applicable. The reference helicopter would initially not have the ability to perform in-flight charging. Thus it was decided that it was unnecessary to further analyze this Failure Condition.

After the review of this list of Failure Conditions from the SFHA there were 7 FCs left, for these, an FTA was conducted. An example is given in Appendix B. The FTAs result in a list of Undesired Events (UE) for each subsystem, which are passed onto the subsystem PSSA. An extract of the list can be found in Appendix B. Below an overview of the UEs per subsystem is given. Here the Electric Propulsion Unit (EPU) entails both Drive Units (DUs) and the Reduction Gearbox (RGB) as one subsystem.

- **GTE**
  - UE.EHPS.001: GTE mechanical power output failure
  - UE.EHPS.002: Loss of fuel supply to GTE
  - UE.EHPS.003: Erroneous shutdown command from avionics
  - UE.EHPS.007: Loss of GTE - MGB link
  - UE.EHPS.009: Loss of MGB
  - UE.EHPS.012: Loss of GTE performance data transmission to avionics
  - UE.EHPS.014: Loss of GTE control
  - UE.EHPS.020: Loss of GTE alert data transmission
  - UE.EHPS.021: Loss of GTE alert data transmission + GTE failure
- **EES**
  - UE.EHPS.004: EPU mechanical power output failure
  - UE.EHPS.005: Loss of HV power to EPU
  - UE.EHPS.016: Loss of EES alert data transmission
  - UE.EHPS.017: Loss of EES alert data transmission + EES failure
- **Electronic Propulsion Unit (EPU = DU + RGB)**
  - UE.EHPS.004: EPU mechanical power output failure
  - UE.EHPS.005: Loss of HV power to EPU
  - UE.EHPS.008: Loss of EPU - MGB link
  - UE.EHPS.009: Loss of MGB
  - UE.EHPS.013: Loss of EPU performance data transmission to avionics
  - UE.EHPS.015: Loss of EPU control
  - UE.EHPS.022: Loss of EPU alert data transmission
  - UE.EHPS.023: Loss of EPU alert data transmission + EPU failure
- **MGB**
  - UE.EHPS.007: Loss of GTE - MGB link
  - UE.EHPS.008: Loss of EPU - MGB link
  - UE.EHPS.009: Loss of MGB
  - UE.EHPS.024: Loss of MGB alert data transmission
  - UE.EHPS.025: Loss of MGB alert data transmission + MGB failure

5.4. Subsystem Preliminary System Safety Assessment (PSSA)

The Undesired Events (UEs) defined in the previous section form the basis for Failure Conditions (FCs) in the subsystem-level Failure Tree Analysis (FTA). Additional FCs without an origin in the HEPS PSSA were analyzed. Because, as the subsystems become more detailed, completely new FCs may be found. The FCs originating directly from the HEPS-level PSSA retain the allocated failure rates and the downwards-cascaded Functional Development Assurance Level (FDAL) from the HEPS level. Now there is a complete overview of how failures progress on both the HEPS- and subsystem levels, with traceability of estimated failure rates and FDALs. Below, an overview of the FCs per subsystem is provided. The numbers are not completely continuous due to restructuring.

- Electrical Energy Storage (ESES):
  - FC.EES.001: Partial loss of EES energy discharge
  - FC.EES.002: Uncontained Fire
  - FC.EES.003: Complete loss of EES energy discharge
  - FC.EES.004: High Voltage (HV) - Low Voltage (LV) aggression
  - FC.EES.005: Battery burst
  - FC.EES.006: Loss of EES alert data transmission
  - FC.EES.007: Loss of EES alert data transmission + EES failure
- Gas Turbine Engine (GTE):
  - FC.GTE.001: GTE mechanical power output failure
  - FC.GTE.002: Loss of GTE performance data transmission to avionics
  - FC.GTE.003: Loss of GTE control
  - FC.GTE.004: Loss of GTE alert data transmission

  - FC.GTE.005: Loss of GTE alert data transmission + GTE failure
- Electric Propulsion Unit (EPU):
  - FC.EPU.001: Uncontained Fire in EPU
  - FC.EPU.002: Partial loss of mechanical power from EPU
  - FC.EPU.003: Total loss of mechanical power from EPU
  - FC.EPU.004: High energy debris from DU
  - FC.EPU.006: Loss of HV power to EPU
  - FC.EPU.008: Loss of EPU performance data transmission to avionics
  - FC.EPU.009: Loss of EPU control
  - FC.EPU.010: Loss of EPU alert data transmission
  - FC.EPU.011: Loss of EPU alert data transmission + EPU failure
- Main Gearbox (MGB):
  - FC.MGB.001: Total loss of mechanical power to main rotor
  - FC.MGB.002: Loss of EPU - MGB link
  - FC.MGB.003: Loss of GTE - MGB link
  - FC.MGB.004: Uncontained fire in MGB
  - FC.MGB.005: Loss of MGB alert data transmission
  - FC.MGB.006: Loss of MGB alert data transmission + MGB failure
  - FC.MGB.007: Loss of MGB - TGB link

5.5. Subsystem System Safety Assessment (SSA)

The subsystem PSSA provided a set of failure trees with failure rates and FDALs. However, the failure rates are a sample estimation originating from the FC failure rate targets set. During the SSA, the system design is validated by checking whether the FC failure rate targets are achieved. The results for each subsystem are given in Table 5.2, Table 5.3, Table 5.4 and Table 5.5.

In the column "FR Target" the failure rate targets attributed to the sub-system failure conditions during the Preliminary System Safety Assessment are given. These are the failure rates that the systems should be able to stay below. In the column "FR Estimate" the failure rates that the failure conditions are estimated to achieve are given. For this estimation, a failure rate was attributed to each basic event. This data originates from either a similar system used by the thesis company or from the NPRD database. As no test data is available for this specific system design, it cannot be said that this is the definitive failure rate that it will be able to achieve, hence it is called an estimation.

For the failure trees where the FC target failure rate was not met the subsystem design was adjusted until it met the target set. Below an overview of the FCs per subsystem is provided, with corresponding failure rate targets and achieved failure rates. It is important to note that not all FCs identified in the subsystem PSSA were used in the SSA, as some were deemed more fitting for a Particular Risk Analysis (PRA) or Zonal Safety Analysis (ZSA) and were thus removed from the FC list in the SSA. The SSA FC identification codes were also reassigned whereas the PSSA UE identification codes were not.

EHPS UE ref	FC ref	FC	FDAL	FR Target	FR Estimate
UE.EHPS.005	FC.EES.001	Complete loss of EES energy discharge	C	5E-04	3.31E-04
UE.EHPS.016	FC.EES.002	Loss of EES alert data transmission	C	1E-07	1.74E-08
UE.EHPS.017	FC.EES.003	Loss of EES alert data transmission + EES failure	B	1E-09	1.74E-12

Table 5.2: Subsystem SSA: EES FC

EHPS UE ref	FC ref	FC	FDAL	FR Target	FR Estimate
UE.EHPS.001	FC.GTE.001	GTE mechanical power output failure	B	1E-05	8.72E-06
UE.EHPS.014	FC.GTE.002	Loss of GTE control	C	7E-05	4.89E-05
UE.EHPS.020	FC.GTE.003	Loss of GTE alert data transmission	C	2E-07	3.31E-10
UE.EHPS.021	FC.GTE.004	Loss of GTE alert data transmission + GTE failure	B	1E-09	2.65E-14

Table 5.3: Subsystem SSA: GTE FC

EHPS UE ref	FC ref	FC	FDAL	FR Target	FR Estimate
UE.EHPS.008	FC.EPU.001	Total loss of mechanical power from EPU	C	1.00E-06	1.04E-07
UE.EHPS.015	FC.EPU.002	Loss of EPU control	C	7.00E-05	1.00E-19
UE.EHPS.022	FC.EPU.003	Loss of 1 DU alert data transmission	C	4.00E-04	4.08E-10
UE.EHPS.023	FC.EPU.004	Loss of EPU alert data transmission + EPU failure	B	1.00E-09	2.05E-13

Table 5.4: Subsystem SSA: EPU FC

EHPS UE ref	FC ref	FC	FDAL	FR Target	FR Estimate
UE.EHPS.009	FC.MGB.001	Total loss of mechanical power to main rotor	A	1E-10	1.08E-11
UE.EHPS.024	FC.MGB.002	Loss of MGB alert data transmission	C	2E-07	1.21E-09
UE.EHPS.025	FC.MGB.003	Loss of MGB alert data transmission + MGB failure	B	1E-09	1.70E-14
n.a.	FC.MGB.004	Loss of power transmission from to TGB	A	1E-10	2.00E-11

Table 5.5: Subsystem SSA: MGB FC

5.6. HEPS Common Mode Analysis (CMA)

For the CMA, no unresolved common modes were identified. Thus, no adaptations to the design were required. The SSA thus also remains unchanged. The questionnaire is provided in Appendix C.

5.7. Theoretical Concepts

To be able to compare different Hybrid-Electric Propulsion System (HEPS) architectures, a set of architectures had to be selected. The first concept was going to be similar to the reference case. This was a double-shaft parallel architecture type with two Drive Units, each consisting of an electrical motor and a motor control unit, and two Electric Energy Systems (EES) or batteries. The first goal of the comparison is to compare the 3 main types of coupled HEPS architectures. These are the parallel, series-parallel and series architecture types. For the parallel architecture type architectures for both sub-types (single-shaft / double-shaft) were created. To best assess the difference caused by the architecture types for each type an architecture was created featuring two Drive Units and two EES. Another aim was to show the influence of the amount of Drive Units and EES in a HEPS. To achieve this, for each of the three main architecture types a concept architecture was created with only a single Drive Unit and a single EES.

During the concept identification phase an additional concept was created featuring a direct connection from the Drive Units to the tail rotor instead of the main gearbox. Even though this is a rather unrealistic concept, it might show how such an architectural choice can affect the safety assessment. The idea came after reading a lot of literature on HEPS systems, where an option that is often mentioned is to only use electric propulsion for the tail rotor. From this idea a second concept was created, an uncoupled HEPS architecture. The idea is that it would show why most papers on HEPS performance do not even consider uncoupled HEPS.

Finally, to allow for a comparison with conventional twin-engine helicopters a concept with 2 Gas Turbine Engines (GTEs) was added. In total, 9 different HEPS concepts were selected. A schematic overview of each concept is provided in Appendix D.

- C1: Double-shaft parallel - 2 Drive Unit (DU) + 2 Electric Energy System (EES)
- C2: Double-shaft parallel - 1 DU + 1 EES
- C3: Single-shaft parallel - 2 DU + 2 EES
- C4: Series-parallel - 2 DU + 2 EES
- C5: Series-parallel- 1 DU + 1 EES
- C6: Series - 2 DU + 2 EES
- C7: Series - 1 DU + 1 EES
- C8: Double-shaft parallel - Electrified tail
- C9: Uncoupled - Electrified tail
- CONV: Conventional - 2 GTE

5.8. Comparative Analysis

5.8.1. Failure Condition (FC) Selection

The five Failure Conditions selected originate from the safety analysis conducted in the reference case. FC1 was selected to show how choices in HEPS architecture affect warning and monitoring systems. FC2, FC3 and FC4 logically are heavily impacted by the choices in HEPS architecture and were thus deemed perfect as a showcase for this study. FC5 was selected to show how propulsion system controls can be affected by HEPS architecture choices. Another advantage of this selection is that it contains FCs classified as Catastrophic, Hazardous and Major. In the results, it can be seen that a higher classification of the FC does not necessarily lead to an FC that is more difficult to achieve, the difficulty also depends heavily on the nature of the FC. For all concepts, all FCs were evaluated with a failure tree analysis.

- FC1: Loss of alert data transmission
- FC2: Loss of power to the main rotor
- FC3: Partial loss of power to the main rotor
- FC4: Loss of power to the tail rotor

- FC5: Loss of EHPS control

To perform a Failure Tree Analysis (FTA) some basic building blocks were created that could easily be moved around the failure tree and copied if necessary, as is shown in Figure 5.2. Here EV1, EV2, EV3, EV4 and EV5 are the basic building blocks.

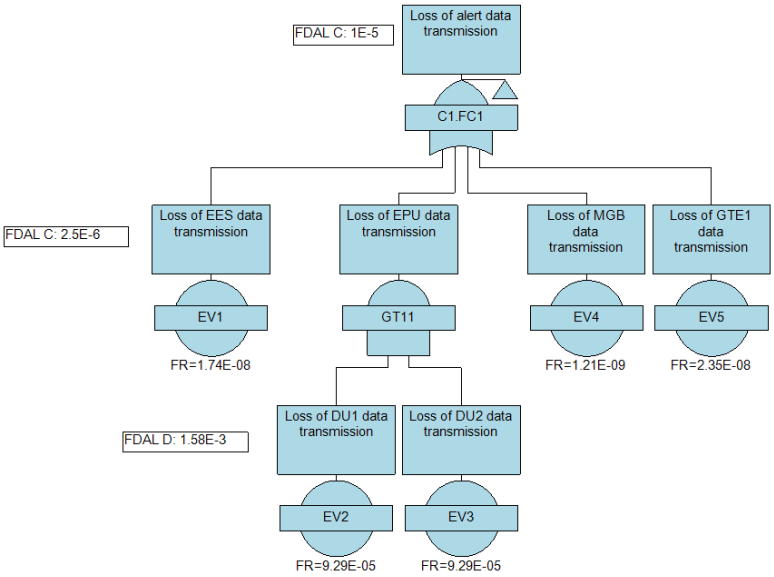


Figure 5.2: Concept 1, Failure Condition 1

5.8.2. Top-down Failure Tree Analysis (FTA)

To be able to perform a top-down comparison first all of the FCs were classified with a severity, a matching failure rate target and a matching Function Development Assurance Level (FDAL), as provided in Table 5.6. The top-down failure allocation method provided the first comparison. Throughout the top-down method, 74 separate basic events were identified. Since the majority are not present in all concepts, the comparison of these basic events does not provide much usable information. However, basic events EV1 through EV22 are present in most or all concepts and thus provide insight into how early failure rate allocation changes with different HEPS architectures.
In the top-down approach, the failure rates of all basic events are assumed to be unknown. The only known failure rate is the failure rate attributed to the top-level Failure Condition. This failure rate is then cascaded downwards in the failure tree using boolean logic, as explained in Section 4.3. Table 5.7 shows the results for the first 5 basic events, while the results for EV1 through EV22 are provided in Section E.2. The full results for FC2 are provided in Section E.1. The first 5 basic events are all part of FC1 and represent the loss of alert data transmission for the different subsystems. The green-coloured cells are the concepts with the highest allocated failure rates per basic event. If the failure rate that is initially attributed to a basic event is higher it means, that the basic event is allowed to occur more frequently. The item is thus allowed to have a higher failure ratio. Since failure ratios differ for similar items from supplier to supplier, this extra margin can make the difference between selecting one item or another.

Ref	FC	Severity	FR Target	FDAL
FC1	Loss of alert data transmission	Major	1E-5	C
FC2	Loss of power to the main rotor	Catastrophic	1E-9	A
FC3	Partial loss of power to the main rotor	Major	1E-5	C
FC4	Loss of power to the tail rotor	Catastrophic	1E-9	A
FC5	Loss of EHPS control	Hazardous	1E-7	B

Table 5.6: Comparison FC classification

Concept	EV1	EV2	EV3	EV4	EV5
	EES data	DU1 data	DU2 data	MGB data	GTE data
C1	2.50E-06	1.58E-03	1.58E-03	2.50E-06	2.50E-06
C2	2.50E-06	2.50E-06	n.a	2.50E-06	2.50E-06
C3	2.50E-06	1.58E-03	1.58E-03	2.50E-06	2.50E-06
C4	2.00E-06	1.41E-03	1.41E-03	2.00E-06	2.00E-06
C5	2.00E-06	2.00E-06	n.a	2.00E-06	2.00E-06
C6	2.00E-06	1.41E-03	1.41E-03	2.00E-06	2.00E-06
C7	2.00E-06	2.00E-06	n.a	2.00E-06	2.00E-06
C8	2.50E-06	1.58E-03	1.58E-03	2.50E-06	2.50E-05
C9	2.50E-06	1.58E-03	1.58E-03	2.50E-06	2.50E-06
CONV	n.a	n.a	n.a	3.33E-06	3.33E-06

Table 5.7: Top-down allocation results EV1-EV5

5.8.3. Bottom-up FTA

The next analysis method is the bottom-up analysis, where the failure rates of each basic event are filled in to calculate the failure rate of the Failure Conditions (FCs) for each concept. Each basic block used has a fixed failure rate. These failure rates come directly from the results of the subsystem SSA. For example, for EV1, the failure rate is 1.74E-8, which comes directly from the failure rate found for FC.EES.002. However, the basic blocks do not always correspond to a subsystem-level FC, they can also come from gates within those trees. An example of this is basic event EV7, which is a part of FC2. The failure rate for EV7 comes from a mid-level gate in FC.EPU.001: "Total loss of mechanical power from EPU", as showcased in Figure 5.3.

