DLR-IB-MO-HF-2024-92

System design and analysis of a battery-electric propulsion system

Studienarbeit

Ricardo Dauer

Deutsches Zentrum
für Luft- und Raumfahrt

Projektarbeit im Forschungspraktikum

ILR-LFT PP 23-12

System design and analysis of a battery-electric propulsion system

Ricardo Dauer

Betreuer:

M.Sc. Robert Meissner, Deutsches Zentrum für Luft- und Raumfahrt, Hamburg

Dipl.-Ing. Chris Fischer, Institut für Luft- und Raumfahrttechnik, TU Dresden

Tag der Einreichung

01.05.2024

Abstract

The proportion of carbon and other environmentally harmful substances in the atmosphere increases steadyly and the climate of the earth is continuously warming up. The climate crisis yet has devastating consequences on humans, flora and fauna. To blame is not least our mobility infrastructure and therefore commercial aviation. Thus, it is proclaimed goal by many aviation players to develop towards a sustainable and emissionfree propulsion system. The improvement of fuel burning reduces the emissions but does not set them to zero, so that new technologies and variants need to be considered. One of these variants is the battery-electric propulsion system. This work aims to create a first design based on which an estimation on upcoming maintenance of such a system can be made and that clarifies at which stadium of development, decisions with most impact on corresponding maintenance effort were taken. Therefore, it was necessary to identify the prescribed steps to be taken to develop a system according valid laws and certification regulations. Subsequently, on a first system design all as necessary identified analyses were performed to define all relevant functions, which need to be certified in the system safety assessment. Based on the V-Model described in SAE ARP 4754A several subsequent analyses were conducted on system level to develop a first draft of the Electric Propulsion System (EPS). This provides the advantage of detailed knowledge of necessary functions, therefore required components, their amount and structure. Further, this work will demonstrate the first decision points for future maintenance and how to participate at the appropriate development phase to derive a maintenance optimized design.

Kurzfassung

Der Anteil an Kohlenstoff und anderen umweltschädlichen Stoffen in der Atmosphäre steigt stetig an und das Klima unserer Erde heizt sich kontinuierlich auf. Der Klimawandel hat bereits jetzt verheerende Folgen auf Menschen, Tier- und Pflanzenwelt. Schuld ist nicht zu Letzt unsere Verkehrsinfrastruktur und somit auch die kommerzielle Luftfahrt. Aus diesem Grund ist es das erklärte Ziel vieler Luftfahrtakteure sich hin zu nachhaltigen, emissionsfreien Antrieben zu entwickeln. Die Verbesserung durch Verbrennungseffizienzsteigerung ist dabei nicht mehr ausreichend, sodass neue Technologien und Varianten in Betracht gezogen werden müssen. Eine dieser Varianten ist das batterie-elektrische Antriebssystem. Diese Arbeit zielt darauf ab, ein erstes Design zu erstellen, auf dessen Basis eine Abschätzung der aufkommenden Instandhaltung vorgenommen werden kann und bestimmt in welchem Entwicklungsstadium Entscheidungen mit dem größten Einfluss darauf getroffen werden. Hierzu wurden an einem ersten Systemdesign alle als erforderlich identifizierten Analysen durchgeführt, um notwendige Funktionen zu definieren, die im Rahmen einer System Sicherheitsbewertung zertifizierbar sein müssen. Hierfür war es erforderlich die notwendigen Schritte zu identifizieren, die für das Design und die Zertifizierung eines solchen Systems nach geltenden Vorschriften erforderlich sind. Basierend auf dem, in Aerospace Recommended Practice (ARP) 4754A beschriebenem V-Modell, wurden verschiedene aufeinander aufbauende Analysen auf Systemebene durchgeführt und ein grundlegender Systementwurf erstellt. Die hierin generierten Ergebnisse bieten ein detailliertes Verständnis zu den erforderlichen Funktionen, die hierfür notwendigen Komponenten, deren Menge und Struktur. Weiterhin zeigt diese Arbeit die ersten Entscheidungspunkte für aufkommende Instandhaltung und wie zugunsten eines wartungsoptimierten Designs darauf Einfluss genommen werden kann.

Contents

Nomenclature **v**

Symbols v

Acronyms v

1 Introduction **1**

1.1 Problem definition 1

1.2 Definition of objectives 1

2 Fundamentals **2**

2.1 Authorities and Regulations 2

2.1.1 Authorities 2

2.1.2 Regulations and Reference material 2

2.2 System Design Aspects 3

2.2.1 Analysis 3

2.2.2 Safety Assessment 4

2.2.3 (Candidate) Certification Maintenance Requirements 5

2.3 Maintenance Methods 5

2.3.1 Physical Maintenance Task 6

2.3.2 Condition Monitoring 7

2.4 Reliability metrics 7

3 Theoretical Concept **9**

3.1 Approach 9

3.1.1 Investigation process 9

3.1.2 Initial System Layout 11

3.2 Assumptions and Limits 12

4 Development of a battery-electric system design **14**

4.1 Functional Breakdown Analysis (FBA) 14

4.2 Functional Hazard Analysis (FHA) 15

4.3 Fault Tree Analysis (FTA) 19

4.3.1 Optimization with Condition Monitoring 19

4.3.2 Optimization with Hard Time Event 21

4.3.3 FTA Redundancy 22

4.3.4 FTA Summary 23

4.4 Failure Mode and Effects Analysis (FMEA) 28

5 Results **30**

5.1 Developed System Layout 30

5.2 Estimation of upcoming maintenance 31

6 Conclusions and Outlook **32**

Bibliography **33**

List of Figures **36**

List of Tables **37**

Appendix A **38**

Nomenclature

Symbols

λ	h^{-1}	Failure Rate

Acronyms

ALI	Airworthiness Limitation Item
ALS	Airworthiness Limitation Section
AMC	Acceptable Means of Compliance
ARP	Aerospace Recommended Practice
BMS	Battery Management System
CAT	Catastrophic event
CBM	Condition Based Maintenance
CCA	Common Cause Analysis
CCMR	Candidate Certification Maintenance Requirement
CM	Condition Monitoring
CMA	Common Mode Analysis
CMR	Certification Maintenance Requirement
CS	Certification Specification
EASA	European Aviation Safety Agency
EDS	Electric Drive System
EPS	Electric Propulsion System
ESD	Energy Storage and Distribution
FAA	Federal Aviation Agency
FBA	Functional Breakdown Analysis
FHA	Functional Hazard Analysis
FMEA	Failure Mode and Effects Analysis
FMES	Failure Mode and Effects Summary
FST	Function Structure Tree
FTA	Fault Tree Analysis
HAZ	Hazardous event
ICA	Instructions for Continued Airworthiness
MAJ	Major event
MIN	Minor event
MTBF	Mean Time Between Failure
MTTF	Mean Time To Fail
POD	Probability of Detection
PRA	Particular Risk Analysis
SAE	Society of Automotive Engineers
TMS	Thermal Management System
ZSA	Zonal Safety Analysis

1 Introduction

The need for global decarbonisation requires sustainable, zero emission propulsion systems in aviation. A battery-electric system is a promising technology to provide the CO_2-free energy demand. Hence, an Electric Propulsion System (EPS) for future carbon-free aircraft shall be developed. Maintenance, Repair and Overhaul (MRO) significantly contributes to airlines cost outlay. Accordingly, the reduction of upcoming maintenance, especially for new technologies, is a main concern of customers.

1.1 Problem definition

In aviation, there is no comparable propulsion system in operation yet, nor any work regarding the application of the conventional certification- or development- approach for new technologies. Hence, the development approach for conventional systems shall be used and adapted. Therefore the prior determination of intended functions is necessary. Following the process the determined components have to be defined and evaluated accordingly, to derive a certifiable system structure. For certification reasons, the failure modes and how the system is intended to fail needs to be investigated as well.

To make an estimation on upcoming maintenance at an early design stage, it must be figured out, at which time the system design allows a concrete statement, for example *that the amount of future maintenance is mainly driven by the development made during the Fault Tree Analysis (FTA)*. As well on which factors a statement can be based on, meaning *the reliability of a specific component, needed to fulfill the function, defines it's reliability*. To meet customers interests, it shall be outlined at which point the system design is optimisable in terms of required maintenance. Therefore, an overview of what a maintenance optimum is, shall be clarified.

1.2 Definition of objectives

Aim of this work is to elaborate an approach for developing a new battery-electric system design. Depending on the requirements set on this system design,

> **necessary components and their structure shall be classified, so that the required (sub-)system structure can be defined.**

For this system structure and further to address customers interests, during the development process the amount of maintenance should be kept to a minimum. Accordingly

> **a first estimation regarding upcoming maintenance shall be derived and additionally the most favorable time for exerting influence on future maintenance should be determined.**

The results of this work will provide a first assessment of the necessary functions, components and interfaces. Additionally, it gives first impressions on maintenance to be expected, in comparison to a conventional kerosene based propulsion system. Based on this results, a more detailed investigation regarding a specific maintenance schedule and corresponding costs, even a more detailed system design can be deducted.

2 Fundamentals

The aim of this chapter is to show the basic regulations and necessary information, which give a guideline for development and assessment of a potential system design and its components. Additionally, a basic overview of maintenance methods shall be given. For quantitative analyses, a comprehensive research regarding components and associated failure rates was necessary so a brief outline of maintenance metrics will be discussed.

2.1 Authorities and Regulations

Due to very high safety standards in aviation, new systems, especially for new technologies, need to be certified and verified. Therefore the knowledge of the authority, responsible for the certification, is necessary. Moreover the regulation, describing the necessities and certification requirements, as well as the strategy and the substantiation need to be clearly understood.

2.1.1 Authorities

The authority responsible for defining and developing regulations for aviation in Europe is the European Aviation Safety Agency (EASA). It defines the certification requirements and recommends documents for standardized practices. Besides there are different other national authorities and organizations which have an influence on developing regulations and instructions, for example the Federal Aviation Agency (FAA), which is the national authority of the United States. With a glimpse in the regulation described in Sec. 2.1.2, another organization is presented, which developed a valid and standardized approach. The herein mentioned Society of Automotive Engineers (SAE) is a global association of engineers and technical experts developing voluntary consensus standards [31]. For an initial system design this work focuses on the regulations given by EASA and FAA and their subsequently referred standard processes from SAE.

2.1.2 Regulations and Reference material

To address the certification process of aircraft equipment, components and (sub-) systems, EASA issued the Certification Specification (CS) 25 for large aircraft. The current version CS 25 Amendment 28 states according paragraph 25.1309 for equipment, systems and installation:

> *The requirements of this paragraph [...] are applicable [...] to any equipment or system as installed in the aeroplane. [...] The requirements of CS 25.1309(b) apply to power plant installations as specified [...].* [10, p. 769]

Additionally, the EASA issues Acceptable Means of Compliance (AMC) for a more detailed description of the regulations. However, this supplements are recommendations for actions rather than regulations. The CS 25.1309 associated AMCs refer to Aerospace Recommended Practice (ARP) 4754A and 4761, which were industry documents published by the SAE and can be seen as advisory material for the development and safety assessment of aircraft systems.

The ARP 4761 introduces the workflow-model, which is a standardized process for development of a certifiable system design. Herein the sequence of recommended analyses and corresponding flow of data, results and information is given. A simplified model is given in Fig. 2.1.

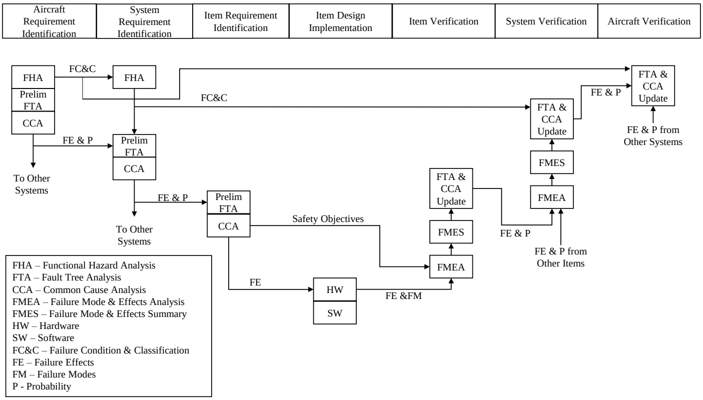


Figure 2.1 Simplified Workflow Model according SAE [30]

Important to mention is that neither this workflow model nor other regulations have legal character, as they are more a recommendation. The competent authority decides about a valid certification.

2.2 System Design Aspects

The following section focuses on the aspects and regulations given by CS 25.1309 for evaluation and assessment of the system under investigation.

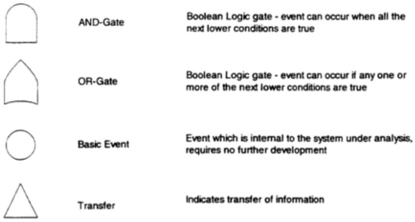
2.2.1 Analysis

From Fig. 2.1 it can be derived that several steps need to be taken for a complete system design process. It starts on aircraft level and can be broken down to the Hard- and Software level. Within this work the analyses shall focus on the system level. Nevertheless it can be seen in the workflow model that some analysis are inevitable like the Functional Hazard Analysis (FHA) and the Fault Tree Analysis (FTA). Before conducting a FHA, the functions the system has to fulfill, must be identified.

