POLITECNICO DI TORINO

Dipartimento di Ingegneria Meccanica e Aerospaziale

Corso di Laurea Magistrale in Ingegneria Aerospaziale

Master's Degree Thesis

Reliability and Safety Assessment of a Thermal Control System of a Hypersonic Transportation Vehicle

Supervisors:

Prof.ssa Ing. Nicole Viola

Co-Supervisors:

Ing. Davide Ferretto

Ing. Roberta Fusaro

Candidate:

Laura Babetto

22 Marzo 2018

A Gas e Tessa

Summary

Index of Figures

Index of Tables

Abbreviations

AIAA	American Institute of Aeronautics and Astronautics
EC	European Community
ECS	Environmental Control System
ES	Electrical System
ESA	European Space Agency
FCS	Flight Control System
FH	Flight Hours
FHA	Functional Hazard Assessment
FMEA	Failure Mode and Effect Analysis
FMECA	Failure Mode, Effect and Criticality
FR	Failure Rate
FRPH	Failure Rate per Hours
FT	Fault Tree
FTA	Fault Tree Analysis
IAEA	International Atomic Energy Agency
HL	Horizontal Landing
HTO	Horizontal Take-Off
LAPCAT	Long-Term Advanced Propulsion Concepts and Technologies
MBSE	Model-Based Systems Engineering
RBD	Reliability Block Diagram
TBC	Thermal Barrier Coating
TCS	Thermal Control System
TEMS	Thermal Energy and Management System
TMS	Thermal Management System

TRL	Technology Readiness Level

Abbreviations (Boolean Equations)

air_not	aeration not present
elec_compr_gas_1	electrical system failure of compressor channel 1
elec_compr_gas_2	electrical system failure of compressor channel 2
elec_pump_liq_1	electrical system failure of pump channel 1
elec_pump_liq_2	electrical system failure of pump channel 2
elec_tempsens	electrical system failure of temperature sensor
hardware_tempsens	hardware errors of temperature sensor
mat_deg_ins_conv	material degradation of gaseous circuit
mat_deg_gas	material degradation of convection walls
mat_deg_ins_rad	material degradation of insulation
mat_deg_passive	material degradation of passive system
mech_compr_2	mechanical failure of compressor channel 1
mech_compr_1	mechanical failure of compressor channel 2
mech_pump_1	mechanical failure of pump channel 1
mech_pump_2	mechanical failure of pump channel 2
mech_reg_gas	heat exchanger failure in gaseous circuit
mech_reg_liq	heat exchanger failure in liquid circuit
other_sens	errors in other sensors of thermal control system
pipes_compr_gas_1	pipes leakages of compressor channel 1
pipes_compr_gas_2	pipes leakages of compressor channel 2
pipes_outflow_gas	pipes leakages of gaseous outflow
pipes_outflow_liq	pipes leakages of liquid outflow

pipes_pump_liq_1	pipes leakages of pump channel 1
pipes_pump_liq_2	pipes leakages of pump channel 2
pipes_reg_gas	pipes leakages of gaseous regenerator
pipes_reg_liq	pipes leakages of liquid regenerator
pressens_compr_gas_1	pressure sensor failure of compressor channel 1
pressens_compr_gas_2	pressure sensor failure of compressor channel 2
pressens_outflow_gas	pressure sensor failure of gaseous outflow
pressens_outflow_liq	pressure sensor failure of liquid outflow
pressens_pump_liq_2	pressure sensor failure of pump channel 1
pressens_pump_liq_1	pressure sensor failure of pump channel 2
pressens_reg_gas	pressure sensor failure of gaseous regenerator
pressens_reg_liq	pressure sensor failure of liquid regenerator
shape_ins_conv	shape degradation of convection walls
shape_ins_rad	shape degradation of insulation
shape_passive_shape	degradation of passive system
software_tempsens	software errors of temperature sensor
radiator_ins_rad	inefficient radiator of insulation
radiator_passive	inefficient radiator of passive system
tank_outflow_gas	tank leakages of gaseous outflow
tank_outflow_liq	tank leakages of liquid outflow
tempsens_outflow_gas	temperature sensor failure of gaseous outflow
vent_boil_off	aeration not present in the boil-off circuit
walls_deg_ins_rad	walls degradation of insulation
walls_deg_passive	walls degradation of passive system
walls_reg_gas	walls degradation of gaseous regenerator
walls_reg_liq	walls degradation of liquid regenerator