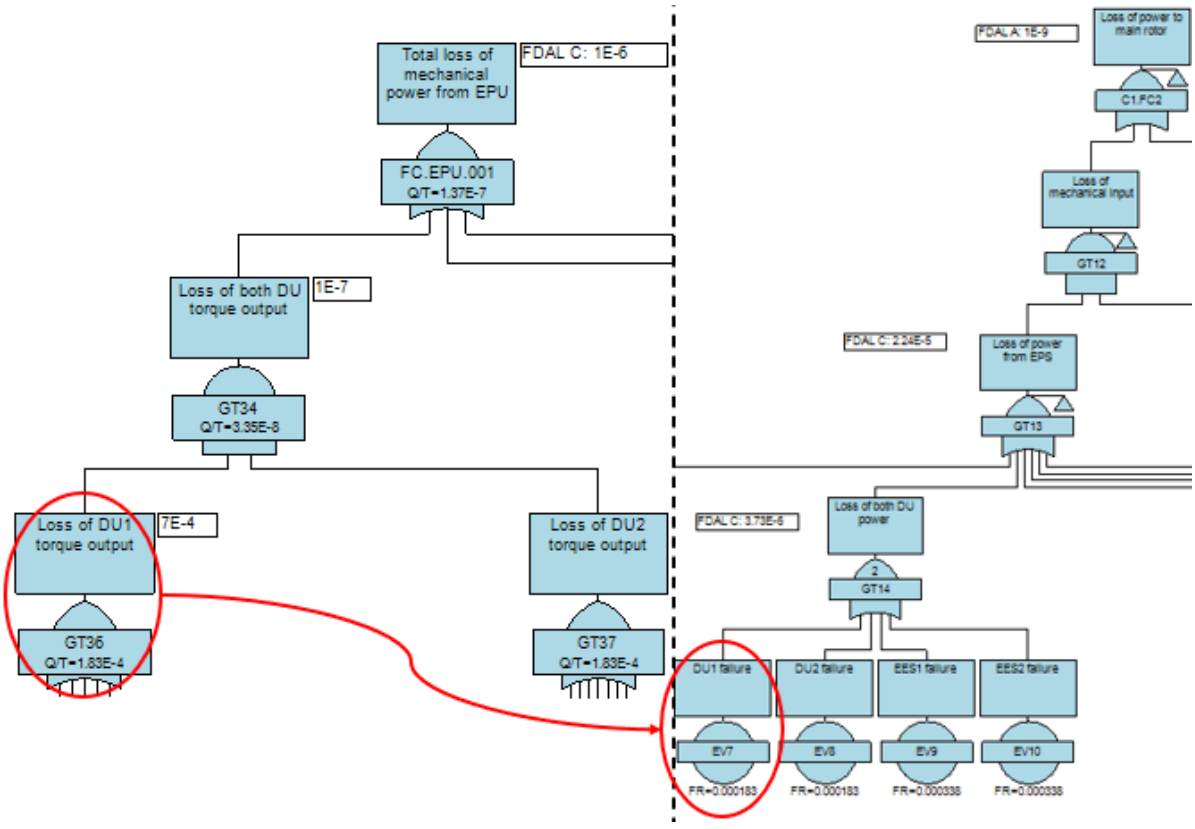


Figure 5.3: EV7 failure rate substantiation

In Table 5.8 the complete results of the bottom-up approach are provided, and the supporting failure trees for FC2 can be found in Appendix E. All of the failure rates are compared to the target failure rates for each FC. If it is close to achieving the target, or if the target is barely achieved, the cell is coloured

yellow. Further, the highest failure rates are red-coloured and the lowest failure rates are green-coloured. The failure rates that fall in between these values are dynamically coloured depending on their position in the range.

The results from the bottom-up Failure Tree Analysis are critical to the safety analysis. It acts as a verification of the system design by evaluating the failure rates of the system. If a failure rate target is not achieved, it will trigger a system redesign. If for a specific Failure Condition, the calculated failure rate is higher than the target failure rate, but still, in the same order of magnitude, the problem can be resolved by using higher-quality parts or a small design adaptation. However, if the calculated failure rate is one or more magnitudes higher than the target failure rate, a significant system redesign will be required, leading to a redesign of other systems. From Table 5.8 it is immediately apparent that the choice in HEPS architecture can heavily affect its failure rates. It should be noted that especially the concepts with a single drive unit and a single battery system perform worse compared to their counterparts.

For each of the concepts, assumptions were made as to what subsystem failures lead to FC2: "Total Loss of Mechanical Power" and FC3: "Partial Loss of Mechanical Power". Since these definitions are not standardized, it is up to the safety engineer to define them in their FTA. For all of the parallel-type architectures (C1-C3, C8) a total loss of power equates to losing power from the Electrical Propulsion System (EPS) and the GTE simultaneously. For parallel architectures with two DUs (C1, C3, C8) a partial loss of power constitutes losing all power from the GTE or a partial loss of power from the EPS. A partial loss of power from the EPU translates to losing power from one of the DUs. The parallel concept with only 1 DU (C2) is said to have a partial loss of power when either the GTE or the DU loses all power.

The same logic is applied to the series-parallel architecture type concepts (C4, C5) with the only difference being in the definition of a partial loss of mechanical power. For this architecture type losing the generator leads to a partial loss of power, the logic behind this is that the generator is used to generate power for the EPS, which would then not be able to deliver the requested power during the entire mission. As such this is also considered a partial loss of mechanical power.

For the series architecture type concepts (C6, C7) a full loss of mechanical power constitutes losing the EPU, losing the generator or losing the GTE. The loss of the EPU can be caused by either losing both DUs or both EES or a combination of one DU and one EES which are independent of each other. A partial loss of power is considered losing one of the DUs or one of the EES.

Further on, there are no failure rates for FC3 for concepts C7 and C9 since losing a single propulsion system leads to a complete loss of power, and thus no partial loss of power can take place. Specifically, in concept C7, if either the GTE or DU fails it will lead to a total loss of power. In concept C9, the main rotor is only powered by the GTE, thus a loss of GTE will result in a total loss of power to the main rotor.

Concept	**Category**	**Detail**	**FC1**	**FC2**	**FC3**	**FC4**	**FC5**
			1.00E-05	**1.00E-09**	**1.00E-05**	**1.00E-09**	**1.00E-07**
C1	Double-shaft parallel	2 DU + 2 EES	5.07E-08	2.26E-11	1.05E-05	4.26E-11	2.84E-14
C2	Double-shaft parallel	1 DU + 1 EES	9.29E-05	5.67E-08	6.20E-03	5.67E-08	1.18E-09
C3	Single-shaft parallel	2 DU + 2 EES	5.07E-08	3.26E-11	1.05E-05	4.26E-11	2.84E-14
C4	Series-parallel	2 DU + 2 EES	5.17E-08	2.26E-11	2.17E-04	4.26E-11	1.93E-09
C5	Series-parallel	1 DU + 1 EES	9.29E-05	5.67E-08	6.20E-03	5.67E-08	3.11E-09
C6	Series	2 DU + 2 EES	5.17E-08	2.15E-04	1.23E-02	2.15E-04	4.89E-05
C7	Series	1 DU + 1 EES	9.29E-05	6.41E-03	-	6.41E-03	1.12E-04
C8	Double-shaft parallel	Electrified tail	5.07E-08	2.26E-11	1.05E-05	1.38E-06	2.84E-14
C9	Uncoupled	Electrified tail	5.07E-08	9.15E-06	-	3.98E-07	2.84E-14
CONV	Conventional	2 GTE	4.82E-08	9.37E-11	1.83E-05	1.14E-10	2.39E-09

Table 5.8: Bottom-up results

Since the baseline was a concept with a parallel engine architecture an additional look was taken at the

series-parallel and series architectures. This was done by taking concepts C4 and C6 and adapting them. They were adapted to reach or at least close the distance to the target failure rates for all of the FCs. Additional subsystems were introduced, such as an additional Drive Unit (DU) or Generator (GEN). This led to the establishment of concepts C4A and C6A.

For concept C4A there are two generators instead of 1, a relatively simple adjustment (Figure 5.4). The only Failure Condition (FC) where concept C4 did not achieve the target failure rate was FC3: "Partial loss of power to main rotor". To figure out where the problem originated the failure tree was further analyzed. As previously stated, for this concept it was assumed the loss of the GEN leads to a partial loss of power. As such, the failure rate of the GEN has a high impact on the top-level failure rate. This can also be shown numerically, the failure rate for a GEN was identified to be 2.07E-4, leading to a top-level failure rate of 2.17E-4. The GEN is by far the biggest contributor to this. However, this contribution can be decreased by the introduction of a second GEN. Now, both generators are required to fail to constitute as a partial loss of power to the main rotor. This leads to an AND-gate where there was previously the basic event of the GEN failure. Following the boolean logic explained previously, the AND-gate has a failure rate of $(2.07E-4)^2 = 4.28E-8$. After the failure rate decrease of one branch of the failure tree, the top-level failure rate decreased to 1.06E-5, putting it near the failure rate target.

For concept 6A major adjustments were made; 1 additional DU, 1 additional EES, 1 additional GTE and 2 additional GEN were added (Figure 5.5). Concept C6 only reached the failure rate target for FC1, meaning the failure trees for FC2, FC3, FC4 and FC5 have to be reanalyzed to ensure that the top-level failure rates for these FCs were improved. For FC2: "Full loss of power to main rotor" the branches for power from the DUs, power from the GTE and the generator were identified as critical. This led to the introduction of 1 additional DU, 1 additional EES, 1 additional GTE and 2 additional GEN. This also immediately influenced the failure rates of the other FCs, as the failure tree structure was heavily affected by these additions. It is important to note that for FC3: "Partial loss of power to main rotor", whenever there are three identical systems, a partial loss of power constitutes losing two out of the three. For example, a partial loss of power originating from the GEN can only be caused by losing two GEN. In the end, this was a major redesign of the HEPS, showcasing how the failure analysis can send a design back to the drawing board.

The effect on the FCs is visible in Table 5.9. For concept 4A there is a significant improvement, as the failure rate for FC3 has dropped by 95%. Concept 6A now reaches 4 failure rate targets and significantly improved the one that failed to reach its target failure rate.

Concept	**Category**	**Detail**	**FC1**	**FC2**	**FC3**	**FC4**	**FC5**
			1.00E-05	**1.00E-09**	**1.00E-05**	**1.00E-09**	**1.00E-07**
C4	Series-parallel	2 DU + 2 EES	5.17E-08	2.26E-11	2.17E-04	4.26E-11	1.93E-09
C4A	Series-parallel	Adjusted	5.08E-08	2.26E-11	1.06E-05	4.26E-11	1.05E-13
C6	Series	2 DU + 2 EES	5.17E-08	2.15E-04	1.23E-02	2.15E-04	4.89E-05
C6A	Series	Adjusted	1.87E-08	1.60E-10	9.72E-05	1.80E-10	1.93E-13

Table 5.9: Concept adaptation results

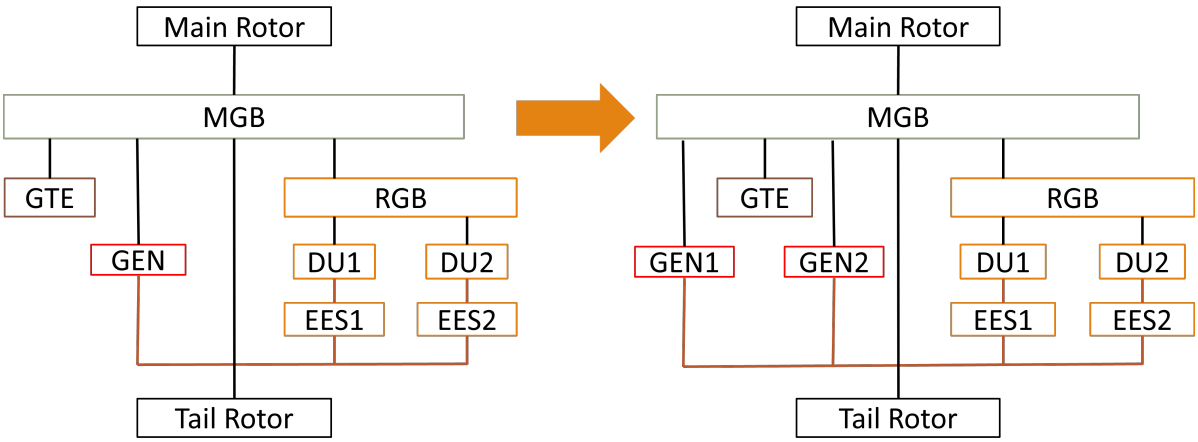


Figure 5.4: Concept C4 to concept C4A

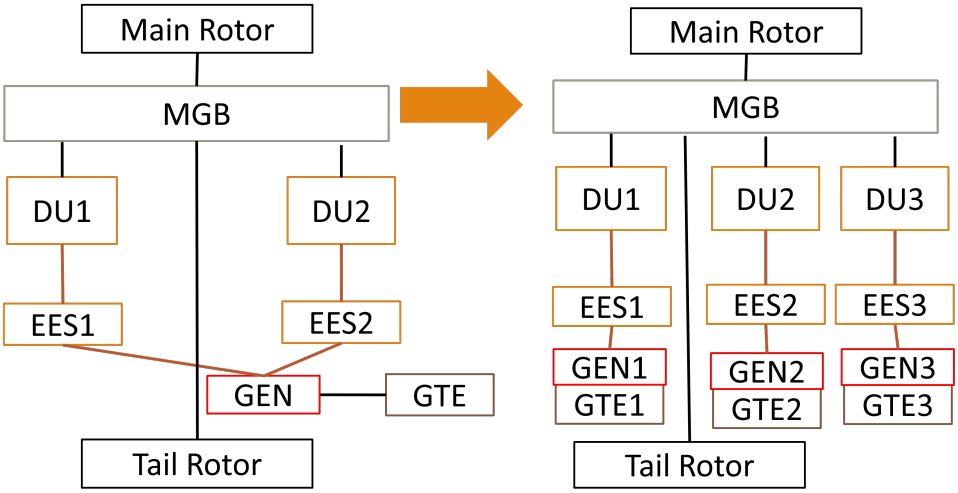


Figure 5.5: Concept C6 to concept C6A

5.8.4. Weight Comparison

To get a grasp of the impact the choice in HEPS architecture has on weight, one of the most important facets in rotorcraft design, a low-fidelity weight estimation was conducted. The results of this analysis can be seen in Table 5.10. The weight change provided is relative to the weight from the baseline concept, thus equal to concept C1. The cells are colour-coded, where green indicates the lowest weight and red is the highest weight among the HEPS. Additionally, a weight estimation is provided for a conventional propulsion system. The concepts are compared to the baseline as this study aims to describe the effects of the different HEPS architecture types in the baseline. This study is not aimed at providing the possible advantages and disadvantages of a HEPS compared to a conventional propulsion system.

Weight information was available internally at the thesis company for the systems in the baseline concept. However, this data was unavailable for the systems only present in the other concepts. Thus, for every "unknown system weight", similar systems with publicly or internally available data were analyzed to find a power density. The systems were sized for maximum continuous power per subsystem, the maximum power is the power a system can provide indefinitely. Thus, a system containing two DUs and one containing a single DU with the same maximum continuous power will not have the same weight. This is similar to how two bottles of 1 litre and one bottle of 2 litre do not have the same total plastic container weight. When multiple data points containing a power density and a maximum

continuous power were found, the data was extrapolated to estimate the power density realistically over the entire range. Generally, there were only two or three data points per system. These data points consisted of a (inverse) power density and a maximum continuous power. These data points were then put in a graph and a trend line was automatically created by Microsoft Excel. Excel has multiple types of trend lines available such as linear, exponential, polynomial and power series. The trend lines were evaluated on behaviour over a large range of maximum continuous power. It was found that the power series trend lines showed the most realistic behaviour over this range. Thus every system with an extrapolated weight was fitted with a power series trend-line that was used to scale the system power density and thus weight according to the maximum continuous power. The systems which were scaled with the maximum continuous power are the E-Motor (EMOTs), the Motor Control Units (MCUs), the Generators (GENs), the batteries (EES) and the Gas Turbine Engine (GTE). These were selected as they have the largest influence on the HEPS weight. The graphs containing the trend lines of these subsystems can be found in Appendix E. Some subsystems and items remained at a constant weight such as the drive shafts, the Main Gearbox (MGB) and the Reduction Gearbox (RGB). Of course, not every concept requires an RGB. Since the total mechanical power required remained constant in the comparison, these mechanical parts could retain their original weight. The high-voltage power cables required for the Electrical Propulsion System (EPS) were scaled with maximum power and cable length for each concept. The weight contributions of items with a minor contribution to the total system weight were multiplied by the number of identical subsystems of which they are a part.

The EES, or batteries, were also sized for total energy, for which the energy density was extrapolated. This was necessary since the maximum stored energy is an important trait affecting EES weight. The maximum stored energy and continuous power were used to estimate the amount of battery cells required, which were then equally divided between the EES present in the concept. Additionally, the number of EES in a concept equalled the number of parallel strings of battery cells, since the assembly weight differs due to the additional casing required with multiple separate EES.