With the FHA several functions, determined in Ch. 4.1, are classified for each flight phase, failure condition and severity, depending on the impact the failure condition would have on the integrity of the component, the subsystem and the connection of subsystems.

The FTA is used to ensure the required classification, determined by the FHA for each function evaluated. This analysis does not require a specific layout as it depends on the components and the systems architecture, to provide the considered function. With the given instructions, there is a regulation how to analyze and evaluate the failure condition. Therefore the FTA uses boolean operators, of which some are displayed in Fig. 2.2. The basic event represents a specific component or failure cause with an individually failure rate (λ). Several basic events were connected with AND- or OR-operators, depending on their connection given by the system design. The transfer-operator is used to connect several failure trees to each other.

Because FHA and FTA do not consider the effects or consequences of a failure and further to understand the mechanisms of failures, it is also useful to perform a Failure Mode and Effects Analysis (FMEA). Additionally, weaknesses of a fail-safe concept can be identified. The FMEA is a bottom-up procedure and aims on avoiding failures or to minimize their consequences and correspondingly implement corrective or preventive actions [7]. Not only to include the



AND-Gate	Boolean Logic gate - event can occur when all the next lower conditions are true
OR-Gate	Boolean Logic gate - event can occur if any one or more of the next lower conditions are true
Basic Event	Event which is internal to the system under analysis, requires no further development
Transfer	Indicates transfer of information

Figure 2.2 FTA Operators

results in the certification of the system, but as well to investigate at which point of this analysis decisions regarding maintainability were taken the FMEAwas conducted. Also if, at this point of investigation, it is possible to contribute an approach for better maintainability.

A detailed description for the three analysis is given by ARP 4761 [30] and 4754A [29].

2.2.2 Safety Assessment

The development of the system design is based on the safety assessment described in the ARP documentation introduced in section 2.1.2. Herein and in CS 25 some phrases are established, which are used to classify and to group the results, equally they were used to derive the safety objectives.

To classify the possible failures of functions, the severity of their effects need to be defined. Therefore a strict definition is given by the regarding AMCs in CS 25, whereby a distinction is made between following cases:

- No safety Effect: Failure conditions without an effect on safety, operational capability or increase of workload for the flight crew
- Minor: Failure conditions that may slightly reduce safety or functional capabilities, slightly increase of workload leading to flight plan changes, discomfort for passengers or crew
- Major: Failure conditions that may significantly reduce safety or functional capabilities, significantly increase workload impairing the crew efficiency, discomfort/distress for crew or passengers; possible injuries
- Hazardous: Failure condition that would lead to a large reduction in safety or functional capabilities, physical distress or excessive workload significantly decreasing crew performance, serious/fatal injury to small number of passengers
- Catastrophic: Failure condition that would lead to multiple fatalities, usually loss of aircraft

With these cases, each failure condition can be allocated to a certain severity of their effects within the FHA.

Each severity classification gets assigned to qualitative and thus a quantitative probability term according the description of safety objectives of the mentioned AMCs. An allocation is displayed in Tab. 2.1.

The quantitative probability term will be used for verification of the safety objectives examined during the analyses and can be understood as *Failures per flight hour*.

Table 2.1 Classification according to severity and probability

Failure Severity	Qualitative Probability Term	Quantitative Probability Term
Catastrophic (CAT)	Extremely improbable	10^{-9}
Hazardous (HAZ)	Extremely remote	10^{-7}
Major (MAJ)	Remote	10^{-5}
Minor (MIN)	Probable	10^{-3}
No Safety Effect (NSE)	No Probability Requirement	-

2.2.3 (Candidate) Certification Maintenance Requirements

First of all, the definition of (significant) latent failures is important, to understand what Candidate Certification Maintenance Requirements (CCMRs) aim to. Latent failure means the failure already exists and needs to be made known to the flight crew or maintenance personnel. It is additionally significant when it's occurrence in combination with one or more failures would lead to a hazardous or catastrophic failure condition.

Kritzinger [23] wrote, to achieve the safety objectives of significant failure condition may lead to the need of mandatory periodic maintenance tasks. They need to be tracked individually and their accomplishment recorded for regulatory oversight. In general, this CCMR analysis is a method to identify and compensate significant latent failures.

CCMRs are maintenance tasks/intervals identified during the development and investigation of the design, specifically during the Fault Tree Analysis (FTA) to demonstrate compliance with 25.1309(b) which can not be accepted as basic servicing or airman ship. After they have been assessed by a specific committee, the system is either iteratively adapted to avoid the task or it will be forwarded as a Certification Maintenance Requirement (CMR) for inclusion in the Airworthiness Limitation Section (ALS) [24] and become part of the Instructions for Continued Airworthinesss (ICAs) (see Ch. 2.3). When they become CMRs they are intended as failure finding tasks and exist solely to limit the exposure to otherwise hidden failures [17]. CMRs are designed to verify that a certain failure has either not occurred [30] or to fix them afterwards, so it can be defined as preventive maintenance.

The system design strives for a minimum of CMRs, which has different reasons. Foremost, to satisfy operators interests, any maintenance event causing additional downtime should be avoided, as it causes additional planning and scheduling with maintenance intervals not necessarily aligned. Aviation aims for reduction of costs, improving efficiency and enhancing maintenance processes. Condition Based Maintenance (CBM) uses digitalization and data analytics to guarantee high flexibility in maintenance scheduling. This is in contrast to predefined and strict CMRs.

2.3 Maintenance Methods

As in the safety analysis maintenance tasks can be used to satisfy the safety requirements, a short presentation of the corresponding implications shall be given. Accordingly, in this chapter the implications to keep the system in an airworthy condition, described in CS 25.1529 and the subsequently referred Appendix H, are explained and contextualized.

Maintenance requirements derived through the safety assessment are intended to ensure that the design of the aircraft meets the defined safety standards. These requirements are compiled and structured into the ALS. The ALS comprises Airworthiness Limitation Items (ALIs), CMRs and other limitation describing documents [2]. ICA are all the necessary instructions to ensure the airworthiness of an aircraft is maintained throughout its operational life. Only those documents and instructions whose purpose is to maintain the design standard and the airworthiness of the aircraft (safety) will be considered as ICA. It contains next to already mentioned ALS, the requirements from design process (CMR) and the initial aircraft maintenance program investigated within MSG-3 process. [24]

The following maintenance methods had been used in this work for system design, so it is helpful to understand the difference and their implications.

2.3.1 Physical Maintenance Task

The definition of maintenance according to industry standards includes those tasks required to restore or maintain an aircraft's systems, components and structures in an airworthy condition. [18]

There are many different ways to classify or differ maintenance, for example the difference whether the maintenance is scheduled and planed or unscheduled. Further there is a classification possible in which detail the maintenance is done, which means if it can be performed On-Wing (Line Maintenance) or if it is necessary to remove the corresponding component to be restored in a separate facility (Base Maintenance). This differentiation can be made for parts and areas of the aircraft [18]. The necessary maintenance tasks results from safety requirements delivered by the design with the corresponding safety analysis (CCMRs) and the subsequently performed MSG-3 Analysis [1] ([12],[18])

The MSG-3 method is used for developing the scheduled maintenance tasks and intervals, which were selected depending on failure severity and consequences. The maintenance strategy includes the tasks given in following list with a short description [2]:

- Lubrication/Servicing (maintaining inherent design capabilities)
- Operational/Visual Check (failure finding task)
- Functional Check/Inspection (check if functions perform within limits)
- Restoration (reworking, partial replacement, cleaning to restore specified standard)
- Discard (removal from service at specified life limit)

For economic optimization reasons as many tasks as possible should be performed together as so called maintenance checks. Maintenance Checks were grouped, based on their interval, parameters and necessary accesses. [24]

The tasks mentioned above can be considered for an integration during the safety analysis to satisfy the safety requirements. In Ch. 4.3.2 the discard task has been chosen to demonstrate this procedure. Each task has a certain influence on the systems reliability and thus requires a different mathematical approach. For the chosen maintenance method a resilient calculation approach had to be defined and integrated.

[1] After dividing the aircraft into zones, components and systems, the MSG-3 Analysis will be conducted for them. This means they are investigated according functions, safety, failure risk and consequences, access for maintainability, probability of defect detection and environmental influences. Based on this analysis the inspection intervals, -intensity, tests and tasks are defined. [18]

2.3.2 Condition Monitoring

One of the most promising approaches on maintenance optimization is the Condition Monitoring (CM), which is used to detect faults of the different components and their interactions, before they become critical. Here, information of a specific component or system behavior is collected during the usage continuously or on demand. These information are used to identify optimal maintenance interventions to increase the efficiency of maintenance operations. Simultaneously, including a CM is intended to improve reliability of the monitored system or component while the monitoring system needs to satisfy safety requirements [37]. Thus a system/component is less tended to fail when their condition is monitored and adequate maintenance is performed when necessary. The advantage of CM is that resulting maintenance tasks adapt according systems/components condition, means if there is no detectable decrease of properties then maintenance is not required. However, the disadvantage is the complex integration in the structure, which may require maintenance and that detailed knowledge of failure occurrence for measurability is necessary. This work will show, in Sec. 4.3.1, an approach how to implement an evaluation method of CM at an early design stage based on the assessment according Schildt et al. [33].

2.4 Reliability metrics

A common approach in evaluating the reliability of components is the usage of reliability metrics. These are statistical descriptions of the failure probability of this considered component. Different metrics were used to describe the different usage conditions addressed by the regarding metric.

The availability of a component is described by the failure rate λ which represents the probability of an object failure during a specific time and is expressed as amount of failures per time unit. Moreover a failure rate is not constant over it's life time, as it varies depending on the stage of life. The so called *bathtub curve*-theory, presented in Fig. 2.3, postulates there are 3 stages: *infant mortality* followed by a lower, steady rate and a wear out age. This work will assume and only consider the constant part *useful life* [36]. It has to be noted though, each λ used in this work depends as well on the model it is based on, so that a specific uncertainty follows.

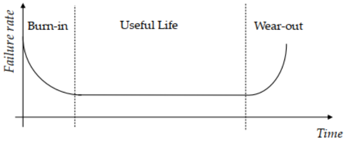


Figure 2.3 Bathtub curve of a generic component during time [36]

With the assumption of a constant λ, equation 2.1 describes the failure density of the regarded object. After integrating, equation 2.2 delivers the failure probability of the considered object, which describes that a failure will have occurred at, or before a specific time [28]. It is also declared as *unavailability*. These equations follow the approach of exponential distribution. An other approach would be the *Weibull Distribution*, which considers additionally the repair and the corresponding time consumption. This is neglected in this work.

$$f(t) = \lambda e^{-\lambda t} \tag{2.1}$$

$$F(t) = 1 - e^{-\lambda t} \tag{2.2}$$

Equation 2.2 will play a major roll in developing an approach on integrating maintenance at an early design stage later in this work, since it is the calculation basis of FTA.

The following metrics were used in this work and will therefore be described in more detail.

$$MTTF = \int_0^\infty e^{-\lambda t}\, dt = \frac{1}{\lambda} \tag{2.3}$$

$$MTBF = \frac{runtime}{No.\, of\ failures} \tag{2.4}$$

Basically it can be said that Mean Time Between Failure (MTBF) and Mean Time To Fail (MTTF) describing the same component behavior, the only difference is that a MTBF-considered component is repairable, whereas a MTTF-considered component is irreparable [36]. For this work no differentiation was made, as it was assumed that a failed component was reinstalled repaired without any decrease in reliability which is comparable to an installation of a new component. The associated downtime is also neglected.

3 Theoretical Concept

This chapter serves to explain the steps taken to develop an investigation process for designing an initial battery-electric propulsion system which fulfills the requirements given by the authority's regulation. Thereby, limits and assumptions in which the propulsion system shall operate were outlined, as well as previous design layouts will be compared. These layouts will be the starting point for the investigation of an appropriate system layout of an aircraft propulsion system.

3.1 Approach

3.1.1 Investigation process

Following Ch. 2.1.2, CS 25.1309 and subsequently the ARP documents are the template of the investigation process. As the goal of this work is the initial design of the EPS, it is not necessary to fulfill the whole process given in Fig. 2.1, thus we can start on system level and can subsequently go deeper to the subsystem and component level, when necessary. With a deeper look in the several analyses, it shall be identified which of them contributes to a significant influence on the system design and which is more useful for an iterative improvement of the first draft. Further, depending on the necessary knowledge of the system design and the required engineering judgment, analyses can be excluded from the initial investigation process. Out of this assessment, based on the author's engineering judgment, an investigation procedure is developed that ensures a consequent and reproducible traceability of the results. At this point it shall be mentioned that this work is not an iterative investigation like the V-Model states. This does not include detailed analysis regarding Hard- and Software of the components, nor an iteration to improve the previously defined functions and components.

Functional Breakdown Analysis (FBA)

Before starting with the system design assessment detailed knowledge of the functions the (sub-) system has to provide is required. Graaf et al. [15] used Function Structure Trees (FSTs) as method for evaluation of required functions, which presupposes a certain knowledge of these functions and their structure. A quite different approach is used by Jäger et al. [19]. Hereby an interaction diagram was chosen to evaluate connections between (sub-) systems and other interactions, so that through this, a data- and energy flow can be derived. This optional interaction diagram serves as the basis for generating a Use Case Diagram, in which functions and their sequence can be displayed, allocated to the corresponding (sub-) system. Hereby, the evaluated data- and energy flow is used to derive the connections and dependence of those functions. As it is easier to figure out what participants require and which functions they provide, the approach by Jäger et al. [19] was chosen for this work.