Abstract (Italian Version)

Lo scopo di questa Tesi è quello di applicare un metodo sistemistico ("Model-Based Systems Engineering methodology") per effettuare un'analisi di Sicurezza e Affidabilità ("Safety and Reliability Assessment"), durante le fasi preliminari di progetto, su un sottosistema innovativo, installato in un velivolo ipersonico. Il velivolo in questione è l'MR2, sviluppato durante il progetto europeo LAPCAT II e il sottosistema su cui l'analisi verrà applicata è il sistema termico (Thermal and Energy Management System -TEMS-), perché è l'unico elemento di cui sono note le caratteristiche fino a livello di componentistica.

Si tratta di una procedura già nota in ambito aeronautico che, però, opportunamente riadattata, è capace di superare le criticità legate a prodotti all'avanguardia come è il TEMS dell'MR2: non esistono infatti database di dati precisi a sufficienza per concetti così avanzati, sia perché non esistono velivoli simili operativi sia perché il livello di studio è ancora concettuale.

Il contenuto della Tesi è la formalizzazione del metodo (con i suoi vantaggi e svantaggi) e la successiva applicazione della procedura, passo-passo, sul velivolo selezionato per lo studio. Il primo capitolo è focalizzato sulla descrizione teorica del metodo, a partire dai concetti di Systems and Reliability Engineering e si conclude con l'esposizione dell'approccio concreto. Questo approccio è costituito da due parti: una prima parte di analisi qualitativa che segue un andamento top-down e una seconda quantitativa che segue un andamento bottom-up. Nel secondo capitolo sono riportate le caratteristiche principali dell'MR2, concentrate sull'ottimizzazione di aerodinamica e layout, sull'integrazione efficace dei sistemi e sottosistemi e sul profilo di missione innovativo. I successivi tre capitoli sono suddivisi in modo da rendere l'applicazione del metodo il più chiara possibile. Nel terzo capitolo è riportata l'analisi preliminare dell'ambiente in cui sarà operativo il velivolo, derivando gli obiettivi di progetto. Nel quarto capitolo viene effettuata l'analisi funzionale che permette di ricavare le funzionalità che il prodotto deve garantire, che costituiscono poi il punto di partenza per la parte qualitativa dell'analisi di rischio. Nel quinto ed ultimo capitolo viene descritto il procedimento quantitativo che conduce ai risultati numerici finali e alla loro comparazione e validazione come requisiti di sicurezza.

Abstract

The aim of this Thesis is to apply a Model-Based Systems Engineering methodology to perform a Safety and Reliability Assessment, during conceptual design phase, of an innovative on-board subsystem of a hypersonic aircraft. Particularly, the case study is based upon the LAPCAT MR2 concept. The systematic procedure is already well-known and applied in the aeronautical sector, where almost all potential useful data are available: the breakthrough is to conform it to the concept of an hypersonic transportation vehicle, for which precise statistical data does not exist, since the project is at preliminary stage and avant-garde, also considering that no other similar products are operational yet. Hence, in this specific case, the approach will be applied to the advanced Thermal Management System of the vehicle, in detail named as Thermal and Energy Management System, because it is the single sub-system whose design is known up to components level.

The Thesis has been firstly organized to introduce the reader to the formalization of the methodology, with its strong points as well as downsides, then to the application of the approach to the selected case study used as example. The first Chapter is focused on the theoretical description of the main steps of the methodology, starting from the basic concepts related to Systems and Reliability Engineering and concluding with the concrete approach, that will be further applied. This approach consists of a first qualitative analysis carried out following a top-down path and a further quantitative analysis performed with a bottom-up course. In the second Chapter the main features of the MR2 vehicle are summarized, focusing on its optimization concerning the most suitable integration of all the systems and sub-systems, its aerodynamics and layout and, in particular, its unusual mission profile. The other three Chapters are structured to divide the whole method in three reasonable main steps in order to elucidate which is the fundamental line of thinking that has been followed. The third and the fourth Chapters contain the way of thinking that has been applied to identify the project objectives, the design requirements and the risky events, which would occur and would compromise the safety, until the proper level of study. In the final Chapter, the quantitative bottom-up analysis has been performed concluding with numerical results and comparisons related to the safety requirements.