Concept	Category	Detail	Weight change [kg]	Weight change [%]
C1	Double-shaft parallel	2 DU + 2 EES	0	0
C2	Double-shaft parallel	1 DU + 1 EES	-63	-7
C3	Single-shaft parallel	2 DU + 2 EES	0	0
C4	Series-parallel	2 DU + 2 EES	121	14
C4A	Series-parallel	Adjusted	124	14
C5	Series-parallel	1 DU + 1 EES	58	7
C6	Series	2 DU + 2 EES	577	66
C6A	Series	Adjusted	659	75
C7	Series	1 DU + 1 EES	546	62
C8	Double-shaft parallel	Electrified tail	0	0
C9	Uncoupled	Electrified tail	1070	122
CONV	Conventional	2 GTE	-303	-34

Table 5.10: Weight Estimation Results

5.8.5. Remainder Failure Tree Analysis (FTA)

Another analysis conducted was FTA where only a single basic event has an unknown failure rate, referred to in this thesis as the "Remainder FTA". This single basic event is a basic event that is already present in the failure tree, but was selected to stay unknown in this analysis. Because the Failure Condition (FC) failure rate target is known, the "left-over" failure rate can be calculated. As a showcase, this was done for the basic event EV-7 "DU1 failure", the result is provided in Table 5.11. If the failure rate is positive (green), there is a failure rate for the basic event where the FC target failure rate is achieved. If the failure rate is negative (red), there is no failure rate for the basic event where the FC target failure rate is achieved. This is validated in Table 5.8, specifically for FC2, which is the FC where EV-7 originates from. This analysis shows that even when no data is available for a single basic event in the fault tree, it is possible to estimate whether the system will achieve the failure rate target.

Concept	**Category**	**Detail**	**EV7**
C1	Double-shaft parallel	2 DU + 2 EES	9.68E-03
C2	Double-shaft parallel	1 DU + 1 EES	-5.92E-03
C3	Single-shaft parallel	2 DU + 2 EES	9.64E-03
C4	Series-parallel	2 DU + 2 EES	9.70E-03
C4A	Series-parallel	Adjusted	9.70E-03
C5	Series-parallel	1 DU + 1 EES	-5.92E-03
C6	Series	2 DU + 2 EES	-6.34E-01
C6A	Series	Adjusted	3.28E-03
C7	Series	1 DU + 1 EES	-6.24E-03
C8	Double-shaft parallel	Electrified tail	1.77E-02
C9	Uncoupled	Electrified tail	-
CONV	Conventional	2 GTE	-
Actual Failure Rate			1.83E-4

Table 5.11: EV-7 Remainder Analysis Results

5.8.6. GTE/EPS FDAL

An FTA can also be conducted qualitatively, without failure rates. This can be done by analyzing the Function Development Assurance Levels (FDALs) attributed to the subsystems. The higher an FDAL, the more development costs and development time a system requires. Having the same system with a lower FDAL is generally desirable. In comparing HEPS architectures, it is interesting to break it down for the two engine types present, the GTE and the Electrical Propulsion System, the EPS. The result is provided in Table 5.12. It is important to reiterate that a lower FDAL is always desired since it has less stringent development requirements and thus lower development costs. In Table 5.12, FDAL C is the most optimal, followed by FDAL B and finally FDAL A. The results show that the architecture types affect the EPS FDAL. Both the parallel and series-parallel allow an FDAL C for the EPS while the series needs an FDAL A for the EPS. However, the architecture types do not affect the GTE FDAL, as it is always FDAL A. For the conventional concept, the GTE has FDAL B, this was decided following standard practice at the thesis company.

Concept	Category	Detail	EPS FDAL	GTE FDAL
C1	Double-shaft parallel	2 DU + 2 EES	C	A
C2	Double-shaft parallel	1 DU + 1 EES	C	A
C3	Single-shaft parallel	2 DU + 2 EES	C	A
C4	Series-parallel	2 DU + 2 EES	C	A
C4A	Series-parallel	Adjusted	C	A
C5	Series-parallel	1 DU + 1 EES	C	A
C6	Series	2 DU + 2 EES	A	A
C6A	Series	Adjusted	A	A
C7	Series	1 DU + 1 EES	A	A
C8	Double-shaft parallel	Electrified tail	A	A
C9	Uncoupled	Electrified tail	A	A
CONV	Conventional	2 GTE	-	B

Table 5.12: GTE FDAL and EPS FDAL

5.8.7. HEPS Complexity

Aside from FDAL analysis, a more basic qualitative analysis can be conducted to understand the impact of HEPS architecture choice. This is done by counting the number of subsystems in the HEPS for each architecture. For each subsystem added, more subsystems must be integrated, more interfaces must be considered, and more internal mounting points are required. This all adds to the complexity of implementing the HEPS architecture. In Table 5.13 the overview of the number of subsystems per concept is provided, colour-coded from best (green) to worst (red). Lower HEPS complexity makes it easier to integrate and place the different systems and will lead to fewer spatial placement constraints.

Concept	Category	Detail	Total Subsystems
C1	Double-shaft parallel	2 DU + 2 EES	6
C2	Double-shaft parallel	1 DU + 1 EES	4
C3	Single-shaft parallel	2 DU + 2 EES	6
C4	Series-parallel	2 DU + 2 EES	7
C4A	Series-parallel	Adjusted	8
C5	Series-parallel	1 DU + 1 EES	5
C6	Series	2 DU + 2 EES	7
C6A	Series	Adjusted	13
C7	Series	1 DU + 1 EES	5
C8	Double-shaft parallel	Electrified tail	5
C9	Uncoupled	Electrified tail	6
CONV	Conventional	2 GTE	3

Table 5.13: Subsystem per concept

6

Validation

In every academic research, the methods used must be validated. This chapter is aimed at providing this validation. This study is not a standard academic study, where a unique method is used to answer a research question. The study follows a more practical method to answer the research questions posed. As laid out in the previous chapter, the first part of the study revolves around the safety analysis of a reference case. The safety analysis is performed by industry standards. More specifically, it follows processes described by SAE ARP 4754A and SAE ARP 4761. These methods thus do not require verification.

For the data used as an input for the Failure Tree Analysis (FTA) of the reference case and the concept comparison, validation is equally non-standard. All of the data used as input originated from internal test data at the thesis company or the NPRD database. All of the data used was already verified by the sources before usage. As such, the input data does not require additional validation.

For the reference case, each of the resulting outcomes such as function lists and failure trees was validated by experts at the thesis company who guided me in every step of the safety analysis. This means that the experts were extensively asked whether the outcomes were realistic. For the concept comparison, each concept was discussed with a helicopter architect and system engineers for relevant systems. A helicopter architect is responsible for the overall design of a helicopter while a system engineer is an expert on a specific system, for example, the electrical system or the transmission system. The helicopter architect was consulted to discuss the theoretical architectures and whether it is technically possible to create them. The system engineers were consulted to verify what the HEPS architecture would require from the systems to function and which integration methods should be applied. Thus, the theoretical concepts were verified through expert consultation.

Finally, for the results of the concept comparison, the failure trees were discussed with safety engineers at the thesis company, to discuss whether they were realistic. The failure trees presented in this study and the results flowing from them were deemed realistic. The failure rates found for the top-level failure conditions in the concept comparison were also deemed realistic. From safety engineering logic, the parallel architecture type should have the lowest failure rates, followed by the series-parallel architecture type, and the series architecture type should have the highest failure rates. This is due to the parallel architecture type having independent mechanical power sources. Meanwhile, the series-parallel architecture type has two mechanical power sources which are connected through a generator but are separately connected to the main gearbox, these are thus semi-independent. For the series architecture, both mechanical power sources are integrated into a single source leading to the main gearbox and thus fully dependent on each other. For the data used in the weight estimation, all input data directly originated from internal weight data of the thesis company or its suppliers, further expanded by publicly available supplier data. Even though this data might not be 100% accurate, it is the most accurate data available next to weighing every single part, leaving it as the most viable option. The weight data could thus not be verified any further.

7

Discussion

After the presentation of the results, this chapter will link the results back to the research questions posed at the start of the thesis research. Next, this chapter will also discuss the limitations of the different analyses conducted and how these could be improved.

7.1. Answering the research questions

Research question 1: How is the safety analysis for helicopters conducted?

The safety analysis for helicopters is conducted by following multiple standards, of which the most important are SAE ARP 4761 and SAE ARP 4754. The analysis is conducted on three levels, the aircraft level, the system level, and the item level. First, the functions are allocated from the aircraft level down to the item level and integrated again from the item level back up to the aircraft level.

Sub-question 1.1: What type of risk assessment is done at the aircraft/function/system level?

On the aircraft level, the assessments conducted are the Aircraft Functional Hazard Assessment (FHA), the Aircraft Common Cause Analysis (CCA) and the (Preliminary) Aircraft Safety Analysis. On the system level, the assessments conducted are the SFHA, the System CCA and the (P)SSA. On the item level, the assessments conducted are the System FTA and System Common Mode Analysis (CMA). In practice, this means first all of the aircraft or system functions are identified. From these functions, Failure Conditions are identified, classifying specific failures of the functions. From these Failure Conditions, failure trees are created, identifying the root causes (basic events) that cascade from the item level up to the aircraft level. After completely mapping the failure trees, the CCA is used to identify possible failures that could lead to single-failure catastrophic situations. If such causes are identified, they need to be addressed by introducing additional redundancy and/or dissimilarity. Finally, all the items are integrated into (sub-)systems which are then integrated on the aircraft level, leading to a complete overview of the safety of the aircraft.

Sub-question 1.2: How is it ensured that the failure rate estimates are conservative?

There are multiple ways in which conservative estimates can be ensured. The first way is to set the target failure rates for the system-level failure conditions lower than the maximum failure rate prescribed in the safety standards. Secondly, whenever an empirical database such as the NPRD is used, the item with the highest failure rate should be selected, ensuring that the actual failure rate will always be lower than the estimate. Thirdly, mechanical parts such as driveshafts and gearboxes are over-designed in terms of strength to ensure a failure rate of 1E-15/FH. In total, this leads to a highly conservative failure rate estimate for all the top-level failure conditions. This is done to ensure the safety targets are reached and to account for undiscovered failure events.

Research question 2: What are the most critical (sub-)systems with respect to safety for helicopters?

The most critical (sub-)systems are the systems which cause the helicopter to crash with only a single failure. The only systems with this criticality are the MGB and the main rotor since there are no redundant systems covering the same functions. Gas Turbine Engines (GTEs) and E-Motors (EMs) can cause Main Gearbox (MGB) failure by causing “blockage”, which is when a drive shaft is blocking the gears from rotating in the MGB, thus also blocking the movement of the rotor. Common modes can also turn (sub-)systems into additional critical parts.

Sub-question 2.1: What functions should a HEPS perform?

There are 6 main functions that a HEPS should perform are:

F1 Provide mechanical power to MGB
F2 To store energy used for propulsion
F3 To distribute energy to propulsion systems
F4 To provide EHPS controls and monitoring
F5 Protect Helicopter (H/C) and EHPS
F6 Emergency engine shut-off

Sub-question 2.2: How can part/system/function redundancy be achieved in HEPS

Firstly, for the mechanical power output, having two independent low-voltage power sources leading to the same GTE or EM constitutes redundancy. For the EMs, an additional option is possible compared to the GTE. EMs can be "double-winded", where there are two independent magnetic spool systems in one EM, leading to a redundancy in power, however, this might not be the same power as when both spools are active. The most common way to ensure redundancy for electrical propulsion is by distributing the requested power over multiple independent E-motors. Secondly, for engine control, having two independent engine controllers for one engine ensures redundancy. Thirdly, for alert data transmission, redundancy can be achieved by having multiple sensors with the same functionality. Battery systems or EES as they are often referred to in this report, have unique internal redundancy possibilities since they consist of large quantities of identical parts. For the Electric Propulsion System (EPS) as a whole, redundancy can be achieved by having multiple Electrical Energy Systems (EESs) with independent High-Voltage (HV) cables to the different Drive Units (DUs).

Sub-question 2.3: What are the most critical common modes?

All resources shared by multiple (sub-)systems can be considered common modes. The most critical of which are:

- Low-Voltage (LV) Power
- High-Voltage Power
- Data
- Cooling fluids
- Lubrication fluids

For all of these common modes, redundancy should be evaluated to ensure independence for critical (sub-)systems.

Research question 3: What are the most frequent failures for HEPS?

The most frequent failures for HEPS can be identified by looking at the failure rates of all basic events identified in the concept comparison. The basic events with the highest failure rates are the ones that occur the most frequently.

Sub-question 3.1: What are the most frequent failures in helicopter GTEs?

The basic events with the highest failure rates for the GTE are mechanical engine failures and a loss of LV power supply.

Sub-question 3.2: What are the most frequent failures in EMs?

The basic events with the highest failure rates for the EM are motor control unit failures and a loss of LV power supply.

Sub-question 3.3: What are the most frequent failures in battery systems?

The basic events with the highest failure rates for the EM are battery management system failures and a loss of LV power supply.

Research question 4: How do the different HEPS architecture types affect the safety analysis?

The different HEPS architecture types affect the safety analysis in multiple ways. The main effect of the architecture type on the safety analysis is the failure tree structure, which changes with each type. This change in failure tree structure results in a numerical difference in the top-level failure rate in the bottom-up approach and a difference in failure rates allocated to basic events in the top-down approach.

Sub-question 4.1: How does the parallel architecture type affect the safety analysis?

For the double-shaft parallel sub-type all the failure rate targets for the selected failure conditions can be achieved. Since this is the same architecture as the reference case, logically, it achieves these targets, as the reference case was designed to achieve them. It also allows an FDAL C for the Electrical Propulsion System (EPS), lowering development requirements for the electrical motor and battery system. The results are similar for the single-shaft sub-type, which also achieves all the failure rate targets for the selected failure conditions and also allows an FDAL C for the EPS.

Sub-question 4.2: How does the series-parallel architecture type affect the safety analysis?

For the series-parallel architecture type most of the failure rate targets for the selected failure conditions can be achieved with one notable exception. It does not achieve the failure rate target for FC3:"Partial Loss of Mechanical Power". This is caused by the failure of a generator, which would directly lead to a partial loss of mechanical power. Since the failure rate for the generator is 2E-4, this has a large influence on the top-level failure rate. Similarly to the parallel architecture type, the architecture allows the EPS to have an FDAL C.

Sub-question 4.3: How does the series architecture type affect the safety analysis?

Of all the architecture types, the series architecture type shows the highest failure rates. For the series architecture type concept with 2 DUs and 2 EES, it is only able to achieve the target failure rate for FC.1"Loss of Alert Data Transmission". This indicates that it would be difficult to implement the series architecture type in a manner that would satisfy the safety requirements. The effect on the FDALs is that both the Gas Turbine Engine (GTE) and the EPS are required to have FDAL A. Thus, imposing strict development requirements on the electrical motor and battery system.

Research question 5: How does the number of engines affect the safety analyses?

The results clearly show the effect of the number of engines on the safety assessment in multiple ways. Naturally, it changes the structure of the failure tree. Numerically, this changes the failure rates of the top-level failure condition. Generally, the concepts with only one Drive Unit (DU) and Electrical Energy Storage (EES) have higher failure rates than concepts with 2 DUs and 2 EES. They often cannot achieve the failure rate targets set for the selected failure conditions.

7.2. Limitations

Every research has its limitations, and so do the analyses described in this thesis report. The main type of analysis conducted in this study is the Failure Tree Analysis (FTA). Its main feature, the failure tree, should accurately describe the progression of failures from the item level to the aircraft level. This is where the first limitation arises, during this research only the propulsion system was taken into account, leaving out most aircraft systems. This disregards potential failures originating in other systems but which also affect the propulsion system. The second limitation regarding failure tree structure is the level of detail. The most important subsystems and item failures were taken into account, however, some failures could be described in more detail for the baseline case. For example, instead of having the basic event be "cooling system failure", the cooling system could be taken as a subsystem and dissected further into basic events such as "cooling fluid duct rupture". This would significantly increase the complexity of the failure tree, risking a loss of overview, but it would create a more accurate failure progression.

Next to the structure, there is also a limitation to the failure rate data used. Most of the failure rate data was taken from the NPRD database. This empirical data is linked to specific equipment, which was not always intended for aerospace applications. Even though conversion factors were applied to account for this, without empirical data for the equipment in an aerospace application it is uncertain what its exact failure rate in an aerospace application would be. The failure rates were standardized per item failure, ensuring the same item had the same failure rate, independent of the system or concept. As some of the failure rates were not represented in the NPRD database, the failure rates then originated from internal data on similar failures. In conclusion, no new failure rate data was generated for the FTAs, for the most accurate outcome, prototypes should be created for every concept and tested to generate accurate failure rate data.

The comparison analysis is not free of limitations either. Each subsystem was standardized to allow a relatively easy comparison of the different HEPS architecture types. The downside of standardizing these subsystems is a loss of detail. Even though each concept was checked for technical feasibility, the different integration required in each concept may lead to different items required to make the concept possible. These item-level requirements are not represented in the concept comparison.

The weight analysis is the most limited analysis in this study. It is referred to as a "low-fidelity" analysis due to the limited data used as input. First, it also falls prey to the same standardization disadvantage. Each subsystem and item taken into account in the weight estimation is standardized. For example, the Main Gearbox (MGB) has to be adjusted to the input it receives, a GTE delivers a different rotating speed than an E-Motor (EM), prompting a change to be required if an EM delivers a direct input to the MGB, which in turn would change the weight of the MGB. The subsystems are sized for maximum continuous power. Yet the estimations on the relation between maximum continuous power and the power density are often based on only a couple of data points, thus having a low accuracy. Another limitation is the assumption of similar technology. Each subsystem is assumed to have the same technology in every concept, e.g. the Drive Unit (DU) in concept C1 is the same type of DU in concept C9 even when the power sizing might be different. Different manufacturers create different EMs leading to different power densities, this difference could lead to a difference in system weight.