Therefore, the FBA [19] shall be conducted on system level for the complete EPS, divided into 3 subsystems - Energy Storage and Distribution (ESD); Thermal Management System (TMS); Electric Drive System (EDS).

Functional Hazard Analysis (FHA)

In the first step of the FHA, all examined functions are classified by Flight Phase and Failure Condition. For both, Jäger et al. [19] delivers the corresponding categories, so that the flight phases are chosen as follows :

- Push Back, Taxi
- Start, Take off
- Climb
- Cruise
- Descent
- Landing, Taxi

The different failure conditions after which a function can fail, is also taken over from Jäger et al. [19], which provides a broad spectrum of failure possibilities.

- Degradation of the function
- Inadvertent operation of function
- Incorrect operation of function
- Partial loss of function
- Total loss of function
- Unable to stop function
- Asymmetrical partial loss of function

Hereby, the classification is carried out according to the categories given in section 2.2.2, with focus on Catastrophic events (CATs) and Hazardous events (HAZs). Those events are grouped by function and failure condition and subsequently transferred to the second step of the FHA for a more detailed evaluation, according the procedure defined by the ARP documents. During the second step those events are investigated regarding the corresponding failure scenario and it's subsequent effects depending on their failure condition. The result of this investigation is a clear understanding of different failure conditions and their effects, corrected classifications as well as the safety requirements corresponding to each function. This includes possible connections to other systems.

Fault Tree Analysis (FTA)

For the initial system design, the focus is on catastrophic events, so that FTA is performed on those functions only. Therefore, all functions that had been assessed as CAT are grouped according to their failure condition, whereby a differentiation by Flight Phase is not made, because it is assumed that the flight phase has no influence on the fault tree structure.

With the performed analyses and investigations, the required amount of components and their redundancies can be quantified. Further, it is shown at which point in the early design phase decisions towards the future maintenance effort are taken or can be influenced.

Failure Mode and Effects Analysis (FMEA)

Conducting the FMEA aims on investigating the cascading failure effects, which delivers in advance the possibility to evaluate the component architecture for common mode failures. Further, the FMEA provides possible approaches on detection and compensation of the failure conditions. However, evaluating the failure modes of each considered component requires on the one hand the knowledge, which components are integrated in the (sub-)system, on the other hand an extensive engineering judgment of different failure modes of these components.

Excluded analyses

Having a look on the V-Model shows that some analyses have been excluded, the Common Cause Analysis (CCA), which consists of 3 different analyses - Common Mode Analysis (CMA), Particular Risk Analysis (PRA) and Zonal Safety Analysis (ZSA) - and the Failure Mode and Effects Summary (FMES). To conduct the ZSA the exact position of each component and the surrounding items, systems and materials needs do be known, which is the case in later design phases. With a PRA, events are analyzed which occur during the component's life time, meaning special cases, e.g., hail, lightning strike and others. It is also excluded as a useful conduction is possible, as soon as the system design is further advanced. Conducting a CMA can be useful at early design stages but requires high engineering judgment, especially for (micro-) electronics. The FMES is excluded, as it is merely a summary of different FMEA-results.

3.1.2 Initial System Layout

Within this section an overview for the necessary components, subsystems and the corresponding structure shall be outlined. On the scale of an A320, there is no example or a comparable model of a battery-electric propulsion system. Accordingly, a research for similar systems or previous investigations is necessary. Currently there are many different system design approaches under investigation which are promising to the sustainability requirements, but usually include a second energy carrier, for example a kerosene-hydrogen hybrid system, or even a third, e.g. a support battery. Mostly used is a combination of fuel conversion and an electric drive train. Evaluating these different system design approaches ([19], [33], [32], [38], [22]) they can be compared for similarities and equally used components.

What all systems have in common next to the battery is an inverter and an electrical motor. Additionally most of those layouts use a Battery Management System (BMS), which can be understood as a microelectronic component directly connected to the battery. It has to ensure the safe and reliable operation of it and provides an effective monitoring of all relevant parameters to improve the performance [34].

Depending on use case and scale of layout the system requires a more or less extended Thermal Management System (TMS). The TMS provides a coolant circuit to reject waste heat, produced by the EPS, via a heat exchanger [9].

A further design approach given by Anker et al. [5] in Fig. 3.1 is developed for the scale of a commuter aircraft. However, this approach provides all necessary subsystems and components to store, transform and provide electrical energy, equally it matches the system layouts already mentioned.

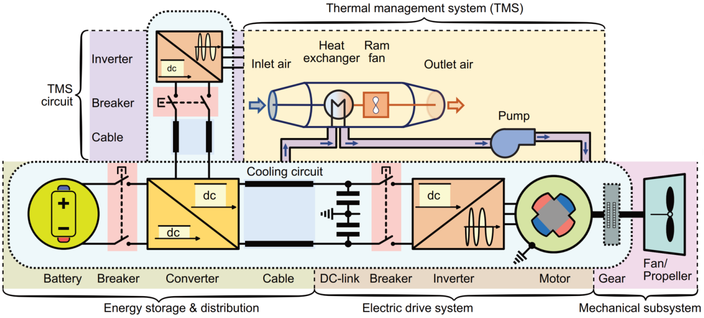


Figure 3.1 EPS Design for Commuter Aircraft [5]

Compared with the other system design approaches it can be determined that there are components which are essential for a battery-electric propulsion system whereas others improve the efficiency and reliability of it. Based on these design examples, Fig. 3.1 is the basis of all following analyses. It is separated in the 3 mentioned subsystems of which each is analyzed separately.

3.2 Assumptions and Limits

To simplify this investigation approach several assumption are made, as well there are specifications given by the aircraft under investigation. In addition, as this is an initial investigation the results are limited by the simplifications on the one hand and the uncertainty of analyses and data basis on the other.

The aircraft on which the investigation is based is an Airbus A320, so that the propulsion system is defined with **2 engines**. As mentioned above the EPS is assumed to be **divided in 3 parts** whereby each engine is considered with a separate Electric Drive System (EDS) and a common TMS and Energy Storage and Distribution (ESD). The TMS, consisting of **2 separate cooling circuits with opposite flow direction**, is designed to cool the whole EPS and is modeled after the common design of a hydraulic system in aviation. It operates on a **constant temperature** profile in which components shall be arranged according their optimized heat production rate and cooling demand. The **coolant** is assumed as a **hydraulic fluid**. Also other parts require a further definition prior to assessment. Hence, the battery is defined as a **Lithium-Ion battery** as it currently provides the highest energy density [32]. This investigation does not include the evaluation or definition of structural integrity, so that the power- and data-transfer components will not be investigated as their required length can not be determined. The decision on the TMS, cooling all components consecutively can lead to insufficient cooling of the last components in flow direction. Thus it would be appropriate to design the coolant flow in a way that those component that require the highest cooling are the first in flow direction.

To simplify the conduction of the investigation as well as to focus on technical aspects only, other aspects are excluded from further investigation. **Environmental and manufacturing conditions as well as human factors are disregarded** in all analyses. Further, each analysis has it's typical restrictions and assumptions. The **failure rates** used in the FTAs follow a conservative approach. When there are different values available always the worst is chosen. During the FHA, as CAT examined failures and failure conditions of one component are grouped, and in case their failure condition is nearly similar, they are investigated as one due to lack of data. During the initial safety assessment combined failures of different components, will be disregarded. An attempt is made in the FMEA. But this analysis is conducted only on the ESD and considers only a few combined failures.

Further, for satisfying the requirements within the FTA, two different approaches are used, for which certain assumptions has to be made. Thus, for the integration of a **hard time maintenance event**, a calculation method based on the mathematical description, given in chapter 2.4, is used. Hereby it is assumed that performing maintenance at a specific time has a **direct influence on the regarded component's reliability** and consequently it's failure rate improves. The impact of this maintenance event on reliability of the systems is neglected.

Equally, including a **CM** is expected to **improve the reliability** of the monitored system or component due to continuous measurement and subsequent condition assessment. A quantitative method according Schildt et al. [33] is used to calculate an improved failure rate. The monitoring system itself is considered certifiable, based on Verhagen et al. [37] and thus has no impact on system's reliability.

All these simplifications and assumptions lead to limitations of the outcome of this investigation. Also the personal engineering judgment and the accordingly made decisions during FHA and FTA subject to an uncertainty of the results.

4 Development of a battery-electric system design

This chapter explains gradually the investigation according the described steps of Ch. 3.1.1. Therefore each analysis will be described regarding their used layout, necessary in- and outputs and a short presentation of results and their further usage.

4.1 Functional Breakdown Analysis (FBA)

The first step, necessary to conduct a system safety assessment, is to figure out which function(s) the EPS and it's corresponding subsystems have to provide to the aircraft and between each other. As described in Ch. 3.1.1, an interaction diagram is created and displayed in Fig. 4.1. Herein all participants and interactions during operation of the EPS are set in relation to it.

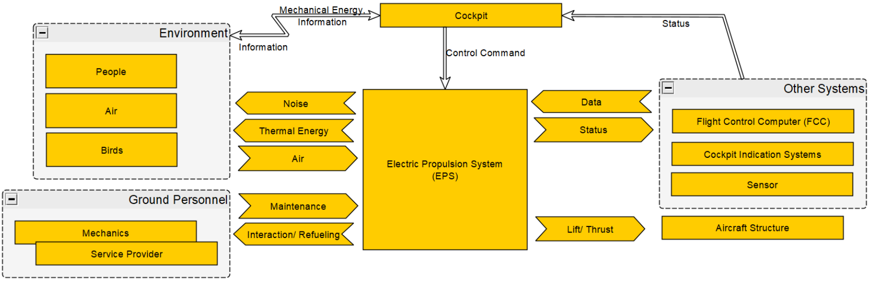


Figure 4.1 Interaction Diagram for EPS

From the identified participants and interactions, excluding those declared in Ch. 3.2, the necessary groups for the the use case diagram can be derived. Commands and data transfer are summarized to the group *Commands*, the EPS is divided into the three predefined subsystems and the aircraft is simplified as *Mechanical System*. The use case diagram is created, using these groups and connects them to each other, depending on the functions they shall provide. To evaluate the interactions during a specific use case, detailed knowledge of aircraft operation, as well as physical effects is necessary. The higher the engineering knowledge and the general understanding of the system, the more accurate is the result.

Generating a Use Case Diagram can be described as an allocation of consecutive tasks to perform the considered Use Case. Depending on the level of detail the analysis was conducted, the several functions can be allocated to special components. The excerpt of the Use Case Diagram in Fig. 4.2 shows, next to participants and interfaces the subsystems of the EPS. Within these blocks each function with it's connection to the corresponding participant is displayed. Thus a basic overview of functions of each subsystem is generated, which will provide the input for the FHA. Herein examined functions do not necessarily belong to the subsystem as stated in this investigation. This will be identified during following analyses.

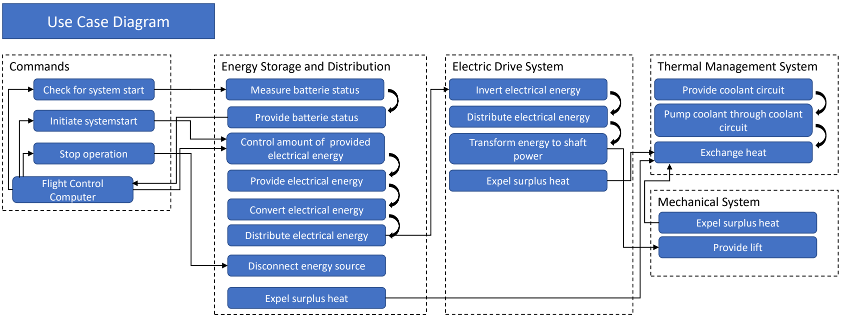


Figure 4.2 Excerpt of Use Case Diagram for an EPS

4.2 Functional Hazard Analysis (FHA)

A detailed description is given by ARP 4761 [30] and 4754A [29] but without any layout. Comparing different sources ([39], [6], [25]) of performed FHAs they deliver several layouts with some similarities listed below:

- Function
- Flight Phase
- Failure Scenario
- Failure Effect
- Failure Condition
- Classification

For a wider information output of this investigation the layout of Noviello et al. [25] was chosen, which extends the similarities above by following points:

- Justification for Classification
- Detection
- Recovery action
- Design parameters

For possible correction in case of a wrong initial assessment a column for a corrected classification in the second step of the FHA was added. As there are 28 determined functions from the FBA, 6 different flight phases and 7 different failure conditions this results in 1176 error states of which this work shall consider CAT events only. Therefore these 1176 states need to be classified before the conduction of the FHA. The classifications after which these functions shall be categorized were already mentioned in Ch. 2.2.2. Jäger et al. [19] delivers a useful approach for a first step analysis. With the conduction of this *function analysis* displayed in Fig. 4.3 the number of error states can be reduced to 211 CAT and HAZ events, which can be transferred to the second step for a more detailed investigation. Fig. 4.4 shows an excerpt from this second step. Previously as CAT classified functions that are corrected during a more detailed evaluation of step two, still will be transferred to the FTA as CAT event. For HAZ events corrected to CAT will be transferred as CAT. This procedure is chosen to address any uncertainties through a conservative approach. For both steps, the initial classification as well as the complete evaluation of each error state require high engineering judgment and understanding of the system and it's components.