At the end of the Thesis, useful data, diagrams, tables and lists have been attached in order to be consulted: these are heavy documents that could compromise the fluency of the report and for this reason, they have been relegated to the final pages.

It is intended to notice that, technical terms are often used in this Thesis, therefore it is obvious that some formalisms, typical of systems engineering jargon, could appear.

1 MBSE approach for the conceptual design of aerospace products

The aeronautical sector and, consequently, the space one are rapidly developing from an industrial but also academic and technical point of view, always trying to find solutions to raise the net of connections and to reduce the flight time, in order to increase the transportation routes capabilities [1]. In this context, there are new potential and sophisticated vehicles characterized by high level of complexity: this proposes a new challenge for designers to envisage innovative systems, technological solutions and integration of the whole model. There is also another important point, that is the multidisciplinary of this kind of new projects, which implicates much more effort.

For this reason, in this Chapter, a new supporting methodology based upon a Model Based Systems Engineering (MBSE) approach, aimed at reducing risk of inappropriate and wrong design choices or processes and limiting time, costs and effort spent during the development phases of an innovative aerospace concept, is illustrated [1]. The main purpose is indeed to apply this new study methodology as preparatory step for the Safety and Reliability Assessment that must be taken into account during the conceptual design phase, to satisfy strict Safety Requirements of new space missions. The final goal is selecting the most suitable baselines with relevant impact on the final product, that has to show the best performances.