Lastly, it is important to understand that this study is not aimed at comparing conventional propulsion systems to HEPS, but at comparing the different architecture options for HEPS, specifically for the safety analyses. As such, the data for the conventional concept is just there to give an idea of how HEPS would compare to the current conventional propulsion systems.

8

Conclusions and Recommendations

8.1. Conclusions

The study aims to answer its main research question:

How is the risk analysis for helicopters affected by hybrid-electric engine architecture?

The choice of hybrid-electric engine architecture mainly affects the Failure Tree Analysis (FTA) in the risk analysis. The choice directly affects the structure of the failure trees for the FTA. This leads to a difference both numerically and qualitatively. Numerically, specific architectures can lead to a requirement for additional redundancy to achieve the top-level failure rate targets. Qualitatively, specific architectures lead to a higher Function Development Assurance Level (FDAL) for the Electric Propulsion Unit (EPU), and thus to a more extensive system development process due to safety requirements, causing longer development times and higher development costs.

Looking more in detail, several conclusions can be drawn about each of the architecture types:

- **Double-shaft parallel**: this architecture has the lowest FC failure rates in this study. Also, this architecture allows for independent sizing of the Gas Turbine Engine (GTE) and EPU leading to a relatively low weight. Finally, the architecture is relatively simple in terms of integration.
- **Single-shaft parallel**: similar performance in terms of failure rate to the double-shaft parallel concept. The weight estimation is also similar. The major difference is the complexity since having the GTE and EPU share a driveshaft requires more complex technology for integration. Another difference is that the drive shaft becomes a critical component, if it fails, all mechanical power is lost.
- **Series-parallel**: in terms of failure rates, this architecture type boasts higher failure rates than the parallel concepts, but still manages to achieve most failure rate targets. The introduction of separate generators does lead to a 14% weight increase compared to the baseline. This architecture is technically more complex as the generator has interfaces with the Main Gearbox (MGB) and Electric Energy System (EES).
- **Series**: this architecture has the highest failure rates of all concepts and requires a lot of redundancy to achieve the failure rate targets, as shown by concept C6A. Additionally, the architecture forces the EPU to have FDAL A compared to FDAL C in the other architecture types. In terms of weight, it causes a weight increase of more than 60 % compared to the baseline. This is due to both the GTE and EPU being sized for maximum continuous power output instead of distributing the power required.

From the results, it is clear that redundancy plays a major factor, especially for the EPU. For every architecture type, the version with 1 Drive Unit (DU) and 1 EES has higher failure rates compared to the version with 2 DUs and 2 EES. This redundancy will however lead to a higher system weight. Additionally, having multiple DUs requires introducing an RGB into the system to combine the power

and rpm from the DUs and transfer it to the MGB, whereas, with a single DU, the output can directly be transferred to the MGB.

A concept where the tail rotor is connected to the EPU instead of the MGB (concept C8) shows that the main problem with an electrified tail rotor is the failure rate that can be achieved. It shows no advantage compared to coupling the tail rotor to the MGB. Similarly, an uncoupled HEPS also provides no advantages. It leads to significant problems with failure rate targets and a massive increase in weight. Both these concepts also require the EPU to have FDAL A, leading to increased development time and costs.

8.2. Recommendations

Several adaptations could be performed to extend the scope of the study. First, the amount of failure conditions could be expanded to generate a complete overview of all the failure conditions affected by the differences in HEPS architecture. Secondly, as mentioned previously, the level of detail could be increased by further dissecting the "building blocks" used in the comparison analysis.

Another option would be to dive into the different technologies present for each subsystem. As there is a lot of diversity in DU and EES manufacturers, not every DU or EES might be usable for each concept as the different concepts require different integration into the HEPS.

Scope extension could also be done by adding additional analyses to the safety analysis. In this study, all of the spatial safety assessments such as the Particular Risk Analysis (PRA) and Zonal Safety Analysis (ZSA) were excluded. However, HEPS architecture might have a significant impact on these assessments. Thus, it would be beneficial to perform both a PRA and ZSA for each concept and compare them to see the impact of the different architectures.

As this study has shown, system weight will be heavily impacted by the choice of HEPS architecture. To get a detailed picture, it is recommended that a full study into system weight is performed. Being able to combine the pre-existing performance studies and this study on safety with a full study of system weight would allow for a significant overview of the impact of architectural choices in the early stages of rotorcraft development.

Bibliography

[1] T. Donateo, A. Carlà, and G. Avanzini. “Fuel consumption of rotorcrafts and potentiality for hybrid electric power systems”. In: *Energy Conversion and Management* (2018).

[2] Y. Xie et al. “Review of hybrid electric powered aircraft, its conceptual design and energy management methodologies”. In: *Chinese Journal of Aeronautics* (2021).

[3] *International Helicopter Safety Symposium*. Elsevier, 2005.

[4] EASA. *EASA CS27 Amdt. 10 "Certification Specification for Small Rotorcraft"*. Tech. rep. EASA, 2003.

[5] EASA. *EASA CS29 Amdt. 11 "Certification Specification for Large Rotorcraft"*. Tech. rep. EASA, 2003.

[6] EASA. *Certification Specifications for Helicopter Flight Simulation Training Devices*. Tech. rep. EASA, 2012.

[7] EASA. *Special Condition Electric Hybrid Propulsion System (EHPS)*. Tech. rep. EASA, 2021.

[8] A.A. Franco. *Rechargeable Lithium Batteries*. 1st ed. Elsevier, 2015, pp. 369–383.

[9] A. Arora et al. *Electric and Hybrid Vehicles*. 1st ed. Elsevier, 2010, pp. 463–491.

[10] Apr. 2024. URL: https://en.wikipedia.org/wiki/Honda_Insight.

[11] X. Li et al. “A Comparison of SAE ARP 4754A and ARP 4754”. In: *Procedia Engineering* (2011).

[12] *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*. Standard. Warrendale, Pennsylvania, USA: The Engineering Society For Advancing Mobility Land Sea Air and Space, 1996.

[13] P. Wang. *Civil Aircraft Electrical Power System Safety Assessment*. 1st ed. Elsevier, 2017.

[14] *Guidelines for Development of Civil Aircraft and Systems*. Standard. Warrendale, Pennsylvania, USA: The Engineering Society For Advancing Mobility Land Sea Air and Space, 2010.

[15] F. Bardé J. Jaguemont. “A critical review of lithium-ion battery safety testing and standards”. In: *Applied Thermal Engineering* (2023).

[16] D. Li et al. “Battery safety issue detection in real-world electric vehicles by integrated modeling and voltage abnormality”. In: *Energy* (2023).

[17] Y. Yang et al. “Towards a safer lithium-ion batteries: A critical review on cause, characteristics, warning and disposal strategy for thermal runaway”. In: *Advances in Applied Energy* (2023).

[18] Y. Yang and I. Jung. “Boolean Algebra Application in Simplifying Fault Tree Analysis”. In: *International Journal of Safety Science* (2017).

[19] *Military Handbook: Electronic Reliability Design Handbook*. Standard. Washington D.C., USA: US Department of Defense, 1998.

[20] *Military Handbook: Reliability Prediction of Electronic Equipment*. Standard. Washington D.C., USA: US Department of Defense, 1991.

A

FHA

Function	Reference	Sub-reference	Functional failure reference	Functional Failure / Scenario / Specific Risk	Effect on other subsystems and on H/C (worst case)	FF severity	FF FR objective	FC ref	Failure Condition	FC severity	FC objective
Emergency engine shut-off	F6	F6.1	FF.054	Loss of GTE shutdown control in combination with shutdown request due to engine fire	Fire in GTE bay	CAT	1.00E-10	FC.EHPS.007	Uncontained fire	CAT	1.00E-09
	F6	F6.1	FF.055	Loss of GTE shutdown control	Possible safety hazard	MAJ	1.00E-06	FC.EHPS.009	Degraded flight safety	MAJ	1.00E-05
	F6	F6.1	FF.056	Loss of GTE shutdown control in combination with shutdown request due to overtorque	High energy debris from GTE	CAT	1.00E-10	FC.EHPS.008	High energy debris	CAT	1.00E-09
	F6	F6.2	FF.057	Loss of EPS shutdown control in combination with shutdown request due to engine fire	Fire in EPS bay	CAT	1.00E-10	FC.EHPS.007	Uncontained fire	CAT	1.00E-09
	F6	F6.2	FF.058	Loss of EPS shutdown control	Possible safety hazard in combination with aggrevating events	MAJ	1.00E-06	FC.EHPS.009	Degraded flight safety	MAJ	1.00E-05
	F6	F6.2	FF.059	Loss of EPS shutdown control in combination with shutdown request due to overtorque	High energy debris from EPS	CAT	1.00E-10	FC.EHPS.008	High energy debris	CAT	1.00E-09
Specific Risks			SR.1	Thermal runaway	Loss of EPS	MAJ	1.00E-06	FC.EHPS.011	Contained thermal runaway	MAJ	1.00E-05
			SR.2	High energy debris	Loss of critical parts	CAT	Qualitative	FC.EHPS.008	High energy debris	CAT	1.00E-09
			SR.3	Uncontrolled fire	Loss of H/C	CAT	1.00E-10	FC.EHPS.007	Uncontained fire	CAT	1.00E-09
			SR.4	Fuel leakage	Fire hazard, possible lower GTE output	HAZ	1.00E-08	FC.EHPS.007	Uncontained fire	CAT	1.00E-09
			SR.5	Flailing shaft	Loss of critical parts	CAT	Qualitative	FC.EHPS.010	Compromised flight safety	HAZ	1.00E-07
			SR.6	Leaking battery acid	Highly corrosive, loss of critical parts, damage to structural parts	CAT	Qualitative	FC.EHPS.010	Compromised flight safety	HAZ	1.00E-07
			SR.7	Cooling fluid leakage	Fire hazard, possible EPS shutdown	HAZ	1.00E-08	FC.EHPS.007	Uncontained fire	CAT	1.00E-09

Figure A.1: FHA worksheet extract

B

HEPS PSSA

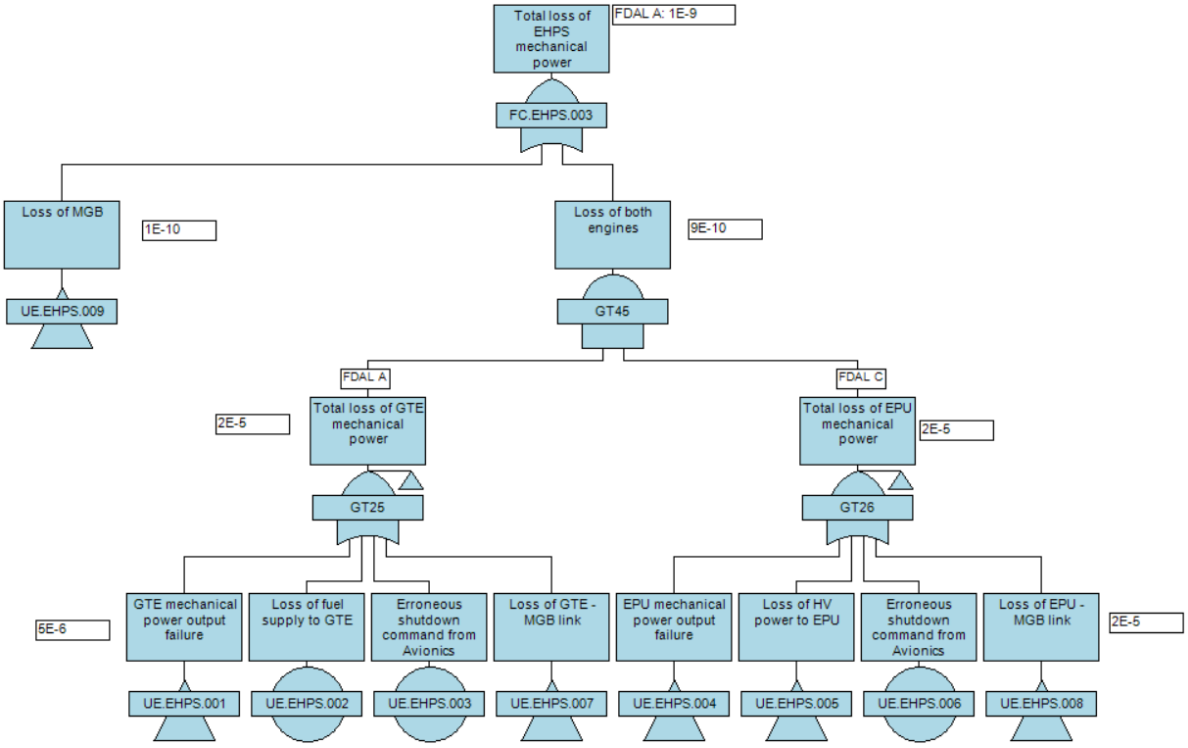


Figure B.1: PSSA FTA FC.EHPS.003

C

CMA

Common Cause Sub-Type	Could independence be affected by a common failure of:	Failure Mode or Error Source Examples
Common Resource - LV Electrical Power		
LV electrical power generation	LV power source / supply malfunction?	- Failure due to loss of single electrical power source / supply - Failure due to common response to over/under voltage output
LV electrical power distribution	Common functions used in LV power distribution system? Common equipment used in power distribution system?	- Loss of electrical power due to malfunctions of switches, relays, circuit breakers
	LV power distribution cabling?	- Failure due to loss of single power source / supply cabling
Common Resource - HV Electrical Power		
HV electrical power generation	HV power source / supply malfunction?	- Failure due to loss of single electrical power source / supply - Failure due to common response to over/under voltage output
HV electrical power distribution	Common functions used in HV power distribution system? Common equipment used in power distribution system?	- Loss of electrical power due to malfunctions of switches, relays, circuit breakers
	HV power distribution cabling?	- Failure due to loss of single power source / supply cabling
Common Resource - Data		
Networks	Receipt or transmission of data on common network?	- Inadequate network infrastructure, protocols - Inadequacy of network protections - Lack of separation of networks by criticality of data
Interfaces (e.g., connectors, routes)	Separation / segregation of signals between interfaces?	- Lack of signal separation between interfaces results in common failure - Inadequate separation maintained through signal path (e.g., cables, flex cable, motherboards) results in failure - Lack of signal separation of two independent functions through same interface supporting the same failure condition (e.g., loss of signal resulting in loss of brake function and loss of signal causing loss of ground spoiler where both used for stop on the runway failure condition)
Processing	Common processing elements?	- Failure of common receive / transmit devices - Failure of common computing devices
Data	Incorrect or corrupted data?	- Missing data- Erroneous data- Incorrect upload/download of data
Sensors	Functions sharing common sensors or common sources?	- Failure of common sensor used for control path and a monitor path that are intended to be independent - Failure of Common sensor used to provide data to multiple functions (systems)
Common Resource - Cooling Fluids		
Water-glycol	No water glycol cooling fluid refreshing	- Lack of separation between cooling paths of different cooling functions
Common Resource - Lubrication / Cooling Oil		
Lubricating oil	No lubrication oil refreshing	- Lack of separation between lubrication oil paths of different lubrication functions
Cooling oil	No cooling oil refreshing	- Lack of separation between cooling oil paths of different cooling functions