The classifications determined in this analysis corresponds to specific quantitative probability according Tab. 2.1. To ensure these requirements, the Fault Tree Analysis (FTA) was chosen.

Fig. 4.3 displays an excerpt of the initial assessment wherein each function grouped by the 3 subsystems is assessed on failure condition and flight phase. CAT- and HAZ-events are colored within the initial assessment and will be further evaluated. Other classifications will not be considered in this work as their impact on initial system design can be neglected, due to lesser safety requirements.

All colored events will be grouped after function and flight phase, separated in CAT- and HAZ-events for a more detailed evaluation. Thereby each failure scenario is described according the failure condition that causes it, as well as the effects on aircraft, occupants and other systems. These results may verify the previous classification or lead to a corrected classification which is then justified separately. Additionally a first investigation on how to detect the regarded failure and how to react appropriately to recover the failure scenario that is evaluated. Possible design parameters to avoid or reduce the risk of appearance shall be given for the safety requirements. An excerpt is displayed in Fig. 4.4.

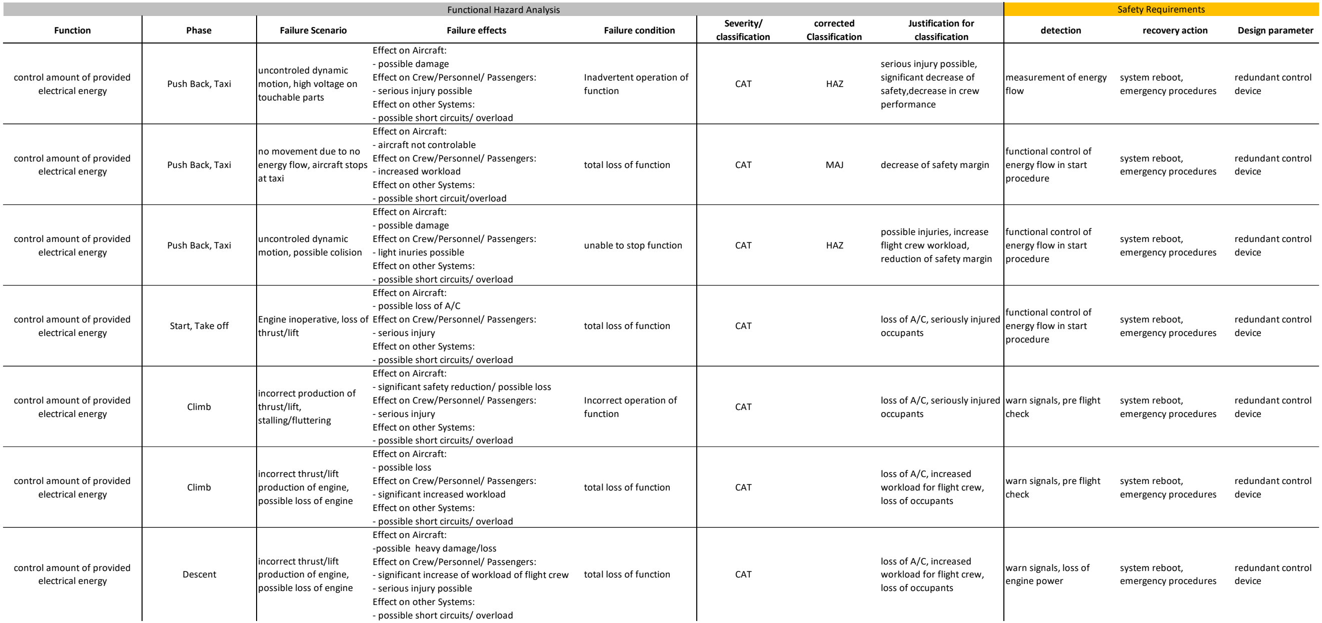
The first Line in Fig. 4.4 shows the first function of the FHA. Exemplary for the function *Control amount of provided electrical energy* during the flight phase *Push Back, Taxi* and with failure condition *Inadvertent operation of function* the investigation according FHA approach shall be explained. The failure scenario depends on the failure condition of the considered function and has different effects depending on the flight phase. With engineering judgment a possible failure scenario is defined and subsequently the effects on aircraft, systems and occupants is evaluated. Accordingly, a possible failure scenario is defined as *uncontrolled dynamic motion or high voltage on touchable parts*, which are serious failure cases on ground endangering ground personnel. The consequences are derived for the aircraft as *possible damage*, for other systems *possible short circuits/ overload* and for the occupants *serious injury possible*. Depending on the investigated effects a justification for classification can approve the previously defined severity or can show the need for correction. This function can be justified as *serious injury possible, significant decrease of safety, decrease in crew performance*. This justification is orientated on the definition of the severity classification given in Ch. 2.2.2.

Within the last three columns a detection method for this failure as well as possible recovery actions to avoid the occurrence of this failure can be defined. To detect a specific failure it is necessary to understand the failure mechanism, so *measurement of energy flow* is evaluated as method. When the failure is detected, the crew must be able to recover the failure, so basic strategies to address it, shall be defined. In this case *system reboot or emergency procedures* seem appropriate. With evaluation of design parameters, herein a possible method to address failure avoidance at early design stage is given. Previously securing the system to avoid the failure can be achieved by *redundancy or a control device*.

The FHA delivers 49 Catastrophic events (CATs) which will be investigated in the next step within the FTA.

		Functions																											
		Energy storage and distribution (ESD)											electric drive system (EDS)									thermal management system (TMS)							
Flight Phase	Failure Condition	measure battery status	provide battery status	control amount of provided electrical energy	provide electrical energy	convert electrical energy	disconnect energy source	expel surplus heat	measure performance of conversion and distribution of electrical energy	measure batterie temperature	save/ store electrical energy	provide battery accesability	invert electrical energy	distribute electrical energy	ensure safe/secure current conversion	transform electrical energy to shaft power	disconnect electrical source	expel surplus heat	provide shaft power	measure electric drive system temperature	measure inverted (alternate) current	provide/ adapt coolant massflow	Adapt Coolant Temperature	Store Coolant	Remove Particles	Measure Coolant Massflow	Measure Coolant Temperature	refill Coolant circuit	control Cooling Circuit
Push Back, Taxi	Degradation of function	HAZ	MIN	MIN	MIN	MIN	MIN	MAJ	MIN	MIN	MIN	TBD	MIN	MIN	MAJ	NSE	MIN	MIN	MIN	NSE	NSE	MIN	MIN	MIN	MIN	MIN	MIN	MIN	MIN
	Inadvertent operation of function	NSE	NSE	CAT	HAZ	MIN	MIN	MIN	NSE	NSE	NSE	TBD	MAJ	MIN	NSE	HAZ	MIN	NSE	HAZ	NSE	NSE	MIN	NSE	NSE	NSE	NSE	NSE	MIN	MAJ
	Incorrect operation of function	HAZ	MIN	HAZ	HAZ	MIN	HAZ	MAJ	MIN	MIN	MIN	TBD	MAJ	MIN	MIN	MAJ	MIN	MIN	HAZ	MIN	MIN	MIN	MIN	MAJ	MAJ	MAJ	MAJ	MIN	MAJ
	partial loss of function	MIN	MIN	HAZ	MIN	MIN	NSE	MAJ	NSE	MIN	MIN	TBD	MIN	MIN	MAJ	NSE	MIN	MIN	MAJ	MIN	MIN	MAJ	MAJ	MAJ	MAJ	MIN	MIN	MAJ	MAJ
	total loss of function	NSE	MIN	CAT	MIN	MIN	CAT	MAJ	NSE	MIN	MIN	TBD	MIN	MIN	MAJ	MIN	MAJ	MIN	MIN	MIN	MIN	MAJ	MAJ	MAJ	MAJ	MIN	MIN	MAJ	MAJ
	unable to stop function	NSE	NSE	CAT	HAZ	NSE	HAZ	NSE	NSE	NSE	NSE	TBD	MAJ	MAJ	NSE	HAZ	MIN	NSE	HAZ	NSE	NSE	MIN	NSE	MIN	NSE	NSE	NSE	MIN	NSE
	asym. Partial loss of function	NSE	NSE	HAZ	MIN	MIN	MIN	MAJ	NSE	MIN	MIN	TBD	MIN	MIN	MIN	MIN	MIN	NSE	MAJ	MIN	MIN	MIN	MIN	MAJ	MIN	MIN	MIN	MIN	MIN
Start, Take off	Degradation of function	MIN	MIN	HAZ	MAJ	MAJ	MAJ	MAJ	MIN	MIN	MIN	NSE	MAJ	MIN	MIN	MAJ	MIN	MIN	MIN	NSE	MIN	MIN	MAJ	MIN	MIN	MIN	MIN	MIN	MIN
	Inadvertent operation of function	NSE	NSE	MAJ	MAJ	NSE	HAZ	MIN	MIN	MIN	MIN	NSE	HAZ	MIN	MIN	HAZ	CAT	NSE	NSE	NSE	NSE	MIN	NSE	NSE	NSE	NSE	NSE	NSE	MIN
	Incorrect operation of function	MIN	MAJ	HAZ	MAJ	HAZ	CAT	MAJ	MIN	HAZ	MAJ	NSE	HAZ	MAJ	MIN	HAZ	CAT	MAJ	MIN	CAT	HAZ	HAZ	HAZ	MAJ	MIN	MAJ	HAZ	MIN	CAT
	partial loss of function	MIN	MIN	HAZ	HAZ	HAZ	MIN	MAJ	MIN	MIN	HAZ	NSE	CAT	MAJ	MIN	CAT	HAZ	HAZ	HAZ	HAZ	HAZ	HAZ	HAZ	MAJ	MIN	MAJ	MAJ	MIN	MAJ
	total loss of function	MIN	MIN	CAT	CAT	CAT	HAZ	HAZ	MIN	MIN	CAT	NSE	CAT	HAZ	MIN	CAT	CAT	CAT	CAT	CAT	HAZ	CAT	HAZ	HAZ	MAJ	MAJ	HAZ	MAJ	CAT
	unable to stop function	NSE	NSE	MAJ	NSE	NSE	CAT	NSE	NSE	NSE	NSE	NSE	MAJ	MIN	NSE	MAJ	CAT	NSE	MIN	NSE	NSE	MIN	NSE	NSE	NSE	NSE	NSE	MIN	MIN
	asym. Partial loss of function	NSE	MIN	HAZ	MIN	HAZ	MIN	MAJ	MIN	NSE	HAZ	NSE	HAZ	MAJ	MIN	HAZ	HAZ	HAZ	HAZ	MAJ	MAJ	MAJ	MIN	MAJ	MIN	MIN	MAJ	MIN	MIN

Figure 4.3 Excerpt of FHA Initial Assessment



Functional Hazard Analysis								Safety Requirements		
Function	**Phase**	**Failure Scenario**	**Failure effects**	**Failure condition**	**Severity/ classification**	**corrected Classification**	**Justification for classification**	**detection**	**recovery action**	**Design parameter**
control amount of provided electrical energy	Push Back, Taxi	uncontroled dynamic motion, high voltage on touchable parts	Effect on Aircraft: - possible damage Effect on Crew/Personnel/ Passengers: - serious injury possible Effect on other Systems: - possible short circuits/ overload	Inadvertent operation of function	CAT	HAZ	serious injury possible, significant decrease of safety,decrease in crew performance	measurement of energy flow	system reboot, emergency procedures	redundant control device
control amount of provided electrical energy	Push Back, Taxi	no movement due to no energy flow, aircraft stops at taxi	Effect on Aircraft: - aircraft not controlable Effect on Crew/Personnel/ Passengers: - increased workload Effect on other Systems: - possible short circuit/overload	total loss of function	CAT	MAJ	decrease of safety margin	functional control of energy flow in start procedure	system reboot, emergency procedures	redundant control device
control amount of provided electrical energy	Push Back, Taxi	uncontroled dynamic motion, possible colision	Effect on Aircraft: - possible damage Effect on Crew/Personnel/ Passengers: - light inuries possible Effect on other Systems: - possible short circuits/ overload	unable to stop function	CAT	HAZ	possible injuries, increase flight crew workload, reduction of safety margin	functional control of energy flow in start procedure	system reboot, emergency procedures	redundant control device
control amount of provided electrical energy	Start, Take off	Engine inoperative, loss of thrust/lift	Effect on Aircraft: - possible loss of A/C Effect on Crew/Personnel/ Passengers: - serious injury Effect on other Systems: - possible short circuits/ overload	total loss of function	CAT		loss of A/C, seriously injured occupants	functional control of energy flow in start procedure	system reboot, emergency procedures	redundant control device
control amount of provided electrical energy	Climb	incorrect production of thrust/lift, stalling/fluttering	Effect on Aircraft: - significant safety reduction/ possible loss Effect on Crew/Personnel/ Passengers: - serious injury Effect on other Systems: - possible short circuits/ overload	Incorrect operation of function	CAT		loss of A/C, seriously injured occupants	warn signals, pre flight check	system reboot, emergency procedures	redundant control device
control amount of provided electrical energy	Climb	incorrect thrust/lift production of engine, possible loss of engine	Effect on Aircraft: - possible loss Effect on Crew/Personnel/ Passengers: - significant increased workload Effect on other Systems: - possible short circuits/ overload	total loss of function	CAT		loss of A/C, increased workload for flight crew, loss of occupants	warn signals, pre flight check	system reboot, emergency procedures	redundant control device
control amount of provided electrical energy	Descent	incorrect thrust/lift production of engine, possible loss of engine	Effect on Aircraft: -possible heavy damage/loss Effect on Crew/Personnel/ Passengers: - significant increase of workload of flight crew - serious injury possible Effect on other Systems: - possible short circuits/ overload	total loss of function	CAT		loss of A/C, increased workload for flight crew, loss of occupants	warn signals, loss of engine power	system reboot, emergency procedures	redundant control device

Figure 4.4 Excerpt of FHA Evaluation

4.3 Fault Tree Analysis (FTA)

To conduct the FTA on the one hand an initial system design is necessary to define the connection of basic events and components, on the other hand the corresponding failure rates of the considered components/events are required for a quantitative result. Appendix A provides a list with all failure rates used in this investigation.