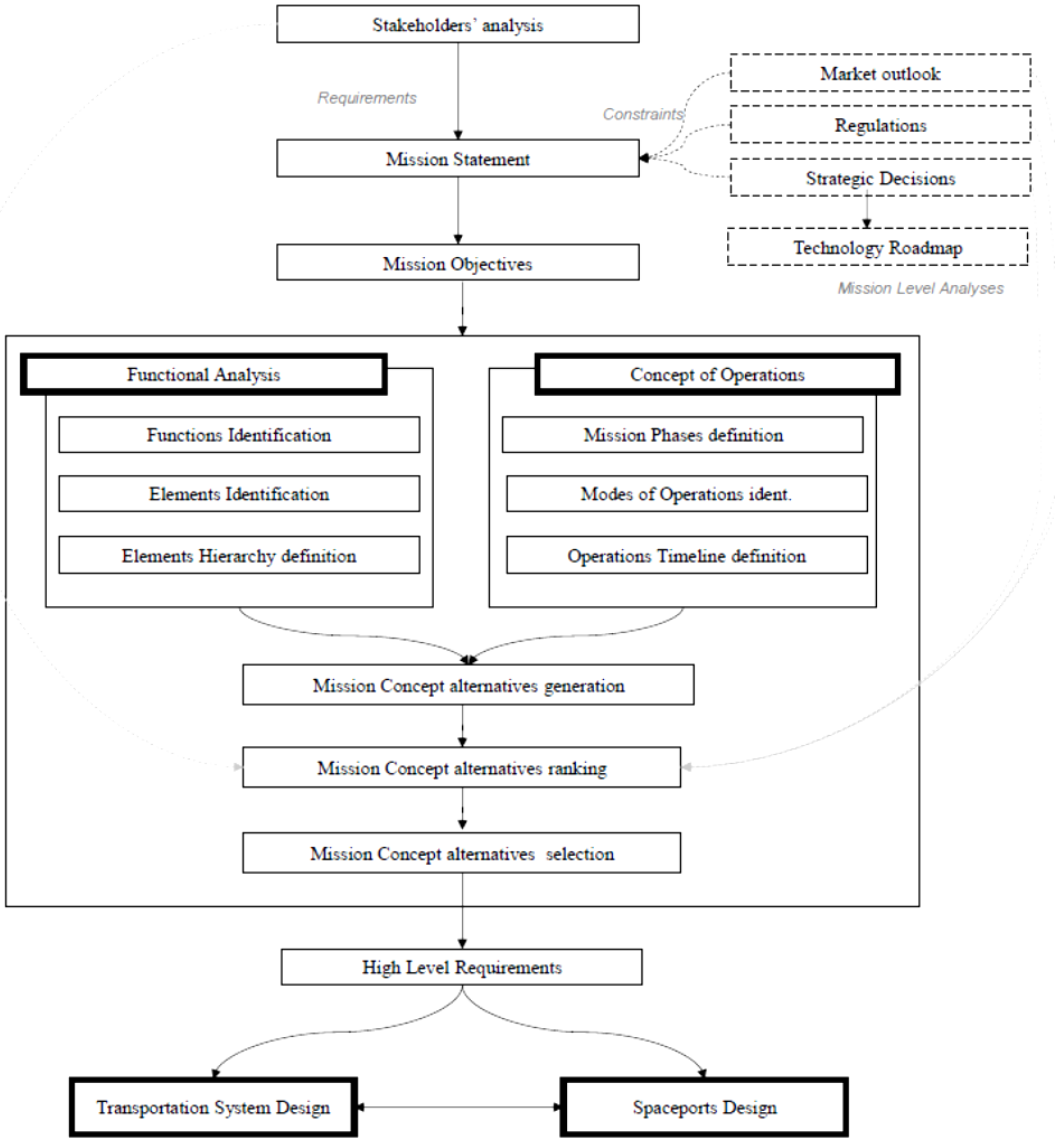


Figure 1.1 Flowchart of the proposed approach [1].

In Section 1.1 the method (schematically illustrated in Figure 1.1) with a step-by-step point of view is theoretically discussed. In the following chapters the methodology will be implemented on the MR2 vehicle, which is an outcome of the European Project LAPCAT, related to the design of a hypersonic transportation vehicle, that will perform commercial flight service.

1.1 Concepts of Safety and Reliability in System Engineering

Before looking closer at the methodology, it is important to remind that, in the Systems Engineering field, a specific "language" related to the Safety Analysis is used, as in the next pages will be illustrated.

In this context, the purpose is to carry out a Safety and Reliability Assessment of an aerospace product during the conceptual design, i.e. trying to identify the hazardous conditions at system, subsystem and components level, and interrelationships between them, to examine the potential risk at a preliminary levels of study.

Actually, every product or process has modes of failure, therefore the role of an analysis of potential non nominal behaviour can help designers to be focused on dangerous conditions, to understand their risky impact on the product itself and people, as well as to prevent malfunctions and hazards.

In this perspective, the key word is *Failure* which is defined as the event causing the lack of required performance and functions of an item, whereas *Fault* is the state of inability to perform what is required. There are many reasons why a product might fail: inappropriate design, overstressing, wearing out, human errors, etc. Each failure is characterized by a different relevance level, all gathered in specific regulations (as shown in Table 1.1).

DESCRIPTION	LEVEL	SPECIFIC INDIVIDUAL ITEM	FLEET OR INVENTORY
Frequent	A	Likely to occur often in the life of an item, with a probability of occurrence greater than 10^{-1} in that life	Continuously experienced
Probable	B	Will occur several times in the life of an item, with a probability of occurrence less than 10^{-1} but greater than 10^{-2} in that life	Will occur frequently
Occasional	C	Likely to occur sometimes in the life of an item, with a probability of occurrence less than 10^{-2} but greater than 10^{-3} in that life	Will occur several times.
Remote	D	Unlikely but possible to occur in the life of an item, with a probability of occurrence less than 10^{-3} but greater than 10^{-6} in that life	Unlikely, but can reasonably be expected to occur
Improbable	E	So unlikely, it can be assumed occurrence may not be experienced, with a probability of occurrence less than 10^{-6} in that life	Unlikely to occur, but possible

Table 1.1 Categorisation of failure levels [2].

According to this, several systematic methods have been developed to quantify the effects of failures in order to ensure product quality, prevent customer dissatisfaction and, obviously, achieve Reliability and Safety standards.

The term *Reliability* refers to the ability of an item to perform a required function under given conditions for a given time interval. In some applications, Reliability is linked to the probability of an event to happen.

The word *Safety* refers to a state of the system where an acceptable level of risk (fatality, damages, injuries, ...) is not overcome and exceeded. A risky situation is an undesirable circumstance that can occur and have negative consequences on a project or product at any time of it: therefore it is important to predict and control the events, in order to mitigate and reduce the likelihood of failure and its consequences.