Table C.1: CMA Questionnaire

D

Concepts

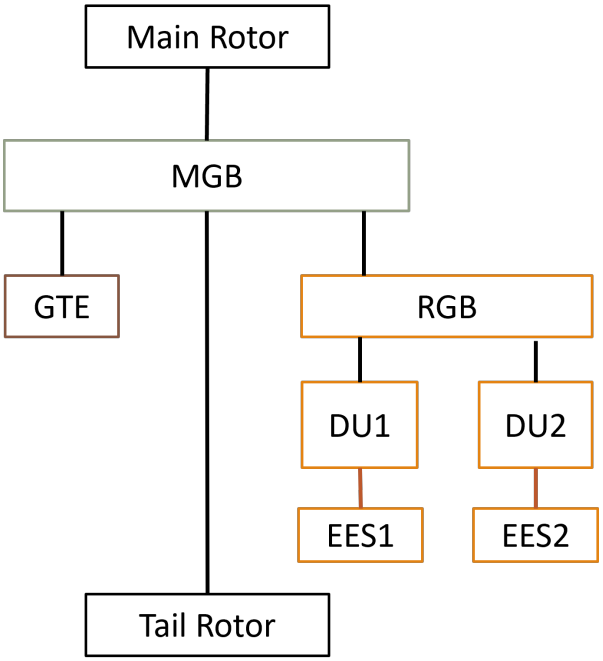


Figure D.1: Concept C1

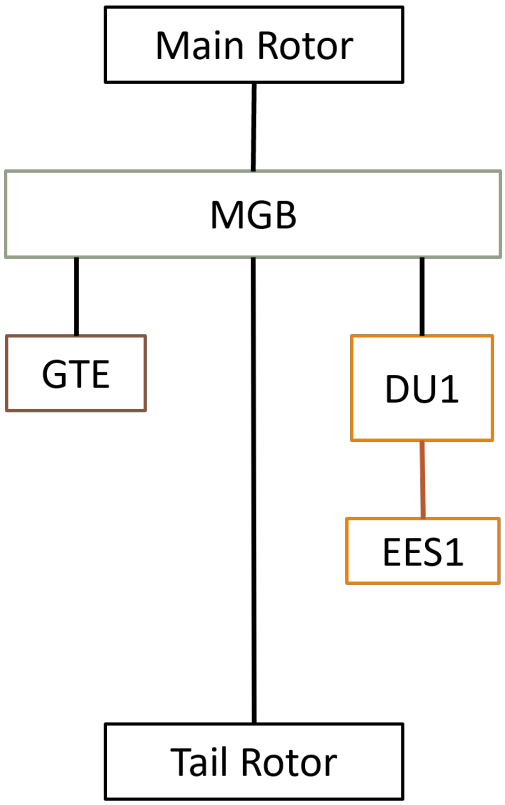


Figure D.2: Concept C2

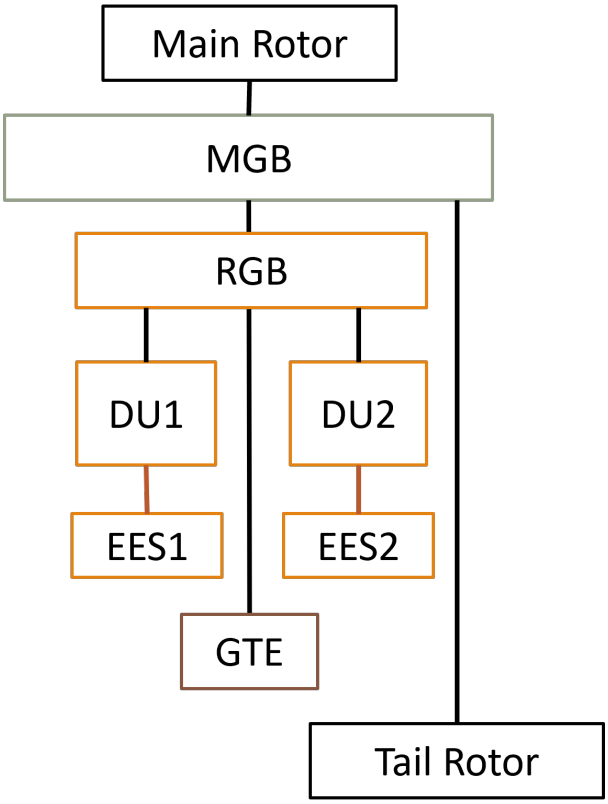


Figure D.3: Concept C3

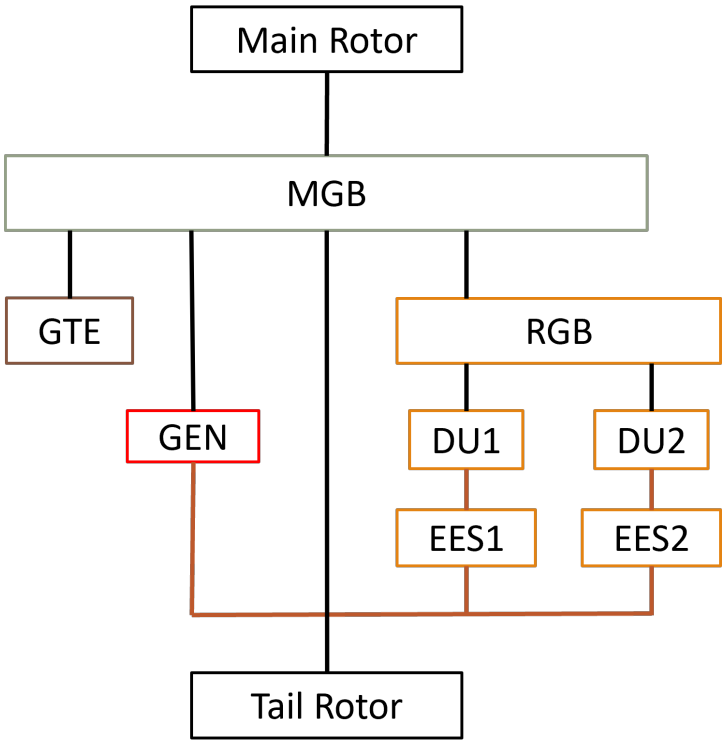


Figure D.4: Concept C4

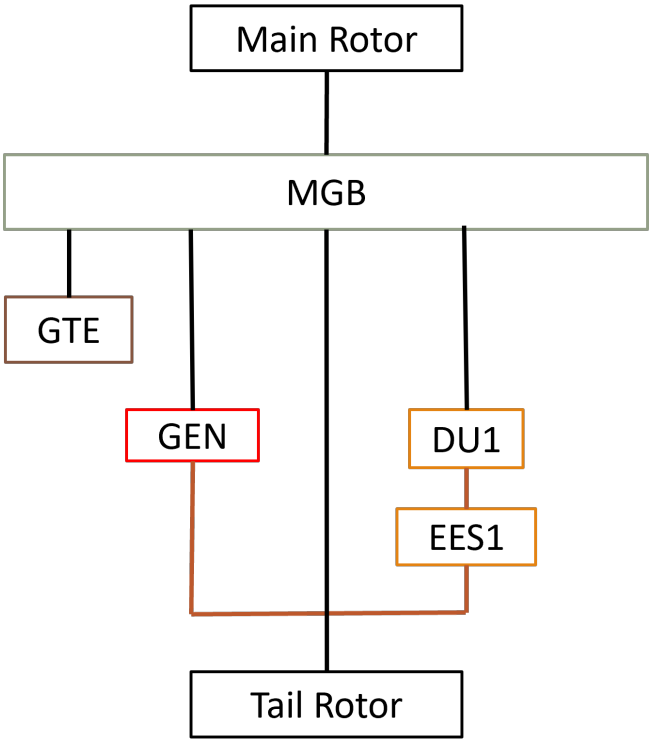


Figure D.5: Concept C5

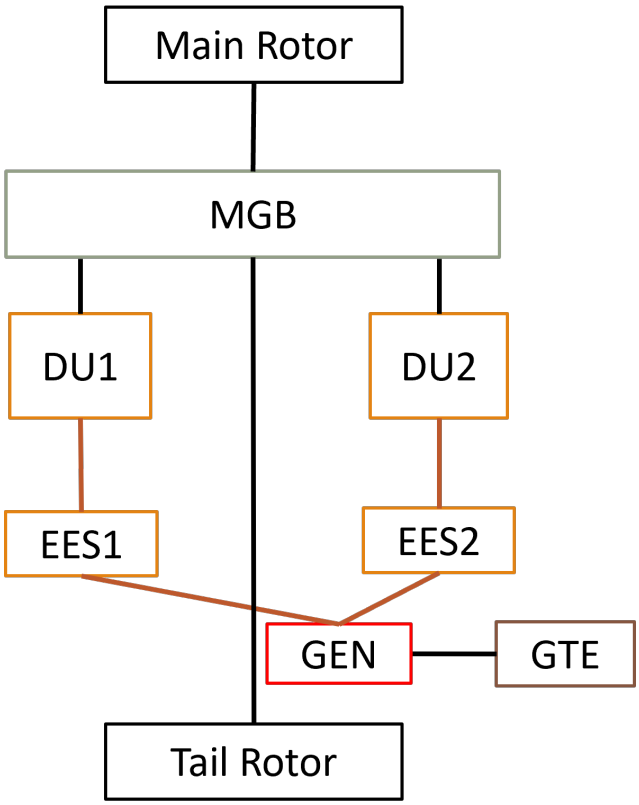


Figure D.6: Concept C6

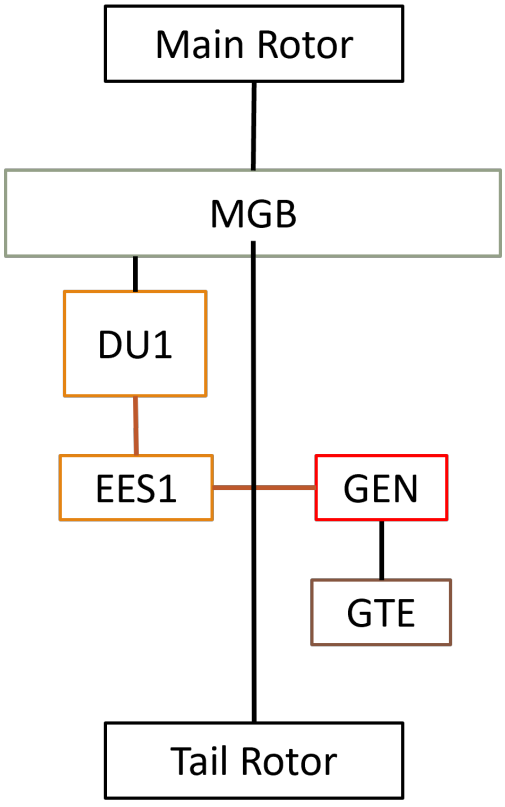


Figure D.7: Concept C7

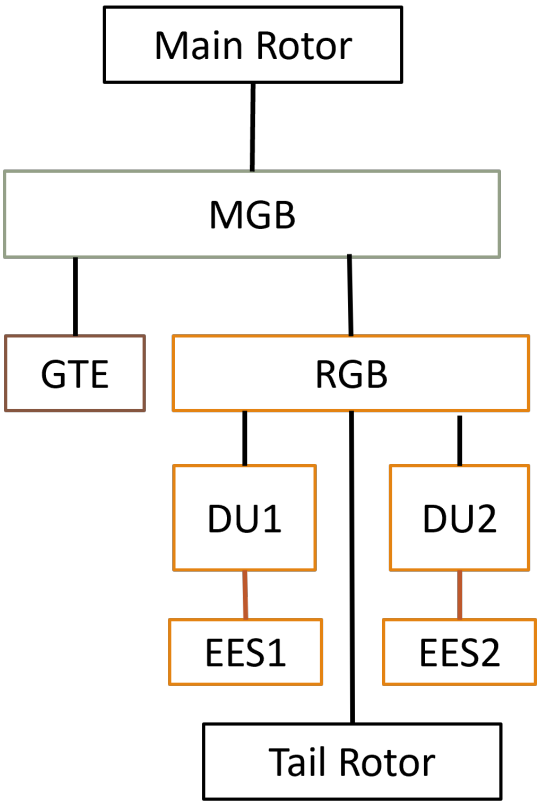


Figure D.8: Concept C8

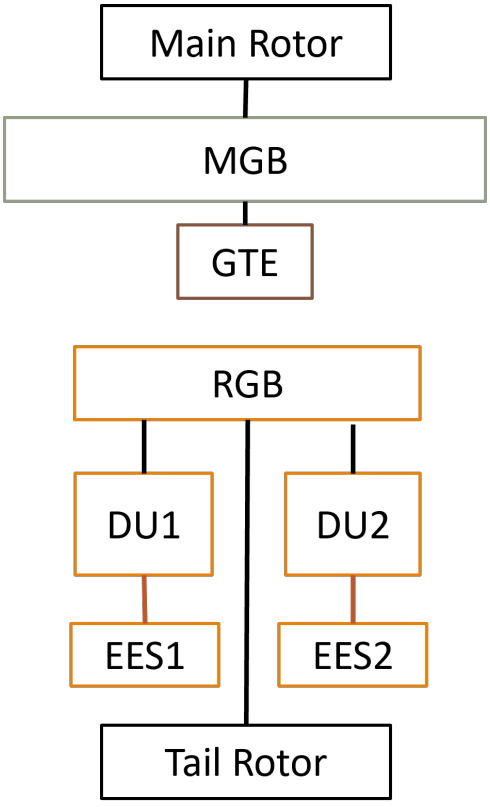


Figure D.9: Concept C9

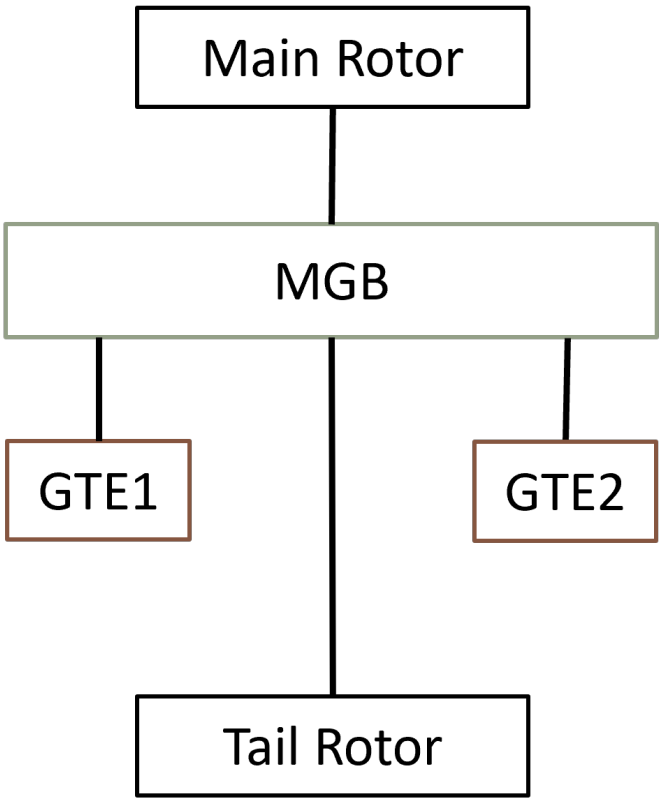


Figure D.10: Concept CONV

E

Conceptual Comparison

E.1. Failure Condition 2 per Concept

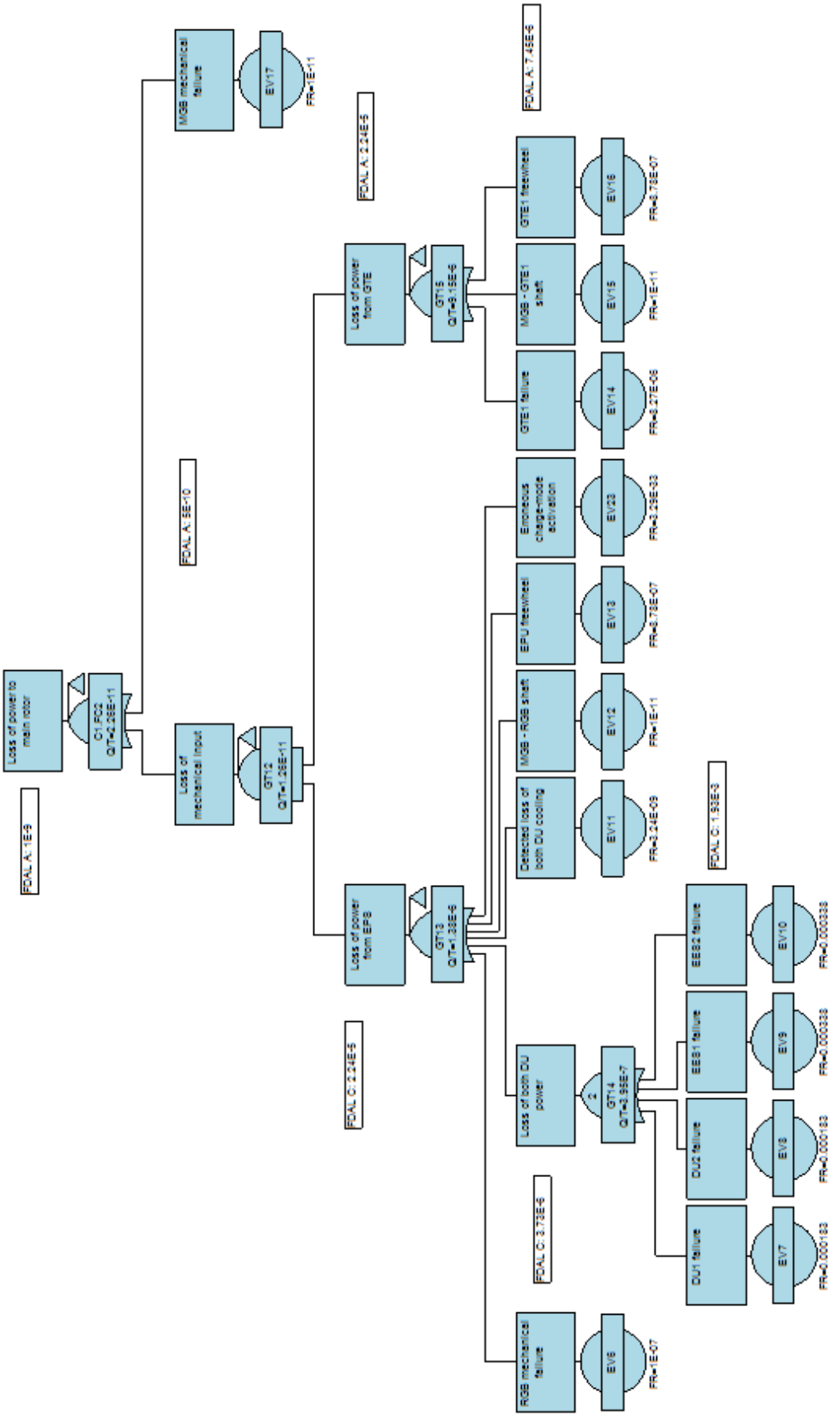


Figure E.1: C1 FC2

E.2. Top-down FTA

Number	EV1	EV2	EV3	EV4	EV5	EV6	EV7	EV8	EV9	EV10	EV11
C1	2.50E-06	1.58E-03	1.58E-03	2.50E-06	2.50E-06	2.64E-06	1.62E-03	1.62E-03	1.62E-03	1.62E-03	2.64E-06
C2	2.50E-06	2.50E-06	n.a	2.50E-06	2.50E-06		1.95E-06		1.95E-06		
C3	2.50E-06	1.58E-03	1.58E-03	2.50E-06	2.50E-06		1.99E-03	1.99E-03	1.99E-03	1.99E-03	3.95E-06
C4	2.00E-06	1.41E-03	1.41E-03	2.00E-06	2.00E-06	2.22E-07	4.71E-04	4.71E-04	4.71E-04	4.71E-04	2.22E-07
C4A	2.00E-06	1.41E-03	1.41E-03	2.00E-06	2.00E-06	5.00E-07	7.00E-04	7.00E-04	7.00E-04	7.00E-04	5.00E-07
C5	2.00E-06	2.00E-06	n.a	2.00E-06	2.00E-06	3.33E-07	1.67E-07		1.67E-07		
C6	2.00E-06	1.41E-03	1.41E-03	2.00E-06	2.00E-06		4.56E-06	4.56E-06	4.56E-06	4.56E-06	2.08E-11
C6A	2.00E-06	1.26E-02	1.26E-02	2.00E-06	1.26E-02		1.38E-04	1.38E-04	1.38E-04	1.38E-04	
C7	2.00E-06	2.00E-06	n.a	2.00E-06	2.00E-06		1.04E-11		1.04E-11		
C8	2.50E-06	1.58E-03	1.58E-03	2.50E-06	2.50E-05	8.33E-11	9.12E-06	9.12E-06	9.12E-06	9.12E-06	8.33E-11
C9	2.50E-06	1.58E-03	1.58E-03	2.50E-06	2.50E-06		1.58E-05	1.58E-05	1.58E-05	1.58E-05	2.50E-10
CONV				3.33E-06	3.33E-06						