To display and conduct these FTAs the open source program *TopEvent FTA* is used. This program provides different calculation methods which consider different approaches on system reliability. A consistent calculation method according Eq. 2.2 was chosen.

Output of this analysis are several fault trees for single component failures but also fault trees for as catastrophic classified function failures. Fig. 4.4a shows a basic connection of parts and events for a specific function of the TMS. The redundant control unit for the TMS is AND-connected, which means, that for a complete controller failure both units have to fail. Mathematically spoken it means both failure probabilities are multiplied. They are OR-connected with the events for each TMS-circuit, which is linked to the failure tree displayed for one circuit in Fig. 4.4b. This failure tree calculates the probability for one circuit providing wrong condition signals. Within the OR-connection all events are added up, as only one of them leads to the top level event. Depending on the fault tree connections the availability of the top level event (here: *Incorrect circuit control*) is calculated. This value needs to satisfy the probability term of the previously performed FHA.

In case the top level availability does not satisfy the probability term, there are several strategies to improve the reliability/availability within a FTA:

- Hard Time Maintenance events
- Condition Monitoring
- Improvement of used components (Failure rate)
- Redundancy of critical component

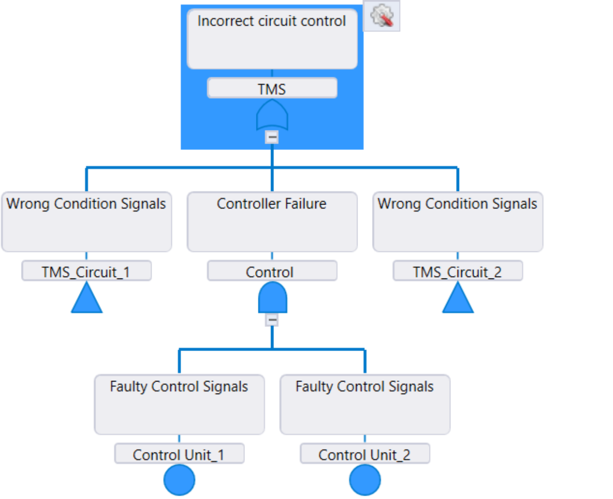
Following, these strategies shall be explained.

Those components not satisfying the safety requirements can theoretically be replaced by a component with a lower failure rate which improves the reliability of the whole function, depending on the component's influence on it. However, this presupposes that several components with different failure rates are available. In this work, for the usage of components with improved reliability, these failure rates need to be lower than those of the optimization methods.

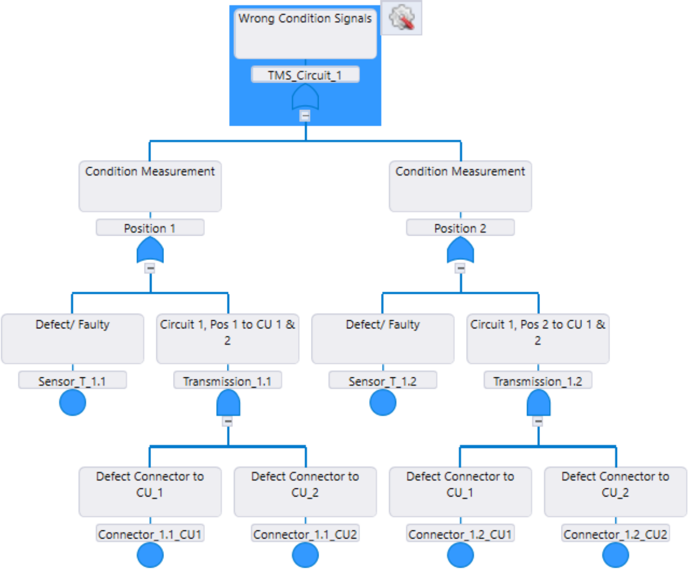
4.3.1 Optimization with Condition Monitoring

To conduct the FTA so that the safety requirement is satisfied several components need to be improved. Next to choosing a better failure rate, it can be improved by monitoring it's condition continuously or in periods. From a conducted FTA it can be seen, which component does not satisfy the required availability or reduces the availability of the considered top level event. Improving this special component is aim of the CM by the approach as follows.

Schildt et al. [33] describes the usage of Probability of Detection (POD) to evaluate the capabilities of CM on the failure mode of a component. This 90/95 POD means "that for a detectable fault of a certain degree, there is a 95% confidence that 90% of the faults will be detected" [33, p. 10], which is the general assumption for a standard maintenance procedure. With integration of a CM it is assumed that the POD increases from 90% to 95%. Thus, the POD factors can be calculated according Eqs. 4.1 and 4.2:



(a) FTA Example: TMS - Incorrect Control



(b) FTA TMS Circuit-Wrong Condition Signals

Figure 4.4 FTA Example

$$POD_{90/95} = 0.90 \cdot 0.95 = 0.855 \tag{4.1}$$

$$POD_{95/95} = 0.95 \cdot 0.95 = 0.9025 \tag{4.2}$$

Using a CM aims on improving the probability of the considered fault tree by improving the availability of the specific component. This means that the corresponding failure rate of this component must be decreasing due to the CM. Eq. 4.3 describes the mathematical approach for that.

$$\lambda_{CM} = \lambda_{Part} \cdot (1 - POD_{95/95}) \tag{4.3}$$

According [33] λ_{CM} is the product of λ_{Part} and the POD so the equation was chosen based on following considerations:

- With a 100% reliable CM, detecting every fault, the POD would equal 1 which would lead to λ_{CM} decreasing to zero according Eq. 4.3
- With a 0% reliable CM, not detecting any fault, the POD would equal 0 which would lead to λ_{CM} equal λ_{Part} according Eq. 4.3

Accordingly, the chosen equation delivers a resilient calculation method for improving the failure rate of a condition monitored component. With λ_{CM} the FTA can be conducted again, so that the failure probability Q of the top level event should be decreasing. Ideally with this increased failure rate the safety requirement of the corresponding fault tree can be satisfied. Basically this method can be used for each component that does not satisfy the requirements without making clear statement regarding the practicability of a CM nor economical properties, for example to monitor a component with huge effort while it would be easier to replace it.

Considering the example from Fig. 4.4a and Fig. 4.4b this calculation method had been used for improvement of the temperature sensor, which is the most probability-decreasing component of the fault tree.

$$\lambda_{CM,Sensor} = 1,7 \cdot 10^{-6} \cdot (1 - 0,9025) = 1,6575 \cdot 10^{-7} \tag{4.4}$$

Eq. 4.4 displays the calculation of the failure rate, improved through CM. The structure of the fault tree does not change, but the improved failure rate, used for the sensor, decreases the top level probability. For both circuits the probability of *Wrong Condition Signals* decreases from $3,4000 \cdot 10^{-6}$ to $3,3150 \cdot 10^{-7}$. Even though the probability term required for the top level event is not satisfied.

Tab. 4.2 shows in the upper part the results for the CM optimization for the limiting components of the conducted FTAs. In column *Improved Fault Tree Probability* the corresponding probability with the improved failure rate of the limiting component is listed.

4.3.2 Optimization with Hard Time Event

With integration of a discard task it is assumed that the replaced component can be considered as *new* so that it's availability is 100%. The interval for replacement is chosen depending on it's failure rate. Therefore Eq. 2.2 is rearranged to "t" and F(t) is defined as 20%. This means that the failure probability is reduced and can equal a maximum of 20% before it is replaced again. Fig. 4.5 displays the original failure probability curve (blue), t_{MTBF} is the time at which with 63,2% probability the considered component has failed. The point at which the curve crosses the previously defined 20% is considered as the discard interval t_{DI}.

Rearranging Eq. 2.2 to λ and λ_N and put them into relation delivers Eq. 4.5. Reducing and transforming of this equation provides Eq. 4.6 and therewith a new improved failure rate λ_N for evaluation in an improved FTA. The decreased failure rate shall lead to a decreased failure probability of the top level event. A very similar approach was used by Bozoudis et al. [8] in their work.

$$\frac{\lambda}{\lambda_N} = \frac{(-1/t_{MTBF}) \cdot ln(1-0,632)}{(-1/t_{MTBF}) \cdot ln(1-0,2)} \tag{4.5}$$

$$\lambda_N = 0,2238 \cdot \lambda \tag{4.6}$$

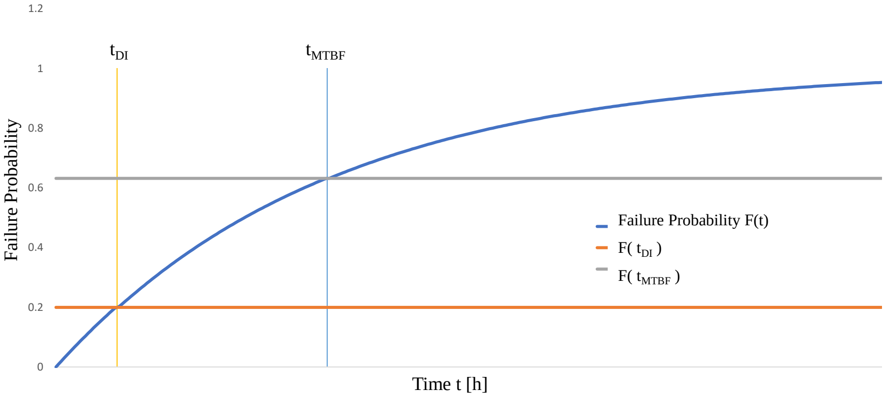


Figure 4.5 FTA Hard Time Optimization

$$\lambda_N = 0,2238 \cdot 1,7 \cdot 10^{-6} = 3,8046 \cdot 10^{-7} \tag{4.7}$$

This approach has been used to calculate an improved failure rate according Eq. 4.7 for the most critical component of the FTA displayed in Fig. 4.4b, which is the temperature sensor. As described in Ch. 4.3.1 the failure rate of the sensor has been replaced by the calculated one, to improve the probability of the *Wrong Condition Signals* event. As before, the probability decreases, from $3,4000 \cdot 10^{-6}$ to $7,6092 \cdot 10^{-7}$. Including the improved failure rate provides a lower failure probability for each circuit, but the top level probability still not matches the required probability term of 10^{-9}.

The bottom part of Tab. 4.2 displays the results for the optimization with a discard event for the probability-decreasing components of the conducted FTAs. Again, in column *Improved Fault Tree Probability* the corresponding probability for the fault tree after using the improved failure rate is listed.

4.3.3 FTA Redundancy

Those fault trees, not satisfying the requirements through a more reliable component, a CM or a discard task had to be extended with a redundant component. This was the case for the FTA example of the TMS, so that an additional temperature sensor with the basic failure rate had to be integrated at each measurement point. The corresponding fault tree structure can be seen in Fig. 4.6. Consecutively the top level probability fulfills the requirements and is lower than 10^{-9}.

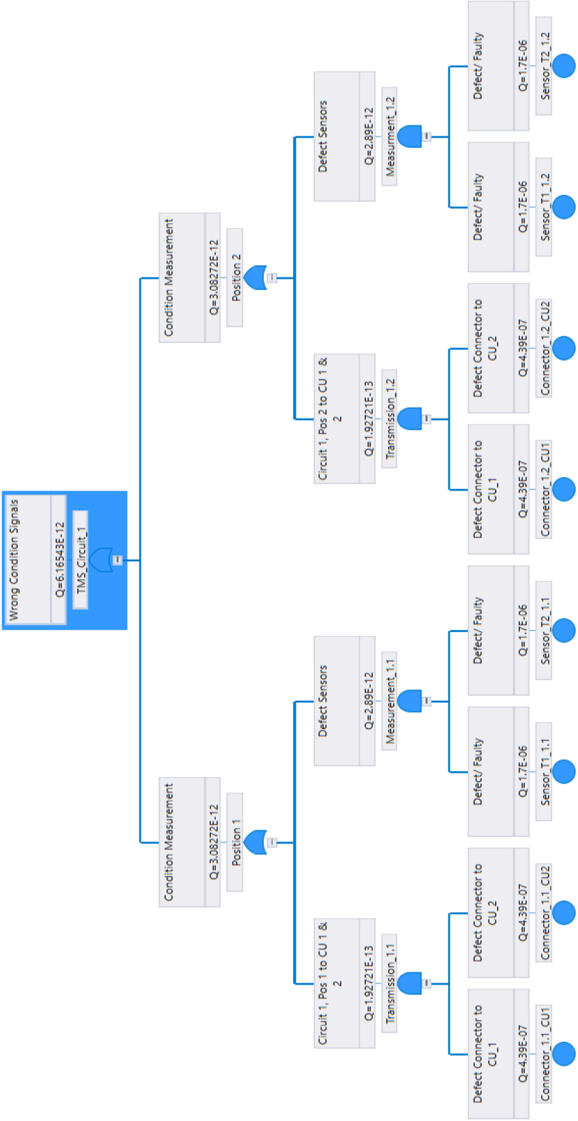


Figure 4.6 FTA TMS Circuit-added redundancy

4.3.4 FTA Summary

Within this work the FTA is used to ensure the required classification determined by the FHA for each function evaluated as Catastrophic event (CAT). In a first step each function was investigated according the in Ch. 3.1.2 described layout for a single circuit. For some components a separate fault tree was built, so that it's failure conditions depending on it's usage is addressed. In the second step these fault trees were extended to the complete system, including all associated circuits. The corresponding results are displayed in Tab. 4.1.