For this reason, the Reliability Engineering[1] discipline has the task, firstly, to adopt engineering knowledge to prevent and reduce the frequency of failures (for example, studying deeply the architecture, selecting the best components or well-organizing maintenance procedures) and then to correct the causes and to apply methods for the estimation of the Reliability of new designs.

It is a concept that refers not only to aerospace engineering context (as could be the specific case of study discussed here) but to every different application as an effectiveness parameter to evaluate the goodness of a product or process [2].

In conclusion, the objective is to apply an innovative approach focused on Safety and Reliability Assessment, that can overcome the lack of statistical data, typical criticality related to the aerospace sector: the proposed solution comes from the idea that an a-priori technique based on Model Based Systems Engineering Methodology can be an innovative way to take into account Safety at the beginning of the project, keeping in mind that a totally safe product does not exist. Starting with the exploitation of the typical systems engineering tools[1], the methodology then consists in a Safety and Reliability two-steps assessment (qualitative and quantitative) to evaluate the safety level of the whole project through the connection of all the required tools in a homogeneous chain of integrated design tasks.

[1] More details in Appendix A.

The importance of this new approach is that it offers the possibility to evaluate RAMS disciplines through functional and product analyses, interfaced with designated Safety and Reliability Engineering tools such as Functional Hazard Assessment (FHA), Fault Tree Analysis (FTA) and FMECA (see Appendix A).

1.2 Safety and Reliability Assessment Methodology

As mentioned in the previous chapter, the point that makes the purpose really difficult to reach is that similar examples of vehicles, potentially usable for comparisons as well as drivers for the design are not existing. Winged re-entry vehicles are in fact not usable as example, since they are characterized by other design points. The high level of complexity of the entire project requires clarity of the estimated performance of the aircraft from the very first stages of the design, (e.g. the interactions among sub-systems, the consequences on the environment, ...etc) in order to devise innovative design methodologies to reduce potential risk due to wrong and inappropriate ways of thinking. Moreover there are also missing regulations and know-how to direct and interface the project. For these reasons, new limitations and restrictions shall be considered to make this new sort of commercial transport feasible and viable as well as constraints that must be respected to guarantee high level of Safety. As already said, the focus is on the importance of considering Safety at the very beginning of the project assuring the reduction of the risk of the mission related to complex technologies.

1.2.1 The Two-Steps Methodology

The traditional approach (purely statistical) based on database cannot be applied in the case of innovative product because a lot of historical data (coefficients, parameters or criteria), usually adopted, are not available at system and sub-systems [3]. The breakthrough is to propose a two steps methodology characterized by a qualitative top-down process and a quantitative bottom-up one.

The top-down step refers to the functional and physical decomposition of the product itself where Safety and Reliability are evaluated from the top system level (the most general level) to the components one, and it consists in a logical way of thinking. On the other hand, starting from the statistical data available from technical databases at components level plus the results obtained from the previous qualitative procedure, the bottom-up process allows the estimation of top system Safety and Reliability leve. It is significant to underline that it is an iterative and recursive procedure where the two-steps have to be well-integrated each other.