Table E.1: Top-down allocation full results part 1

Number	EV12	EV13	EV14	EV15	EV16	EV17	EV18	EV19	EV20	EV21	EV22
C1	2.64E-06	2.64E-06	5.27E-06	5.27E-06	5.27E-06	2.50E-10	2.50E-10	2.50E-10	3.16E-04	1.78E-02	1.78E-02
C2		3.95E-06	5.27E-06	5.27E-06	5.27E-06	2.50E-10	2.50E-10	2.50E-10	3.16E-04	3.16E-04	
C3		3.95E-06	7.90E-06	2.50E-10	7.90E-06		2.50E-10	2.50E-10	3.16E-04	1.78E-02	1.78E-02
C4	2.22E-07	2.22E-07	3.70E-07	3.70E-07	3.70E-07	2.50E-10	2.50E-10	2.50E-10	3.16E-04	1.26E-02	1.26E-02
C4A	5.00E-07	5.00E-07	5.27E-06	5.27E-06	5.27E-06	2.50E-10	2.50E-10	2.50E-10	3.16E-04	1.26E-02	1.26E-02
C5	3.33E-07	3.33E-07	5.55E-07	5.55E-07	5.55E-07	2.50E-10	2.50E-10	2.50E-10	1.58E-04	1.58E-04	
C6			4.17E-11			2.50E-10	2.50E-10	2.50E-10	4.64E-03	6.81E-02	6.81E-02
C6A			2.17E-04			2.50E-10	2.50E-10	2.50E-10	3.22E-03	3.22E-03	3.22E-03
C7			4.17E-11			2.50E-10	2.50E-10	2.50E-10	3.33E-08	3.33E-08	
C8	8.33E-11	1.00E-06	1.57E-06	1.57E-06	1.57E-06	5.00E-10	3.33E-10		3.16E-04	1.78E-02	1.78E-02
C9			1.67E-10	1.67E-10	1.67E-10	5.00E-10	5.00E-10		3.16E-04	1.78E-02	1.78E-02
CONV			1.67E-06	1.67E-06	1.67E-06	2.50E-10	2.50E-10	2.50E-10	3.16E-04		