Table 4.1 FTA Initial Function Results

Document	Function	Failure Condition	Failure Rate
FTA Battery 01	provide electric energy	total loss of function	$1.7347 \cdot E - 10$
FTA BMS 01	control amount of provided electrical energy	incorrect operation of function	$3.2334 \cdot E - 10$
FTA BMS 02	control amount of provided electrical energy	total loss of function	$3.9405 \cdot E - 16$
FTA Circuit Breaker ESD 01	disconnect energy source	inadvertent operation of function	$2.9214 \cdot E - 06$
FTA Circuit Breaker ESD 02	disconnect energy source	total loss of function	$2.6062 \cdot E - 14$
FTA Converter 01	convert electrical energy	total loss of function	$9.5413 \cdot E - 11$
FTA TMS 01	provide/ adapt coolant massflow	total loss of function	$1.5147 \cdot E - 09$
FTA TMS 03	control cooling circuit	incorrect operation of function	$6.8000 \cdot E - 06$
FTA Motor EDS 01	transform electrical energy to shaft power	partial loss of function	$1.1756 \cdot E - 10$
FTA Motor EDS 02	transform electrical energy to shaft power	total loss of function	$5.8779 \cdot E - 11$
FTA Inverter EDS 01	invert electrical energy	partial loss of function	$2.2890 \cdot E - 08$
FTA Inverter EDS 02	invert electrical energy	total loss of function	$1.3105 \cdot E - 16$
FTA Shaft EDS 01	provide shaft power	total loss of function	$1.5441 \cdot E - 12$
FTA Circuit Breaker EDS 01	disconnect energy source	inadvertent operation of function	$2.9214 \cdot E - 06$
FTA Circuit Breaker EDS 02	disconnect energy source	total loss of function	$2.6062 \cdot E - 14$

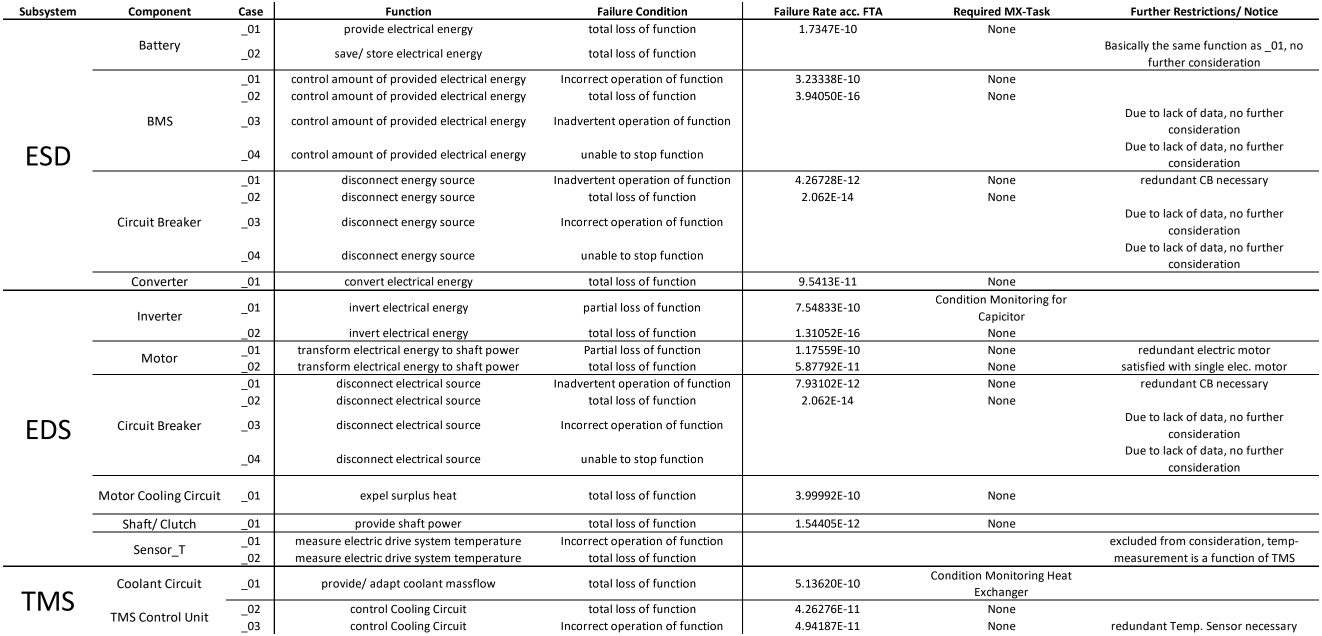
For those FTAs that not satisfy the safety requirements, what means that the top level probability is higher than 10^{-9}, in the next step an optimization is necessary. The third step includes the three optimization approaches described in Ch. 4.3.2 and 4.3.1 and 4.3.3 or usage of a component with improved failure rate. Components that limit the top level probability are chosen for improvement by either a CM or by including a discard maintenance task. Tab. 4.2 shows the result of these approaches, together with a statement regarding it's usage in the column *Note*.

Table 4.2 FTA Optimization Results

Document	Component	Failure Rate	Improved Failure Rate	Improved Fault Tree Probability	Task	Note
			$\lambda_{Part,CM}$	P_{CM}		
FTA Inverter EDS 01	Capacitor	$9.7000 \cdot E-05$	$9.4575 \cdot E-06$	$7.4583 \cdot E-10$	CM Capacitor	possible?
FTA Circuit Breaker ESD 01	Circuit Breaker	$1.4607 \cdot E-06$	$1.4242 \cdot E-07$	$2.8484 \cdot E-07$	CM CircBreak	possible?
FTA Circuit Breaker EDS 01	Circuit Breaker	$1.4607 \cdot E-06$	$1.4242 \cdot E-07$	$2.8483 \cdot E-07$	CM CircBreak	possible?
FTA TMS 03	Sensor_{Temp}	$1.7000 \cdot E-06$	$1.6575 \cdot E-07$	$6.6304 \cdot E-07$	CM Sensor_{Temp}	possible?
FTA TMS 01	Heat Exchanger	$3.8717 \cdot E-06$	$3.7749 \cdot E-07$	$5.1362 \cdot E-10$	CM Heat Exchanger	
			$\lambda_{Part,DIS}$	P_{DIS}		
FTA Inverter EDS 01	Capacitor	$9.7000 \cdot E-05$	$2.1709 \cdot E-05$	$2.0070 \cdot E-09$	DIS Capacitor	practical?
FTA Circuit Breaker ESD 01	Circuit Breaker	$1.4607 \cdot E-06$	$3.2690 \cdot E-07$	$6.5380 \cdot E-07$	DIS CircBreak	practicable?
FTA Circuit Breaker EDS 01	Circuit Breaker	$1.4607 \cdot E-06$	$3.2690 \cdot E-07$	$6.5381 \cdot E-07$	DIS CircBreak	practicable?
FTA TMS 03	Sensor_{Temp}	$1.7000 \cdot E-06$	$3.8046 \cdot E-07$	$1.5219 \cdot E-06$	DIS Sensor_{Temp}	
FTA TMS 01	Heat Exchanger	$3.8717 \cdot E-06$	$8.6649 \cdot E-07$	$5.3134 \cdot E-10$	DIS Heat Exchanger	expensive

Where these approaches not satisfy the safety requirements a redundancy was added. Due to lack of data several functions for which the FTA would be the same but would only differ in the failure condition of considered items, events and correspondingly their failure rates, haven been excluded from this investigation. With all other FTAs successfully conducted, the structure, the connections and the amount of the required components to ensure the failure probability are defined.

The results of the investigations as well as the neglected functions and the reference to their exclusion are summarized in Fig. 4.7. Additional any necessary maintenance implication identified in the third step of each FTA is given.



Subsystem	Component	Case	Function	Failure Condition	Failure Rate acc. FTA	Required MX-Task	Further Restrictions/ Notice
ESD	Battery	_01	provide electrical energy	total loss of function	1.7347E-10	None	
		_02	save/ store electrical energy	total loss of function			Basically the same function as _01, no further consideration
	BMS	_01	control amount of provided electrical energy	Incorrect operation of function	3.23338E-10	None	
		_02	control amount of provided electrical energy	total loss of function	3.94050E-16	None	
		_03	control amount of provided electrical energy	Inadvertent operation of function			Due to lack of data, no further consideration
		_04	control amount of provided electrical energy	unable to stop function			Due to lack of data, no further consideration
	Circuit Breaker	_01	disconnect energy source	Inadvertent operation of function	4.26728E-12	None	redundant CB necessary
		_02	disconnect energy source	total loss of function	2.062E-14	None	
		_03	disconnect energy source	Incorrect operation of function			Due to lack of data, no further consideration
		_04	disconnect energy source	unable to stop function			Due to lack of data, no further consideration
	Converter	_01	convert electrical energy	total loss of function	9.5413E-11	None	
EDS	Inverter	_01	invert electrical energy	partial loss of function	7.54833E-10	Condition Monitoring for Capicitor	
		_02	invert electrical energy	total loss of function	1.31052E-16	None	
	Motor	_01	transform electrical energy to shaft power	Partial loss of function	1.17559E-10	None	redundant electric motor
		_02	transform electrical energy to shaft power	total loss of function	5.87792E-11	None	satisfied with single elec. motor
	Circuit Breaker	_01	disconnect electrical source	Inadvertent operation of function	7.93102E-12	None	redundant CB necessary
		_02	disconnect electrical source	total loss of function	2.062E-14	None	
		_03	disconnect electrical source	Incorrect operation of function			Due to lack of data, no further consideration
		_04	disconnect electrical source	unable to stop function			Due to lack of data, no further consideration
	Motor Cooling Circuit	_01	expel surplus heat	total loss of function	3.99992E-10	None	
	Shaft/ Clutch	_01	provide shaft power	total loss of function	1.54405E-12	None	
	Sensor_T	_01	measure electric drive system temperature	Incorrect operation of function			excluded from consideration, temp-measurement is a function of TMS
		_02	measure electric drive system temperature	total loss of function			
TMS	Coolant Circuit	_01	provide/ adapt coolant massflow	total loss of function	5.13620E-10	Condition Monitoring Heat Exchanger	
	TMS Control Unit	_02	control Cooling Circuit	total loss of function	4.26276E-11	None	
		_03	control Cooling Circuit	Incorrect operation of function	4.94187E-11	None	redundant Temp. Sensor necessary

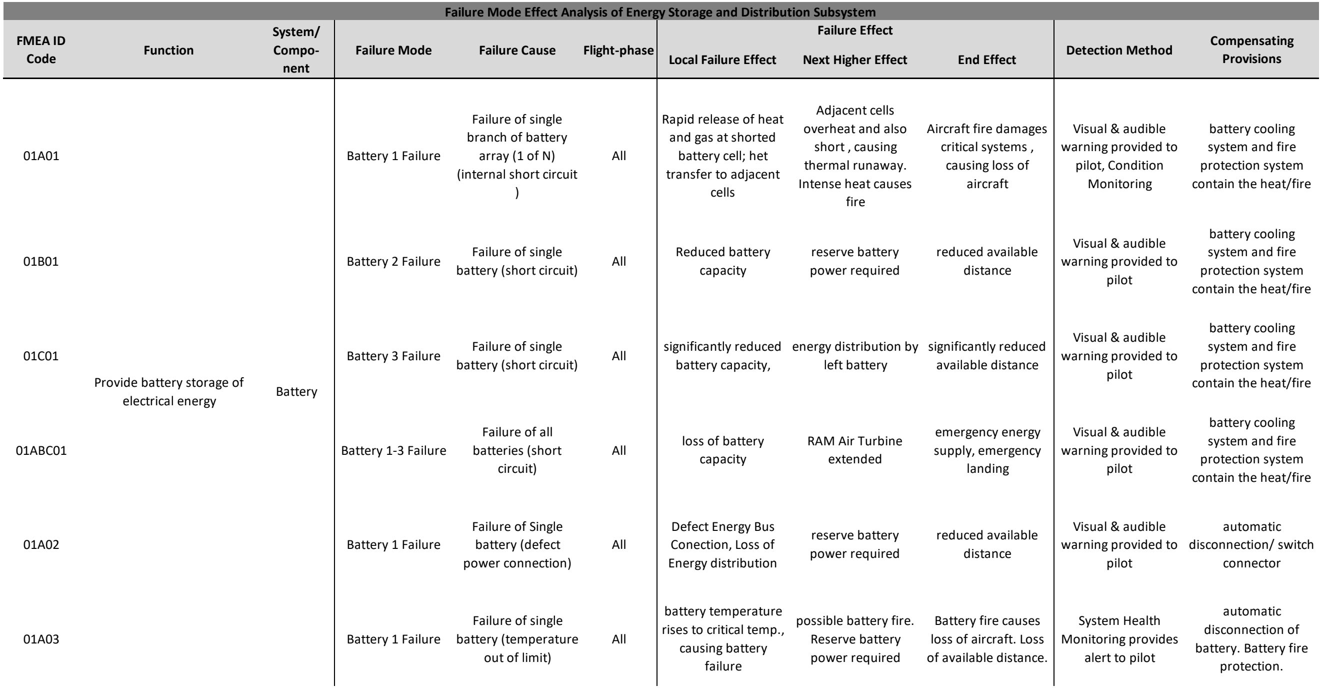
Figure 4.7 FTA Results of Catastrophic event (CAT)

4.4 Failure Mode and Effects Analysis (FMEA)

ARP 4761 provides a very rough investigation layout, so that other layouts with more significance would be preferred. Literature research showed different layouts ([23], [7], [6]) of which the approach of Beidermann et al. [6] is the one with the most informative value. Their analysis includes a criticality assessment which has been omitted here. The chosen layout is displayed in Fig. 4.8.

The FMEA was conducted for the ESD subsystem only and is used to get an impression on the information required and generated by this analysis. As failure modes are equal for the same components, multiple listing is omitted to reduce the scope of the analysis. Within the FMEA combinations of failure modes resulting from the Common Cause Analysis (CCA) can be analyzed in more detail. As the CCA was not performed in this work there are no results to include.

The FMEA assess the failure modes classified during the FHA for components of the model evaluated. With increasing requirement on accuracy, the level of required engineering judgment increases. Thus, for an initial system design approach, the level of detail is kept simple. The different failure causes are oriented on the events and items of each component investigated within the FTA. The FMEA delivers for each failure cause the cascading failure effects and provides additionally an adequate detection method and compensating provisions. This analysis provides a possible starting point for condition monitoring or measurement of relevant condition variables for an in-flight warning system. Further, possible regulation methods to keep a safe state is given as well.



Failure Mode Effect Analysis of Energy Storage and Distribution Subsystem										
FMEA ID Code	Function	System/ Compo-nent	Failure Mode	Failure Cause	Flight-phase	Failure Effect			Detection Method	Compensating Provisions
						Local Failure Effect	Next Higher Effect	End Effect		
01A01	Provide battery storage of electrical energy	Battery	Battery 1 Failure	Failure of single branch of battery array (1 of N) (internal short circuit)	All	Rapid release of heat and gas at shorted battery cell; het transfer to adjacent cells	Adjacent cells overheat and also short , causing thermal runaway. Intense heat causes fire	Aircraft fire damages critical systems , causing loss of aircraft	Visual & audible warning provided to pilot, Condition Monitoring	battery cooling system and fire protection system contain the heat/fire
01B01			Battery 2 Failure	Failure of single battery (short circuit)	All	Reduced battery capacity	reserve battery power required	reduced available distance	Visual & audible warning provided to pilot	battery cooling system and fire protection system contain the heat/fire
01C01			Battery 3 Failure	Failure of single battery (short circuit)	All	significantly reduced battery capacity,	energy distribution by left battery	significantly reduced available distance	Visual & audible warning provided to pilot	battery cooling system and fire protection system contain the heat/fire
01ABC01			Battery 1-3 Failure	Failure of all batteries (short circuit)	All	loss of battery capacity	RAM Air Turbine extended	emergency energy supply, emergency landing	Visual & audible warning provided to pilot	battery cooling system and fire protection system contain the heat/fire
01A02			Battery 1 Failure	Failure of Single battery (defect power connection)	All	Defect Energy Bus Conection, Loss of Energy distribution	reserve battery power required	reduced available distance	Visual & audible warning provided to pilot	automatic disconnection/ switch connector
01A03			Battery 1 Failure	Failure of single battery (temperature out of limit)	All	battery temperature rises to critical temp., causing battery failure	possible battery fire. Reserve battery power required	Battery fire causes loss of aircraft. Loss of available distance.	System Health Monitoring provides alert to pilot	automatic disconnection of battery. Battery fire protection.

Figure 4.8 Excerpt of the FMEA

5 Results

5.1 Developed System Layout

With determined functions from the FBA, classified within the FHA, the safety requirements can be derived, so that the system design can be evaluated through the FTA. Iterative conduction of the FTA, using different optimization approaches, delivers the necessary amount and structure of components.

The investigation of the ESD-functions delivers the necessity of three redundant BMSs and batteries and two converters to satisfy the safety requirements. Equally, the EDS-functions deliver the demand for two inverters per circuit and two electrical motors. Air cooling, ensured by 2 redundant fans per EDS-circuit, is selected for motor cooling. Further, the FTA shows the need for redundant circuit breaker in both ESD and EDS. Within the conduction of the analysis, decisions on the connection of components to each other are taken. For the signal transfer the controlling units are connected with a signal BUS. The energy flow is distributed via the energy transfer DC-BUS to the inverters. Via the AC-BUS the alternate current is distributed to the motor.

The figures 5.1 and 5.2 display the results of the safety analyses. According to safety requirements, necessary redundancies have been included as well as necessary components to provide all defined functions. Chapman et al. [9] describes for state of the art technology that there are temperature limits to ensure a high efficiency. This concerns mainly battery, converter and inverter. These components are highlighted with a red colored background in Fig. 5.1. In Fig. 5.2 these components are summarized into the red box labeled with *EPS*.

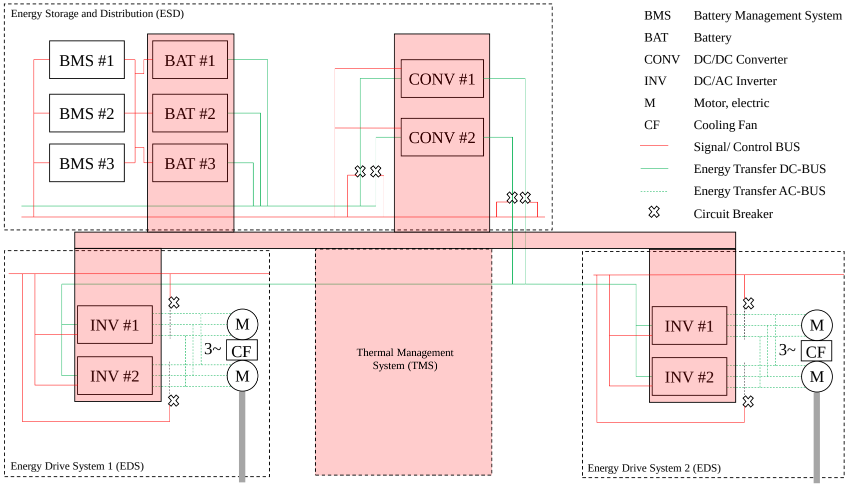


Figure 5.1 EPS Initial Design Approach on scale of A320

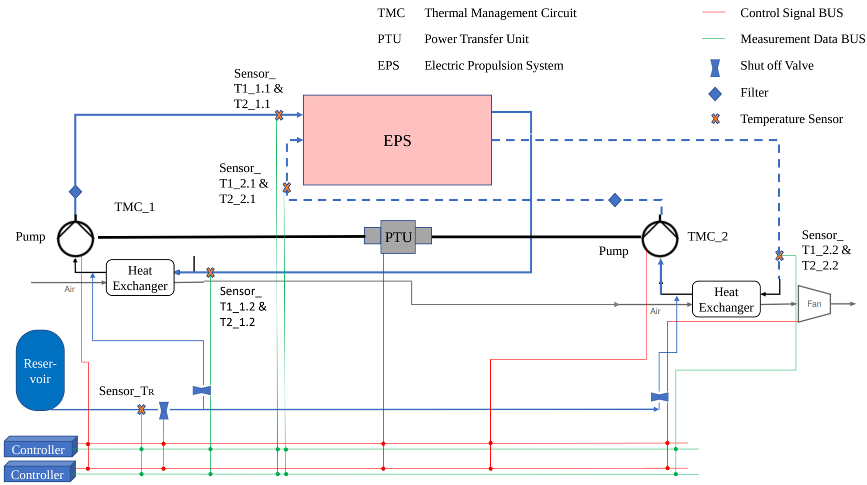


Figure 5.2 TMS Initial Design Approach on scale of A320

As stated before, the EPS is divided in three subsystems, each framed by a dashed line, of which the Electric Drive System (EDS) consists of two circuits, one for each engine. An other specialty is that the TMS is connected to each subsystem providing the coolant flow individually for each component that requires cooling.

5.2 Estimation of upcoming maintenance

The battery-electric propulsion system is attended to completely replace the kerosene based propulsion system. Accordingly all components and subsystems necessary for storage and distribution of kerosene are omitted from maintenance consideration. This includes for example the tanks, tank nozzles, pipes, valves and fuel conditioning devices. With exclusion of these components, the corresponding maintenance tasks can be excluded as well. On the other side, many new components have to be integrated with the new EPS design. Further, the three subsystems developed in this work require other physical attention and maintenance than a kerosene based system. For a maintenance optimized system design, a low amount of physical and scheduled tasks is aspired. The battery requires a condition monitoring to continuously measure the capacity and trend of the battery condition. To ensure proper function of the batteries, a functional check on a scheduled basis can be necessary. During the conduction of the safety analysis (FTA), for two components maintenance tasks have been included in the certification process. According to Fig. 4.7, this includes two additional CM tasks. On the one hand for the capacitor of each inverter in the EDS and on the other, for the heat exchanger of the TMS. These tasks are mandatory and so they have to be included in the Airworthiness Limitation Section (ALS). For the EDS it can be assumed that rotating components like the motor, it's cooling fans, shaft and clutch have to be investigated for wear out. This leads to servicing tasks and possible restoration. In advance, functional checks for several components, like circuit breakers or components integrated as passive load path, can be expected. Additionally, the system underlies a certain degradation through vibrations, temperature cycles, humidity and other influences.

6 Conclusions and Outlook

This work identified a simplified approach to develop and evaluate an initial Electric Propulsion System (EPS) layout depending on regulations given by EASA. System-intended functions as well as several safety requirements had been classified, whereby assumptions and possibilities for simplification had been made. These assumptions lead to several limitations of the outcome. To satisfy the outlined safety requirements of the chosen approach, several maintenance implications had been evaluated and used. Accordingly, an initial design of necessary components and their structure had been derived. Further, the corresponding amount of maintenance compared to a conventional kerosene based propulsion system had been estimated. Advantage of this work is a better understanding of the design stages, at which decisions towards maintenance were made. So at these points the system design can be influenced with the aim of a maintenance optimized design.

This initial system design demonstrate just a first iteration point from which all analyses will be conducted again for improvement of efficiency and reliability. Within the next iteration, functions classified as HAZ, MAJ or MIN can also be evaluated in more detail. Also the TMS requires a more detailed investigation regarding the necessary coolant provision for each component. With reduction of simplifications and an iteration of the chosen analyses the system design can be improved, so that additional functions and accordingly necessary components can be identified. In a next step, the developed system design can also be used for a detailed maintenance calculation like the MSG-3 analysis. The work in general can be used as a basic approach for developing new propulsion systems and evaluate the corresponding integration. Additionally, it provides a method for integrating maintenance tasks in early design phases.

Bibliography

[1] A. Abu Kasim, M. Chan, and E. J. Marek. “Performance and failure analysis of a retrofitted Cessna aircraft with a Fuel Cell Power System fuelled with liquid hydrogen.” In: *Journal of Power Sources* 521 (2022), p. 230987. ISSN: 03787753. DOI: 10.1016/j.jpowsour.2022.230987.

[2] A. Ahmadi, P. Söderholm, and U. Kumar. “On aircraft scheduled maintenance program development.” In: *Journal of Quality in Maintenance Engineering* 16.3 (2010), pp. 229–255. ISSN: 1355-2511. DOI: 10.1108/13552511011072899.

[3] J. Ahn et al. “Performance and availability of a marine generator-solid oxide fuel cell-gas turbine hybrid system in a very large ethane carrier.” In: *Journal of Power Sources* 399 (2018), pp. 199–206. ISSN: 03787753. DOI: 10.1016/j.jpowsour.2018.07.103.

[4] Airbus. *Component Heat Map Report*. 2023.

[5] M. A. Anker, C. Hartmann, and J. K. Nøland. *Feasibility of Battery-Powered Propulsion Systems for All-Electric Short-Haul Commuter Aircraft*. 2023. DOI: 10.36227/techrxiv.23634597.v1.

[6] A. Beidermann and P. R. Darmstadt. “Hazard Analysis Failure Modes, Effects, and Criticality Analysis for NASA Revolutionary Vertical Lift Technology Concept Vehicles.” In: *Proceedings of the 77th Annual Forum And Technology Display*. Ed. by Vertical Flight Society. Virtual, 2021.

[7] A. Birolini. *Reliability Engineering*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2017. ISBN: 978-3-662-54208-8. DOI: 10.1007/978-3-662-54209-5.