Table E.2: Top-down allocation full results part 2

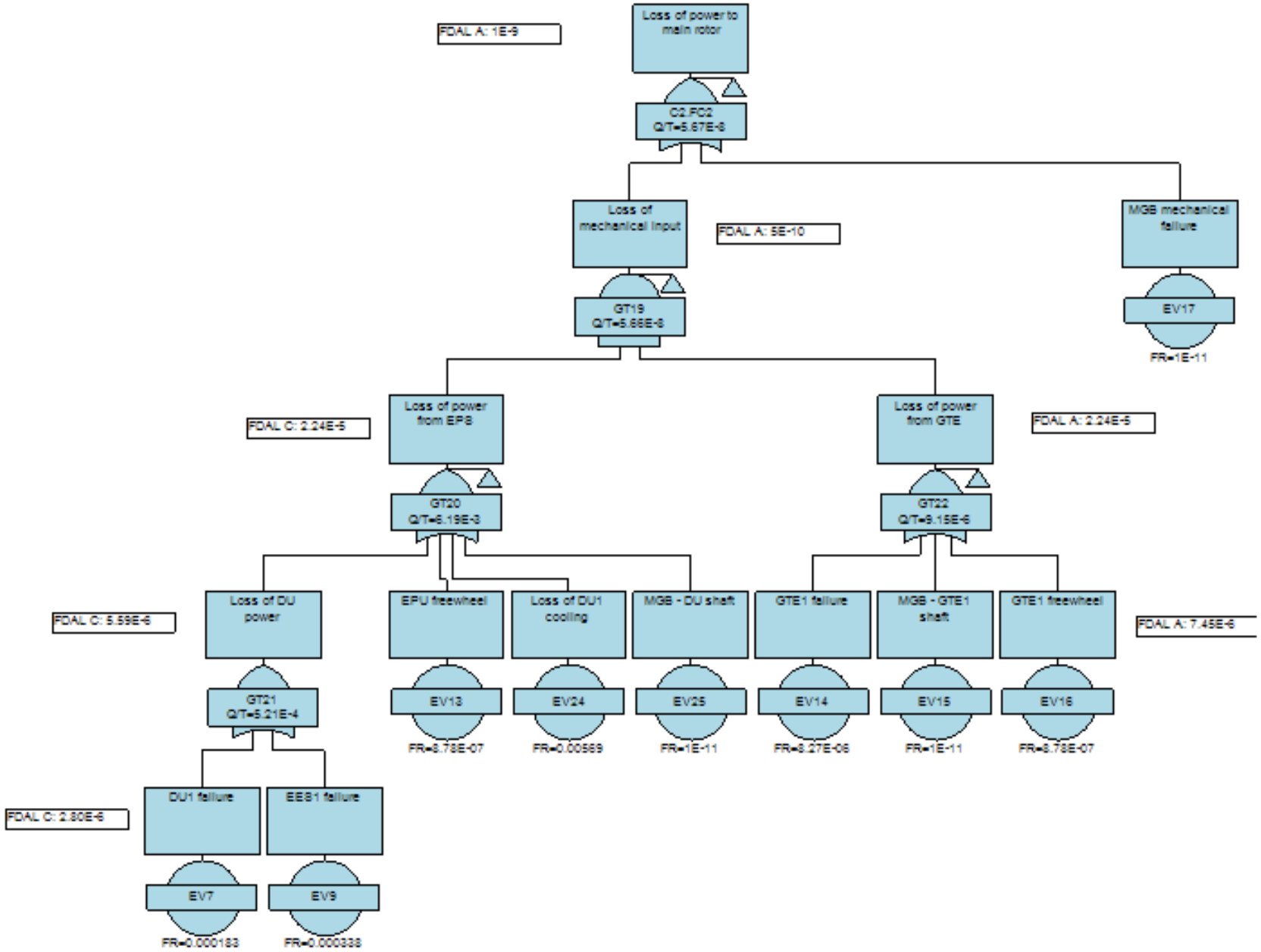


Figure E.2: C2 FC2

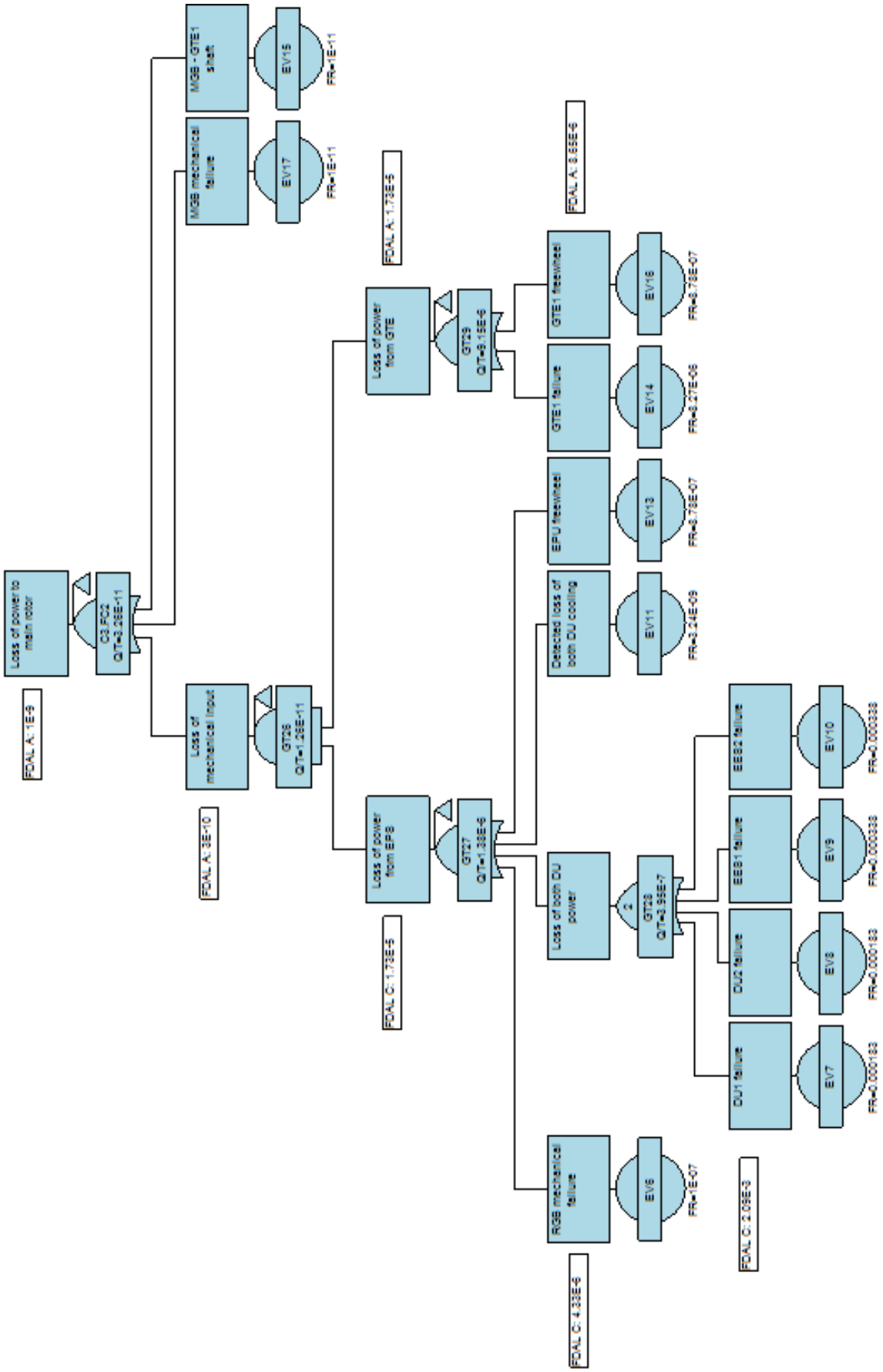


Figure E.3: C3 FC2

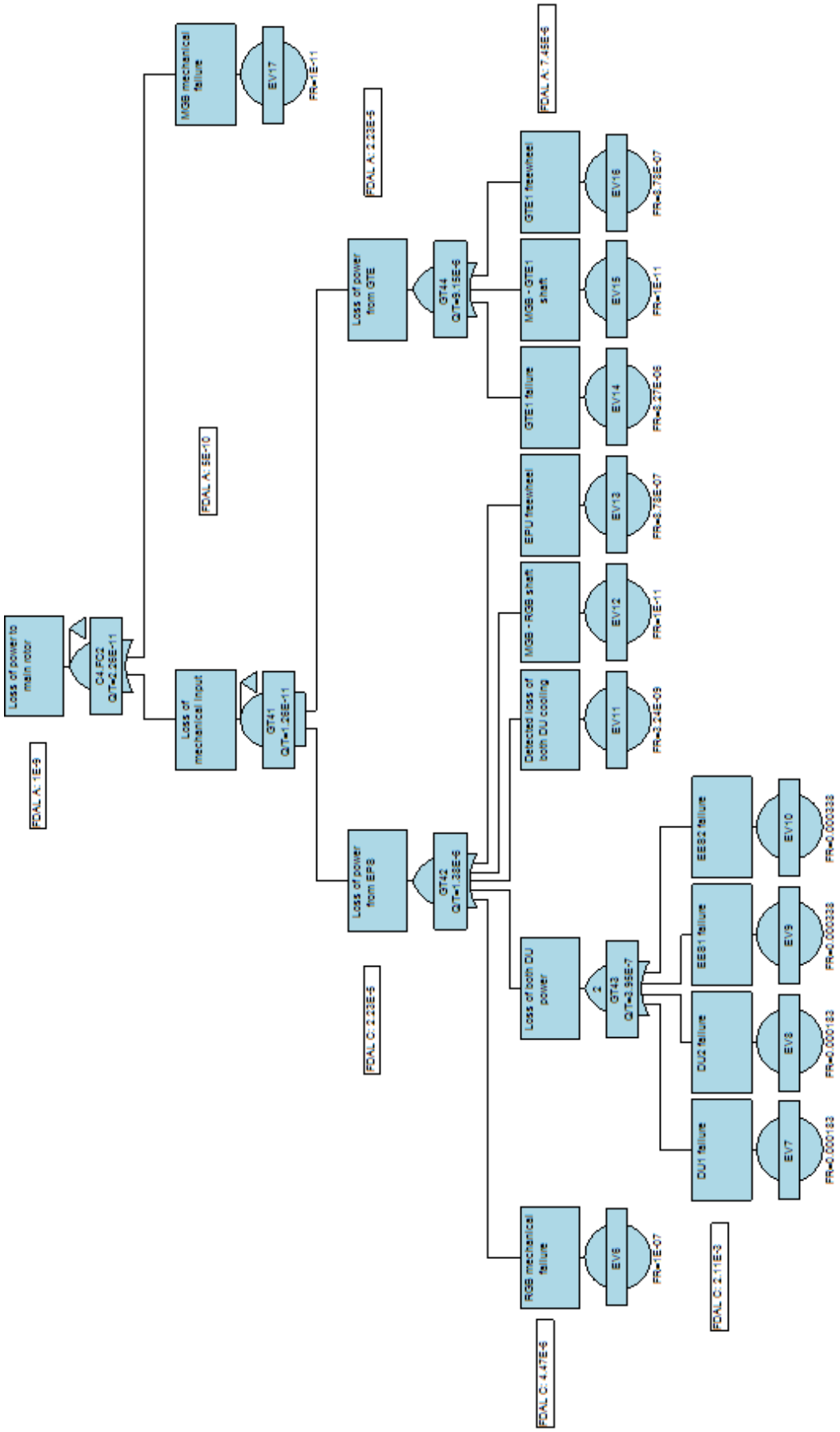


Figure E.4: C4 FC2

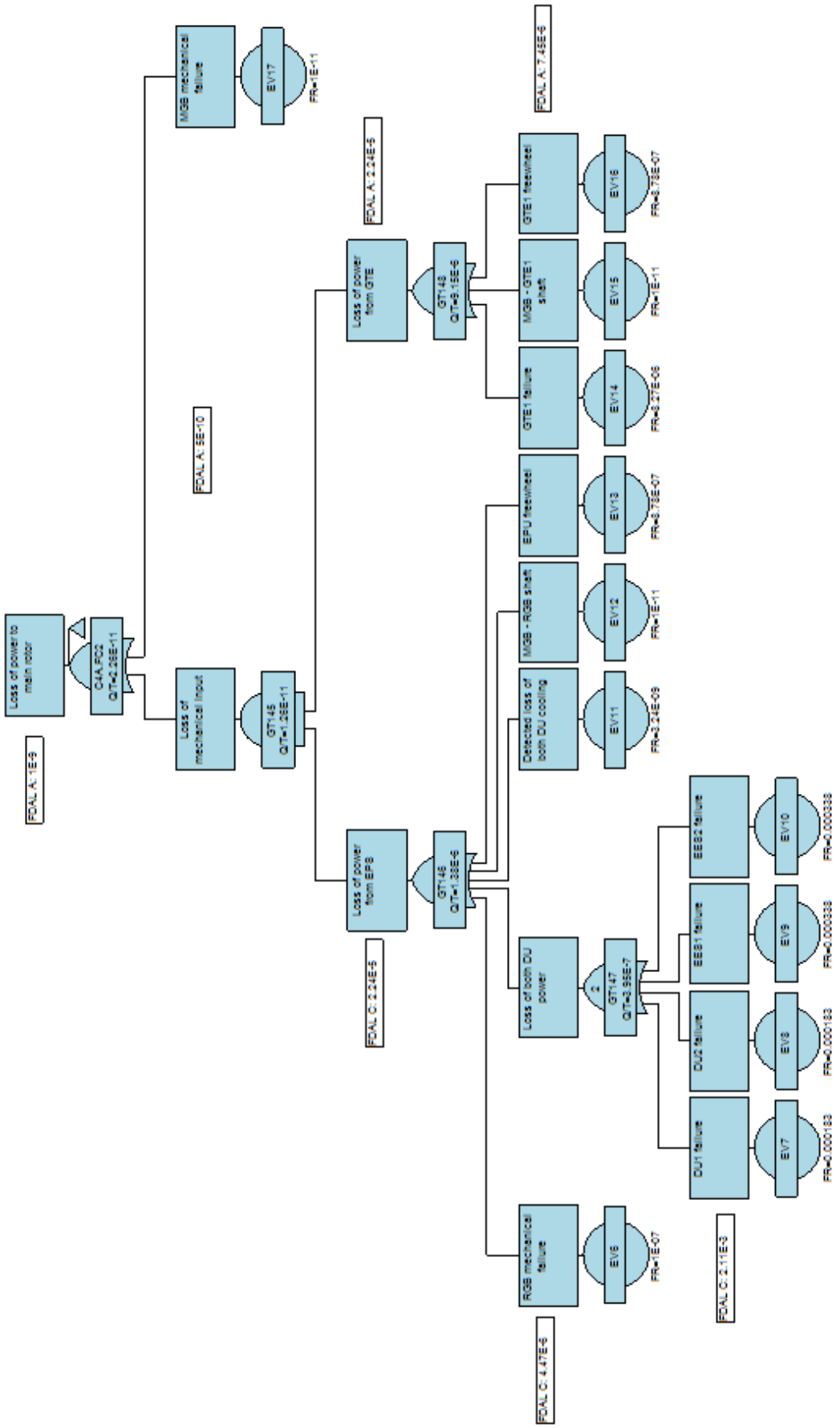


Figure E.5: C4A FC2

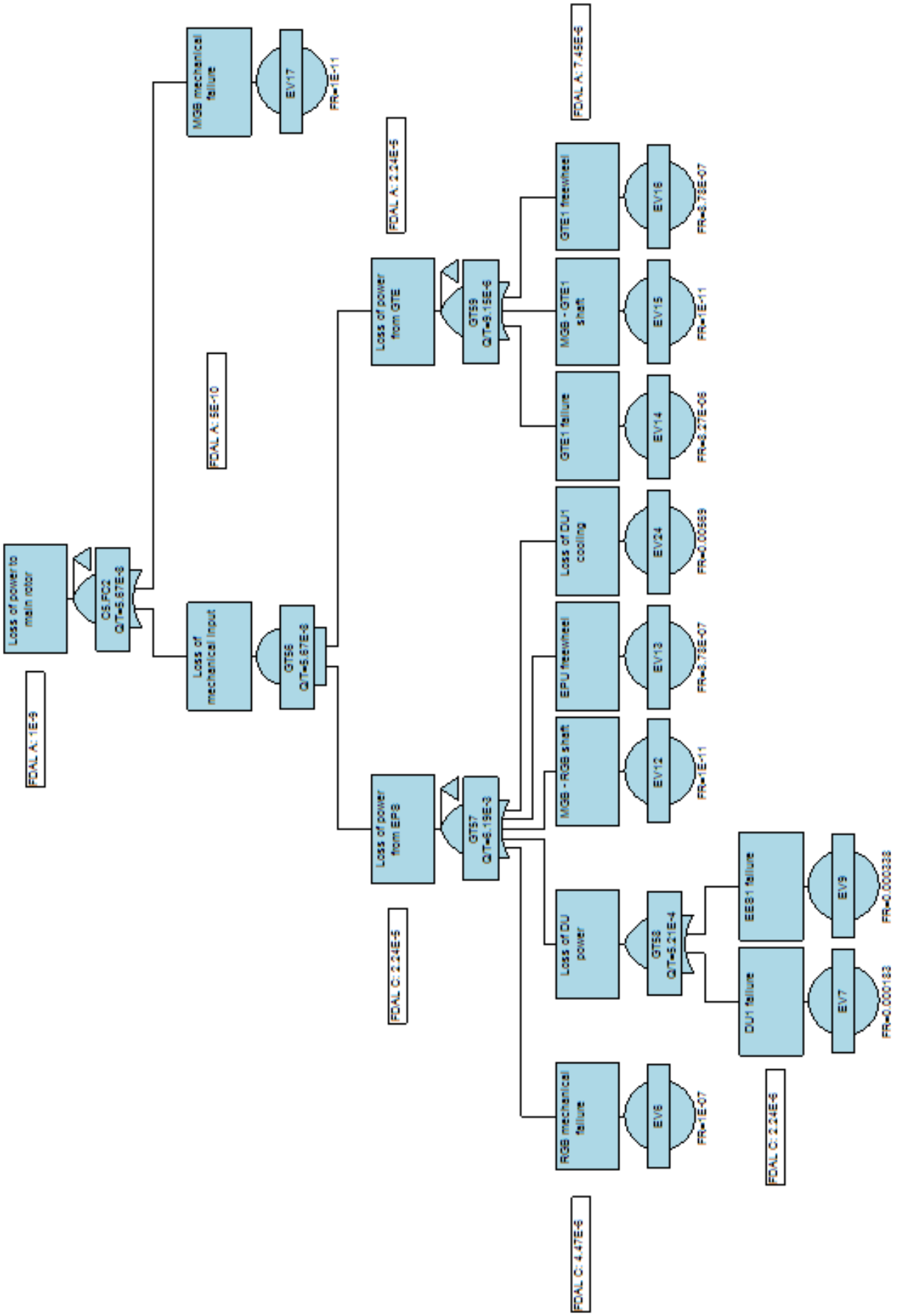


Figure E.6: C5 FC2

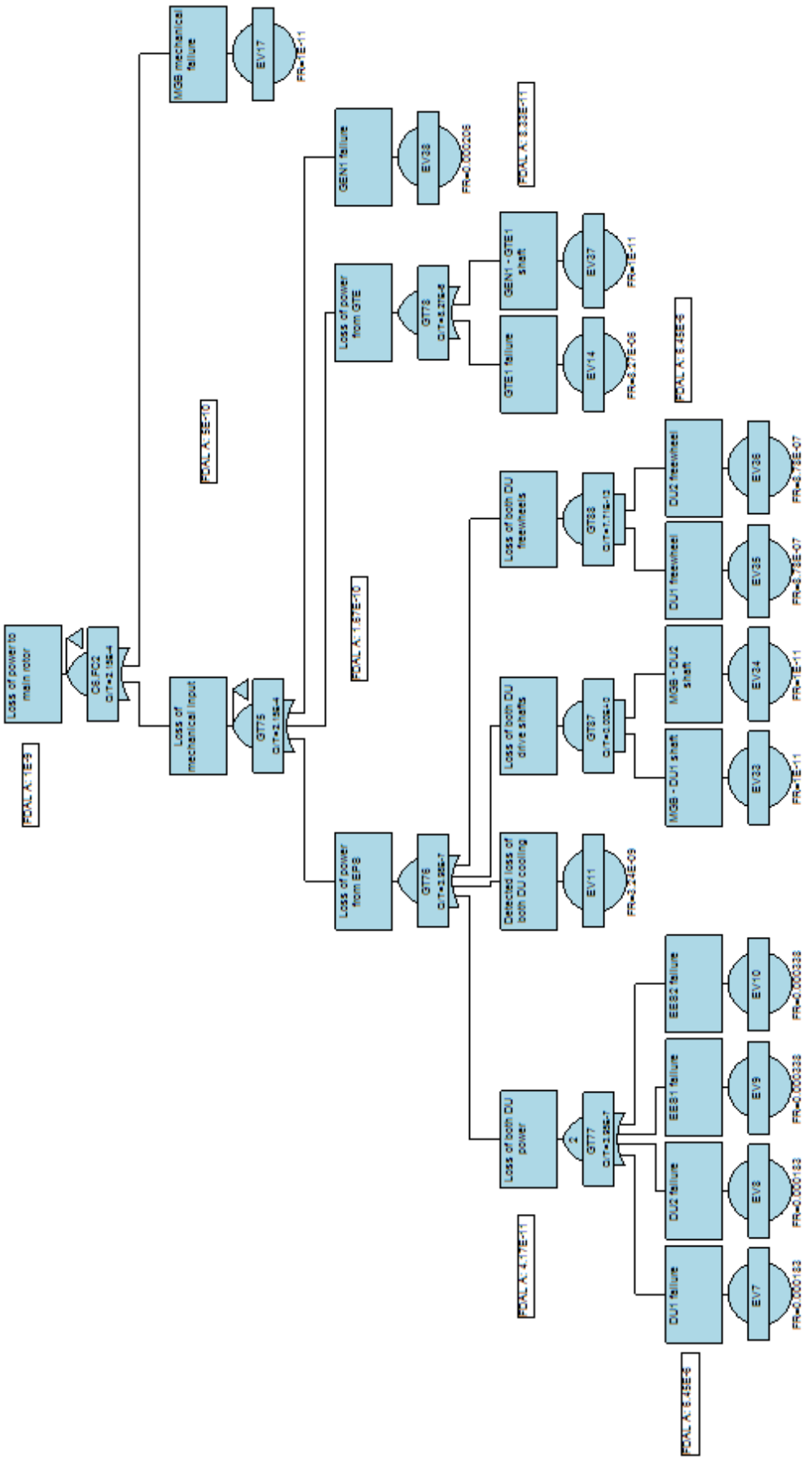


Figure E.7: C6 FC2

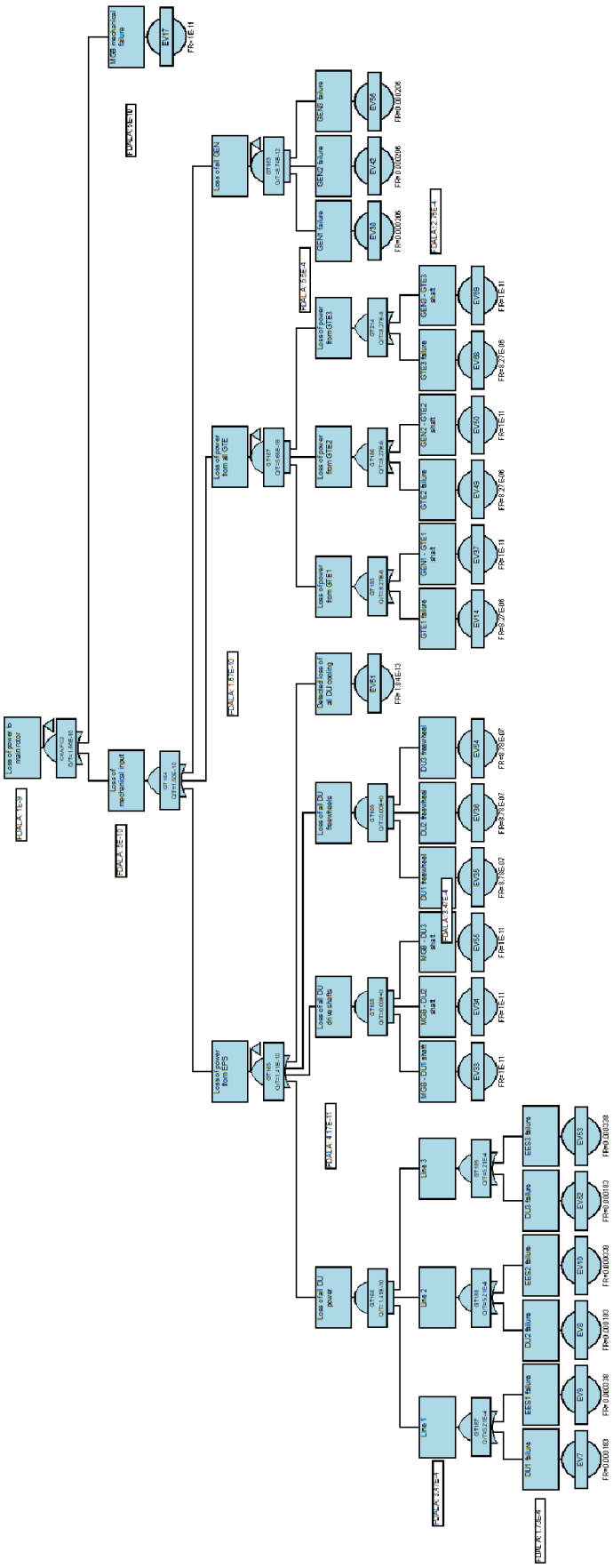


Figure E.8: C6A FC2

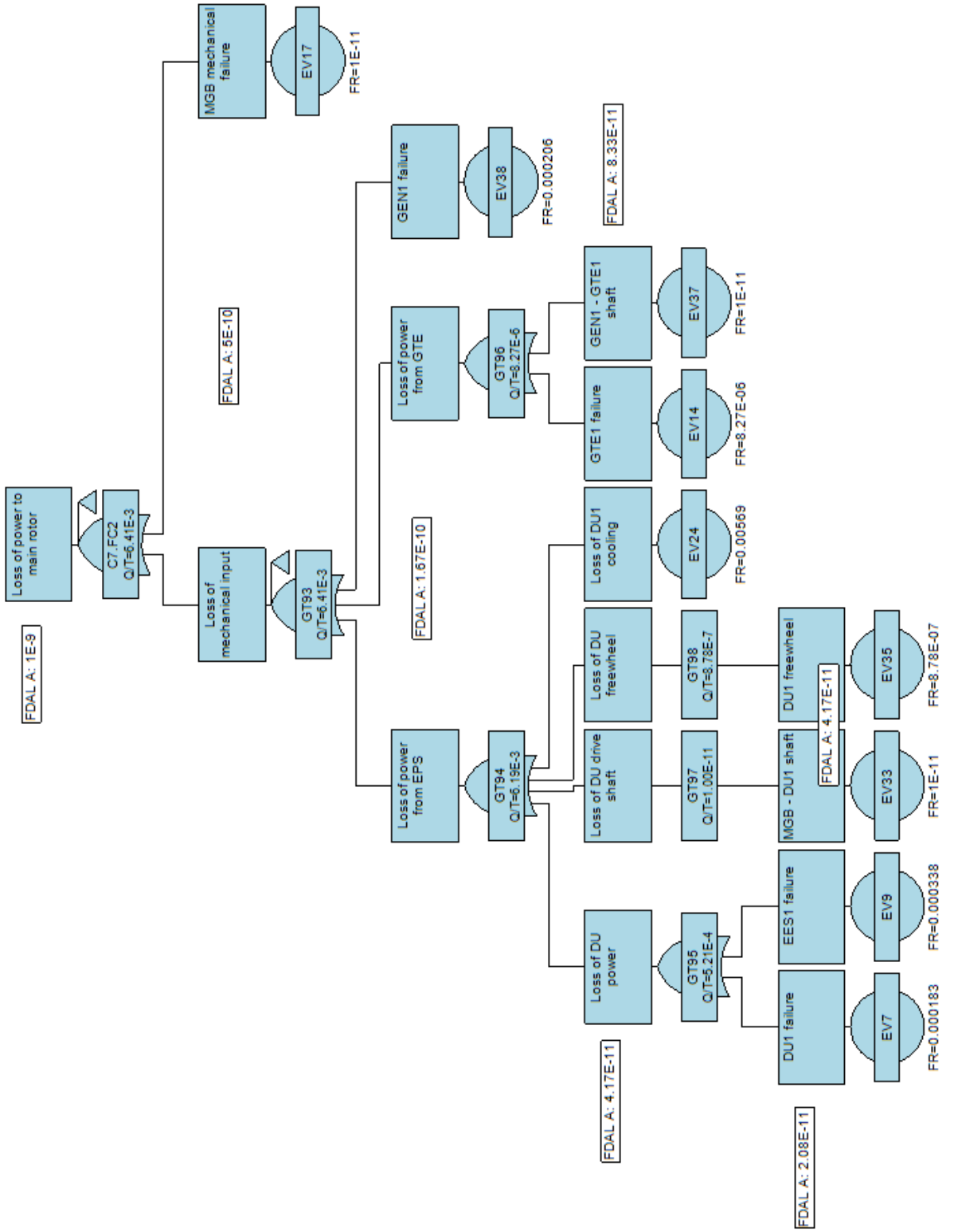


Figure E.9: C7 FC2

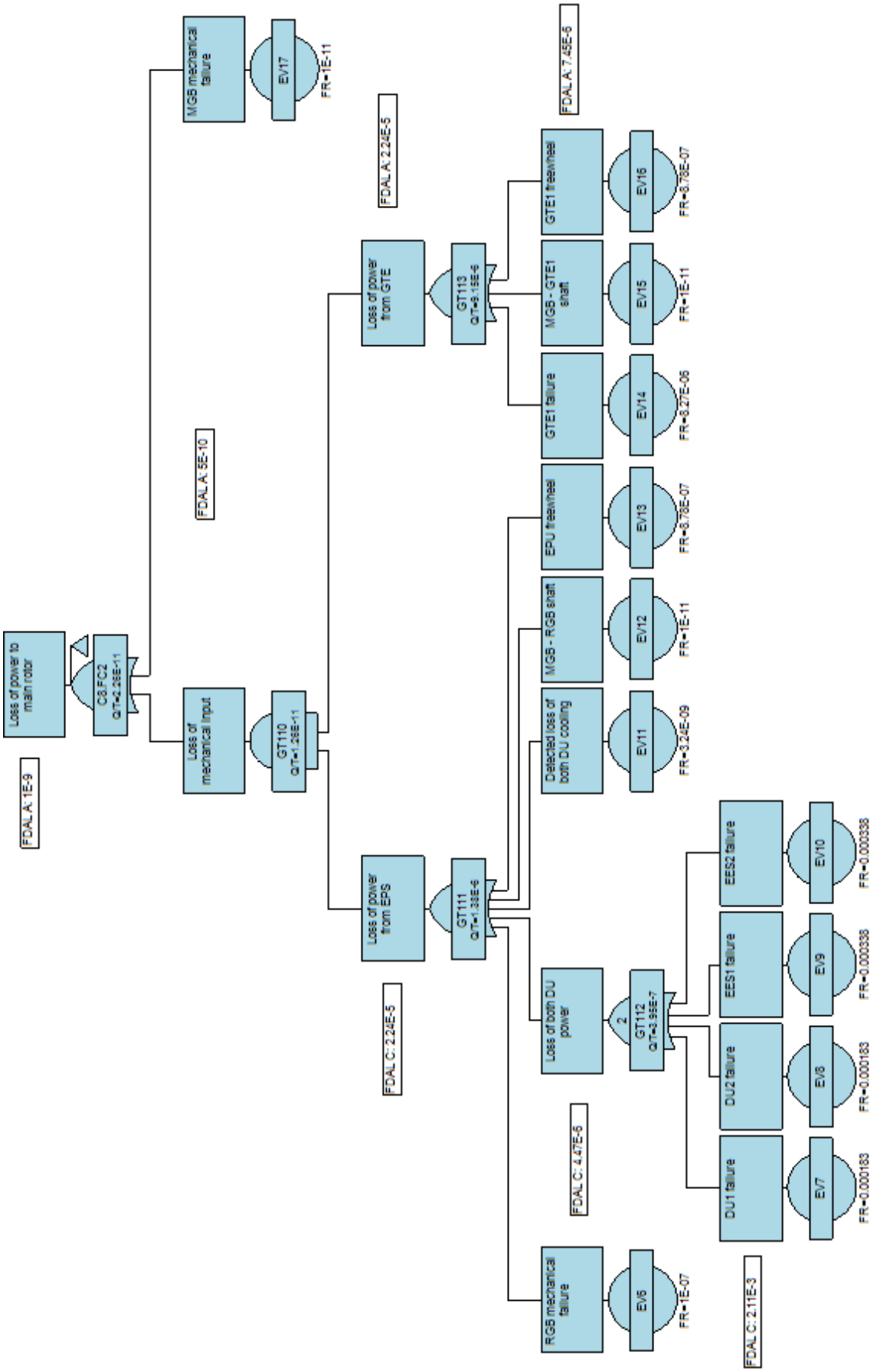


Figure E.10: C8 FC2

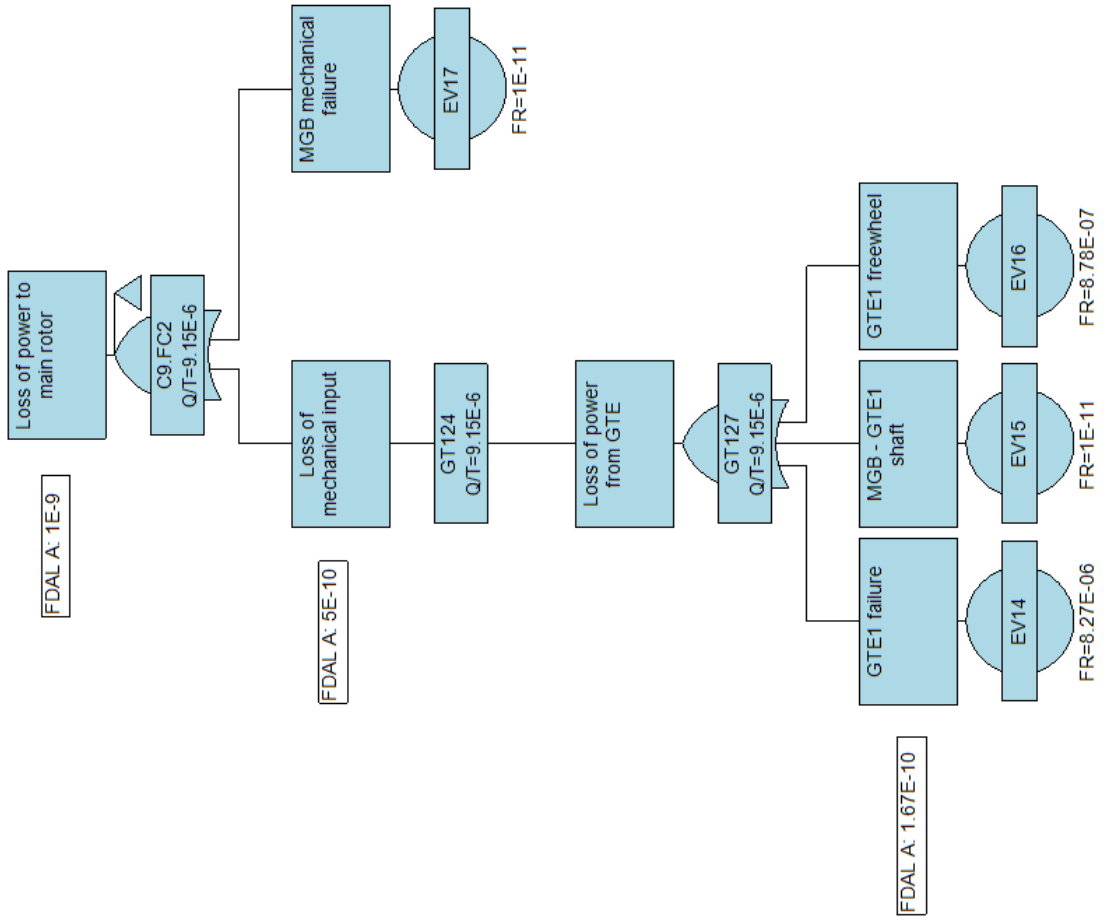


Figure E.11: C9 FC2

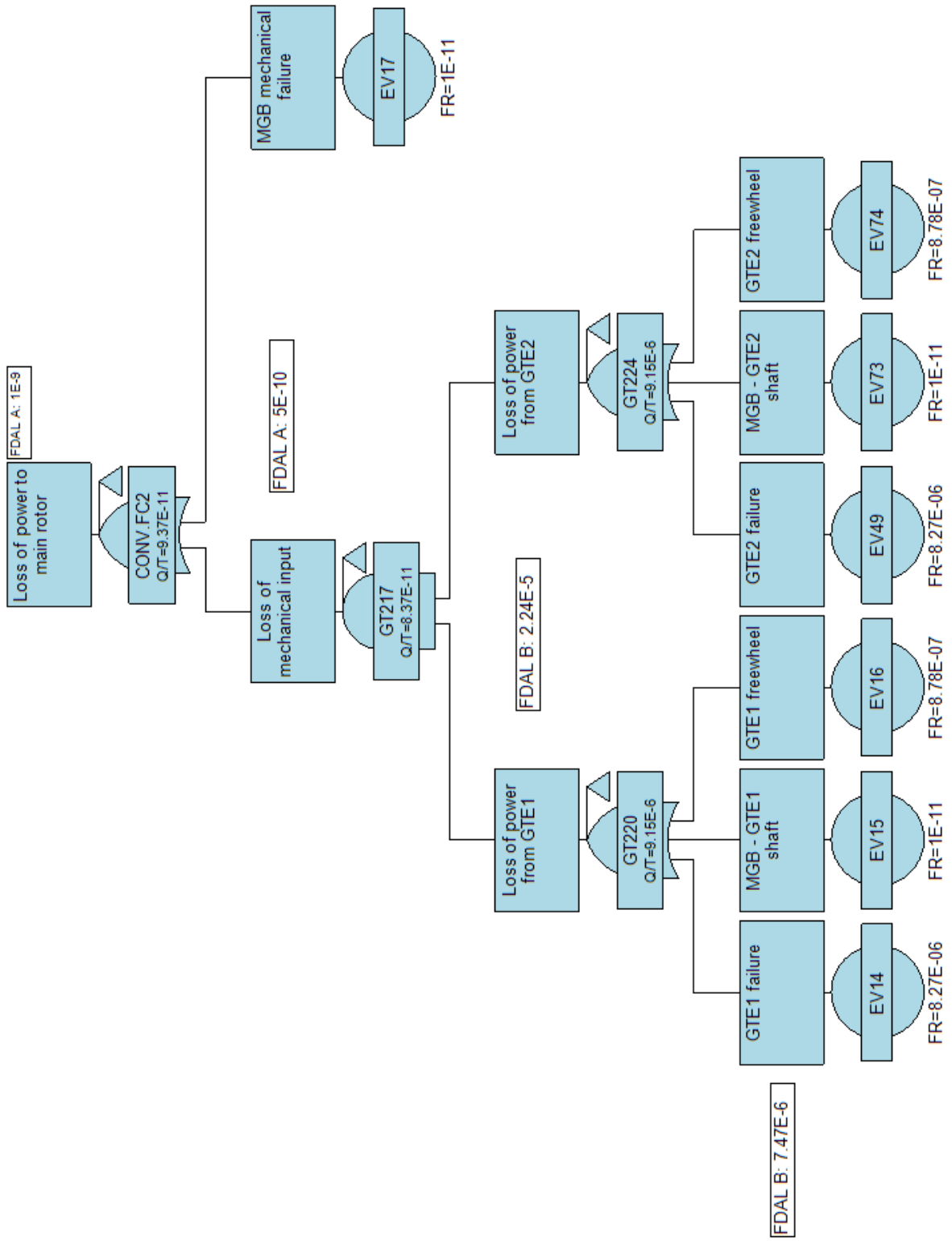


Figure E.12: CONV FC2

E.3. Weight Estimation Data

E.3.1. Battery Weight Estimation

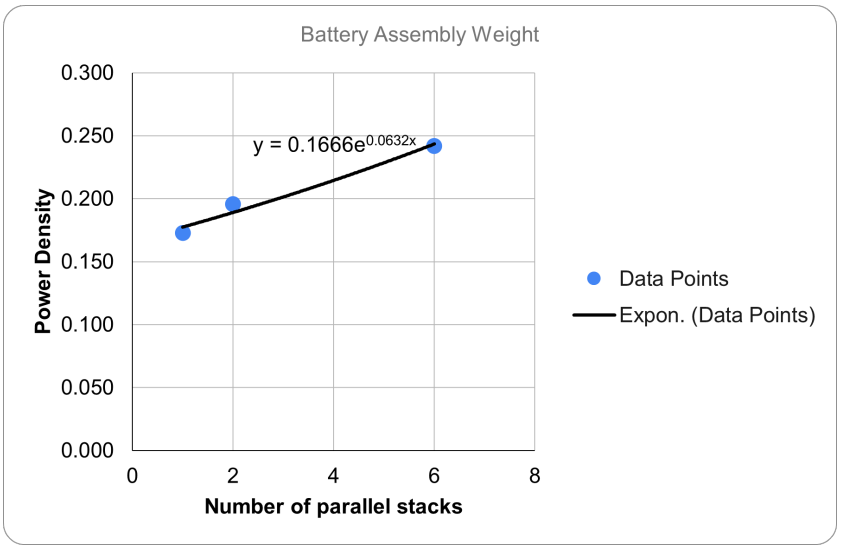