[8] M. Bozoudis, I. Lappas, and A. Kottas. “Use of Cost-Adjusted Importance Measures for Aircraft System Maintenance Optimization.” In: *Aerospace* 5.3 (2018), p. 68. DOI: 10.3390/aerospace5030068.

[9] J. W. Chapman, H. Hasseeb, and S. L. Schnulo. “Thermal Management System Design for Electrified Aircraft Propulsion Concepts.” In: *AIAA Propulsion and Energy 2020 Forum*. Reston, Virginia: American Institute of Aeronautics and Astronautics, 2020. ISBN: 978-1-62410-602-6. DOI: 10.2514/6.2020-3571.

[10] EASA. *Certification Specification for Large Aeroplanes (Amendment 28): CS-25*. 2023.

[11] M. Fadaeefath Abadi et al. “Fault Identification and Fault Impact Analysis of The Vapor Compression Refrigeration Systems in Buildings: A System Reliability Approach.” In: *Energies* 15.16 (2022), p. 5774. DOI: 10.3390/en15165774.

[12] Federal Aviation Administration. *Certification Maintenance Requirements: AC 25-19A*. 2011.

[13] K. Fischer, K. Pelka, and J. Walgern. “Trends and Influencing Factors in Power-Converter Relaibility of Wind Turbines.” In: *PCIM Europe*. Berlin and Offenbach: VDE Verlag GmbH, 2023. ISBN: 978-3-8007-6091-6.

[14] K. Fischer et al. “Reliability of Power Converters in Wind Turbines: Exploratory Analysis of Failure and Operating Data From a Worldwide Turbine Fleet.” In: *IEEE Transactions on Power Electronics* 34.7 (2019), pp. 6332–6344. ISSN: 0885-8993. DOI: 10.1109/TPEL.2018.2875005.

[15] S. de Graaf and S. Kazula. "Development of a Controls Approach for Fuel Cell-Powered All-Electric Aero Engines based on an FHA." In: *ICAS Proceedings 33th Congress of the ICAS*. Ed. by International Council of the Aeronautical Sciences. Virtual, 2022.

[16] S. Gradel, B. Aigner, and E. Stumpf. "Model-based safety assessment for conceptual aircraft systems design." In: *CEAS Aeronautical Journal* 13.1 (2022), pp. 281–294. ISSN: 1869-5582. DOI: 10.1007/s13272-021-00562-2.

[17] B. Han, L. Zhu, and Y. Jiang. "Candidate Certification Maintenance Requirement Analysis and Certification Practice." In: *Procedia Engineering* 80 (2014), pp. 17–25. ISSN: 18777058. DOI: 10.1016/j.proeng.2014.09.055.

[18] M. Hinsch. *Industrielles Luftfahrtmanagement*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2022. ISBN: 978-3-662-66451-3. DOI: 10.1007/978-3-662-66452-0.

[19] F. Jäger and O. Bertram. *Development of a Safe Powertrain System Architecture for the HorizonUAM Air Taxi Concept*. 2022.

[20] F. Jäger et al. "Battery-Electric Powertrain System Design for the HorizonUAM Multirotor Air Taxi Concept." In: *CEAS Aeronautical Journal*. Ed. by CAES. 2024.

[21] A. Janssen, D. Makareinis, and C.-E. Solver. "International Surveys on Circuit-Breaker Reliability Data for Substation and System Studies." In: *IEEE Transactions on Power Delivery* 29.2 (2014), pp. 808–814. ISSN: 0885-8977. DOI: 10.1109/TPWRD.2013.2274750.

[22] S. Kazula, S. de Graaf, and L. Enghardt. "Preliminary Safety Assessment of PEM Fuel Cell Systems for Electrified Propulsion Systems in Commercial Aviation." In: *Book of Extended Abstracts for the 32nd European Safety and Reliability Conference*. Ed. by M. C. Leva et al. Singapore: Research Publishing Services, 2022, pp. 2613–2620. ISBN: 978-981-18-5183-4. DOI: 10.3850/978-981-18-5183-4{\textunderscore}S16-02-019-cd.

[23] D. Kritzinger. *Aircraft system safety: Assessments for initial airworthiness certification*. Woodhead Publishing in mechanical engineering. Duxford, United Kingdom: Woodhead Publishing, 2016. ISBN: 978-0-08-100889-8.

[24] D. Lapesa Barrera. *Aircraft Maintenance Programs*. 1st ed. 2022. Springer Series in Reliability Engineering. Cham: Springer International Publishing and Imprint Springer, 2022. ISBN: 978-3-030-90262-9. DOI: 10.1007/978-3-030-90263-6.

[25] M. C. Noviello et al. "Aeroelastic Assessments and Functional Hazard Analysis of a Regional Aircraft Equipped with Morphing Winglets." In: *Aerospace* 6.10 (2019), p. 104. DOI: 10.3390/aerospace6100104.

[26] Quanterion Solutions Incorporated. *Quanterion Automated Databook (NPRD-2016, FMD-2016, EPRD-2014)*. New York, NY, 2014.

[27] M. K. Rahmat and S. Jovanovic. "Reliability modelling of uninterruptible power supply systems using fault tree analysis method." In: *European Transactions on Electrical Power* 19.2 (2009), pp. 258–273. ISSN: 1430-144X. DOI: 10.1002/etep.211.

[28] A. Ristow et al. "Development of a Methodology for Improving Photovoltaic Inverter Reliability." In: *IEEE Transactions on Industrial Electronics* 55.7 (2008), pp. 2581–2592. ISSN: 0278-0046. DOI: 10.1109/TIE.2008.924017.

[29] SAE. *ARP4754A Guidelines for Development of Civil Aircraft and Systems*. Warrendale, PA, USA, 2010.

[30] SAE. *ARP4761 Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airbone Systems and Equipment*. Warrendale, PA, USA, 1996.

[31] SAE International. *SAE International – Advancing Mobility Knowledge and Solutions*. vitual, 2024.

[32] S. Sahoo, X. Zhao, and K. Kyprianidis. "A Review of Concepts, Benefits, and Challenges for Future Electrical Propulsion-Based Aircraft." In: *Aerospace* 7.4 (2020), p. 44. DOI: 10.3390/aerospace7040044.

[33] P. Schildt, C. Braun, and P. Marzocca. "Metric evaluating potentials of condition-monitoring approaches for hybrid electric aircraft propulsion systems." In: *CEAS Aeronautical Journal* 11.1 (2020), pp. 177–190. ISSN: 1869-5582. DOI: 10.1007/s13272-019-00411-3.

[34] K. W. See et al. "Critical review and functional safety of a battery management system for large-scale lithium-ion battery pack technologies." In: *International Journal of Coal Science & Technology* 9.1 (2022). ISSN: 2095-8293. DOI: 10.1007/s40789-022-00494-0.

[35] X. Shu et al. "A Detailed Reliability Study of the Motor System in Pure Electric Vans by the Approach of Fault Tree Analysis." In: *IEEE Access* 8 (2020), pp. 5295–5307. DOI: 10.1109/ACCESS.2019.2963197.

[36] F. Spertino et al. "Reliability Analysis and Repair Activity for the Components of 350 kW Inverters in a Large Scale Grid-Connected Photovoltaic System." In: *Electronics* 10.5 (2021), p. 564. DOI: 10.3390/electronics10050564.

[37] W. J. C. Verhagen et al. "Condition-Based Maintenance in Aviation: Challenges and Opportunities." In: *Aerospace* 10.9 (2023), p. 762. DOI: 10.3390/aerospace10090762.

[38] A. Wilken et al. "Hybrid Electric Propulsion Systems for Medium-Range Aircraft from a Maintenance Point of View." In: *Deutscher Luft- und Raumfahrtkongress 2023, Stuttgart*. Ed. by Deutsche Gesellschaft für Luft- und Raumfahrt - Lilienthal-Oberth e.V. Bonn: Deutsche Gesellschaft für Luft- und Raumfahrt - Lilienthal-Oberth e.V., 2023. DOI: 10.25967/610084.

[39] P. J. Wilkinson and T. P. Kelly. "Functional hazard analysis for highly integrated aerospace systems." In: *IEE Certification of Ground/Air Systems Seminar*. IEE, 1998, p. 4. DOI: 10.1049/ic:19980312.

[40] W. Wu et al. "Electromechanical Actuator Cooling Fan Reliability Analysis and Safety Improvement." In: *SAE Technical Paper Series*. SAE Technical Paper Series. SAE International400 Commonwealth Drive, Warrendale, PA, United States, 2016. DOI: 10.4271/2016-01-1997.

List of Figures

2.1 V-Model . . . 3
2.2 FTA Operators . . . 4
2.3 Bathtub-Curve . . . 7

3.1 EPS Design . . . 11

4.1 Interaction Diagram . . . 14
4.2 Excerpt of Use Case Diagram . . . 15
4.3 Excerpt of FHA Initial Assessment . . . 17
4.4 Excerpt of FHA Evaluation . . . 18
4.4 FTA Example . . . 20
4.5 FTA Hard Time Optimization . . . 22
4.6 FTA TMS Circuit-added redundancy . . . 23
4.7 FTA Results of Catastrophic event (CAT) . . . 27
4.8 Excerpt of the FMEA . . . 29

5.1 EPS Initial Design Approach . . . 30
5.2 TMS Initial Design Approach . . . 31

List of Tables

2.1 Failure Condition Classification 5

4.1 FTA Initial Function Results 24
4.2 FTA Optimization Results 25

A1 Failure Rates for FTA 39

Appendix A

Table A1 Failure Rates for FTA

Component/ Event	**Failure Rate λ**	**Data Source**
Battery	$9{,}31{\cdot}10^{-5}$	[20]
Battery Modules	$2{,}85{\cdot}10^{-6}$	[35]
Battery Cell	$2{,}40{\cdot}10^{-6}$	[38]
Battery Fastening Screw	$1{,}02{\cdot}10^{-6}$	[38]
BMS	$5{,}29{\cdot}10^{-6}$	[35]
DC/DC Converter	$2{,}30{\cdot}10^{-6}$	[1]
Converter	$2{,}04{\cdot}10^{-6}$	[26]
Converter Cooling, liquid	$2{,}19{\cdot}10^{-6}$	[14]
Converter System, liq. cooled	$2{,}37{\cdot}10^{-5}$	[13]
Power Device	$4{,}09{\cdot}10^{-6}$	[38]
Battery Signal Connector	$1{,}76{\cdot}10^{-7}$	[38]
Battery Power Connector	$2{,}96{\cdot}10^{-7}$	[38]
Voltage Sensor	$1{,}80{\cdot}10^{-6}$	[38]
Current Sensor	$2{,}00{\cdot}10^{-6}$	[38]
Temperature Sensor	$1{,}70{\cdot}10^{-6}$	[38]
Heat Exchanger	$1{,}73{\cdot}10^{-5}$	[3]
Battery Cooling Circuit	$5{,}08{\cdot}10^{-4}$	[6]
Coolant Pump	$1{,}21{\cdot}10^{-5}$	[11]
Shut-Off Valve	$3{,}73{\cdot}10^{-6}$	[1]
Control Computer	$6{,}09{\cdot}10^{-6}$	[16]
Filter Failure	$4{,}50{\cdot}10^{-8}$	[27]
Pipe and Tubing	$1{,}40{\cdot}10^{-5}$	[26]
Reservoir	$2{,}00{\cdot}10^{-7}$	[4]
Cooling Fan	$2{,}00{\cdot}10^{-5}$	[40]
Power Transfer Unit	$7{,}48{\cdot}10^{-6}$	[4]
Rotor Defect	$3{,}00{\cdot}10^{-7}$	[35]
Stator Defect	$2{,}52{\cdot}10^{-7}$	[35]
Transducer Defect	$2{,}58{\cdot}10^{-7}$	[35]
Other Motor Defects	$5{,}68{\cdot}10^{-6}$	[35]
Control Modul Defect	$3{,}44{\cdot}10^{-6}$	[35]
Drive Module Defect	$1{,}40{\cdot}10^{-6}$	[35]
Discharging Module Defect	$2{,}70{\cdot}10^{-8}$	[35]
Communication Module Defect	$2{,}83{\cdot}10^{-7}$	[35]
Other Controler Module Defect	$1{,}36{\cdot}10^{-7}$	[35]
Storage Capacitor	$9{,}70{\cdot}10^{-5}$	[28]
Power Stage Driver	$7{,}20{\cdot}10^{-6}$	[28]
Inverter Cooling	$2{,}40{\cdot}10^{-6}$	[28]
Isolation Transformer	$3{,}70{\cdot}10^{-7}$	[28]
Shaft	$2{,}26{\cdot}10^{-8}$	[35]
Clutch	$1{,}22{\cdot}10^{-6}$	[38]
Circuit Breaker, Failure Cases		
Breakdown to Earth	$1{,}71{\cdot}10^{-9}$	[21]
Does not break the current	$6{,}85{\cdot}10^{-9}$	[21]
Breakdown across open pole	$6{,}16{\cdot}10^{-9}$	[21]
Breakdown between poles	$4{,}11{\cdot}10^{-9}$	[21]
Fails to carry the current	$4{,}45{\cdot}10^{-9}$	[21]
Fire/ Damage	$1{,}42{\cdot}10^{-8}$	[21]
Short Circuit	$1{,}00{\cdot}10^{-6}$	[6]
Thermal Runaway	$1{,}00{\cdot}10^{-6}$	[6]