Figure E.13: EES assembly weight data

Power Density Inverse				
Parallel Stacks	**1**	**2**	**3**	**6**
Assembly [kg/kW]	0.172	0.196	0.211	0.241
HV battery [kg/kW]	0.434	0.434	0.434	0.434
EES assembly [kg/kW]	0.606	0.630	0.645	0.675
EES Weight per Stack				
Parallel Stacks	**1**	**2**	**3**	**6**
250kW EES [kg]	151.44	157.43	161.31	168.67
400kW EES [kg]	242.31	251.88	258.09	269.86
1166kW EES [kg]	505.78	505.78	505.78	505.78
2135kW EES [kg]	1293.32	1344.43	1377.57	1440.40

Table E.3: EES Weight Data

E.3.2. E-Motor Weight Estimation

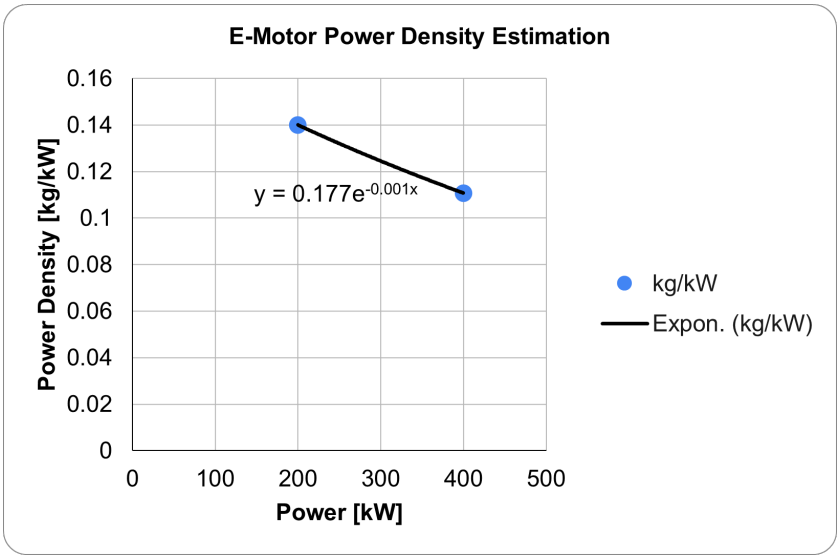


Figure E.14: EM weight data

E.3.3. Gas Turbine Engine Weight Estimation

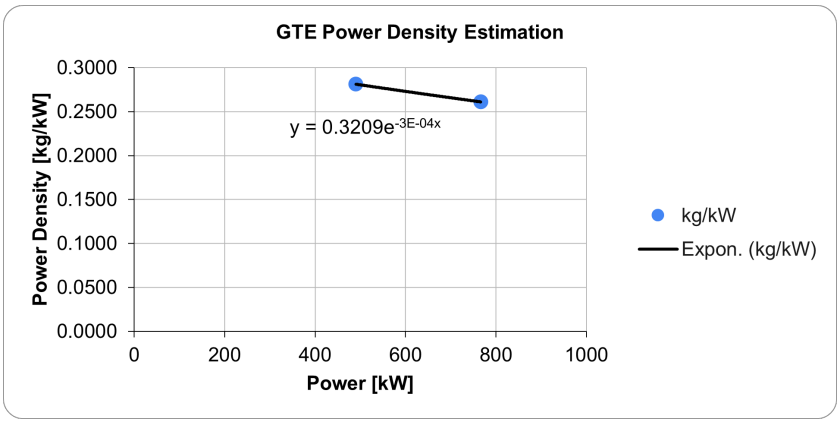


Figure E.15: GTE weight data

E.3.4. Generator Weight Estimation

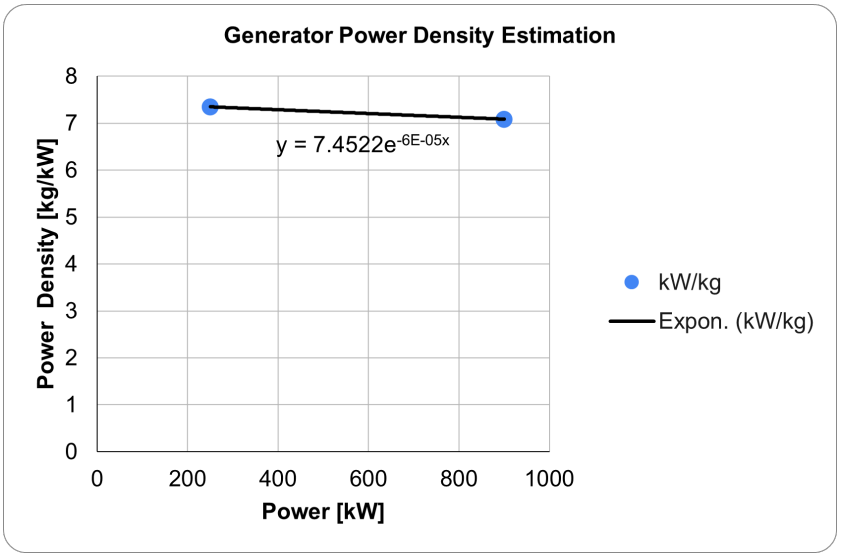


Figure E.16: GEN weight data