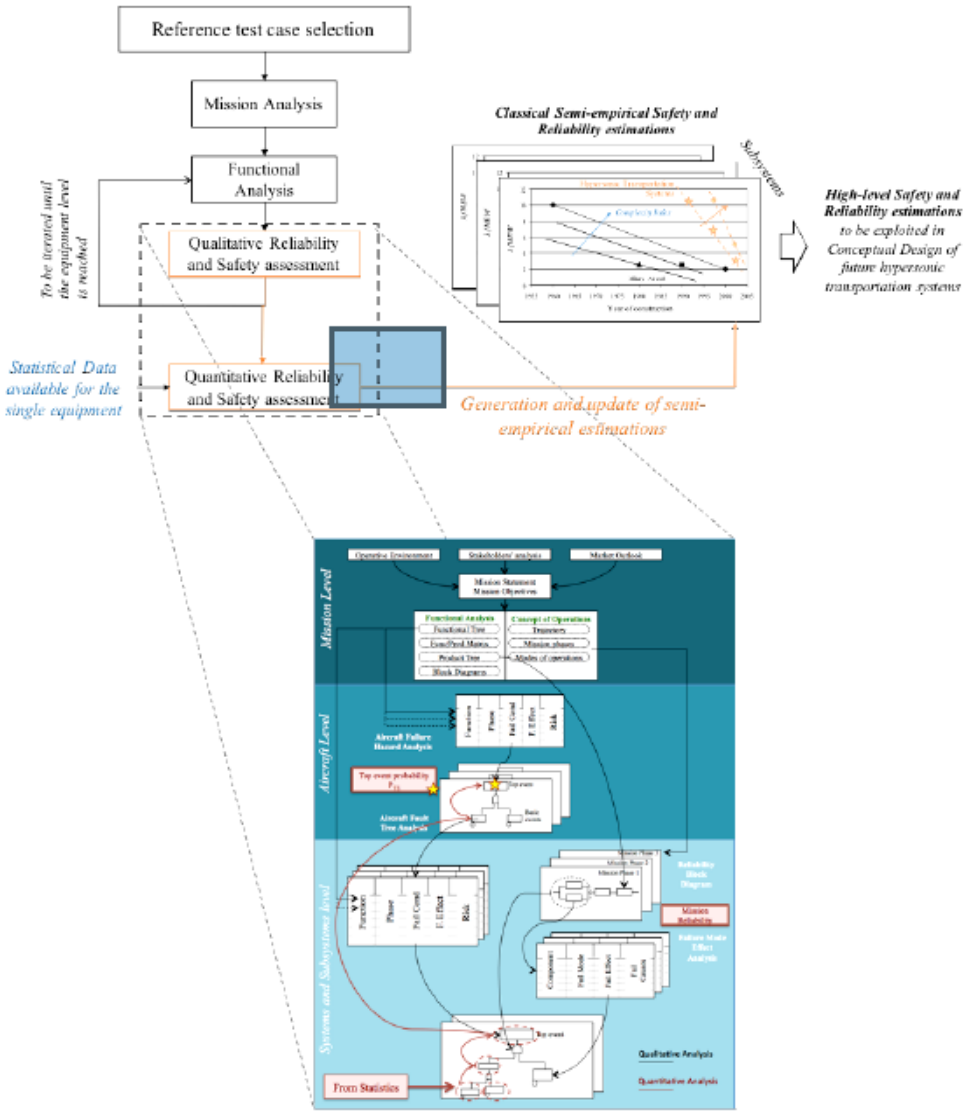


Figure 1.2 Scheme of the methodology [4].

1.2.1.1 The Qualitative Top-Down Approach

The high mission level begins with a market analysis in order to derive which are the needs and the potential innovations "to be launched" and where the applications can assure competitiveness, bringing effective advantages. Concurrently, it is important to derive also the regulations because they act as constraints for the development of the project. In parallel to this, the stakeholders analysis that is the definition and identification of the entities (researchers and university, industries and enterprises, companies, private agencies, ordinary people..., etc,...) which can be interested in developing this topic in every aspect and which are their most relevant foreseeable interests, comes.

After the preliminary analysis of the current market, the regulatory framework and the result of the stakeholders analysis, the Mission Statement (that is a sort of contextualization of the product) and the Mission Objectives can be derived. In a secondary moment the Mission Requirements can be listed as "first draft". There are also a list of Constraints and a list of Programmatic Requirements that are a sort of project schedules useful at the end of the procedure to compare with the final outcomes. At the end of this first part, the relationship between the stakeholders and the objectives is characterized in a more specific way thanks to graphical tools.

All the stakeholders have different purposes, so it is useful to characterize the different interests of the stakeholders and classify them in four most important positions:

- **Sponsors**: the public or private associations which invest in the project;
- **Operators**: engineering associations who want to control and maintain the assets;
- **End-users**: everyone who receives benefits from the project such as scientific or engineering community;
- **Customers**: all the people who really exploit the product [5].

Each stakeholder can assume different positions depending on the interest.

At the end of the analysis, all the elaborated concepts are formalized and gathered in a diagram: the best diagram that yields all these important pieces of information is the "*Use Case Diagram*" where all the actors (the Stakeholders) are properly represented and linked to their specific use cases (the Mission Objectives). Figure 1.3 shows schematically the special symbols used in a Use Case Diagram and Figure 1.4 illustrates a generic example of this scheme [6].

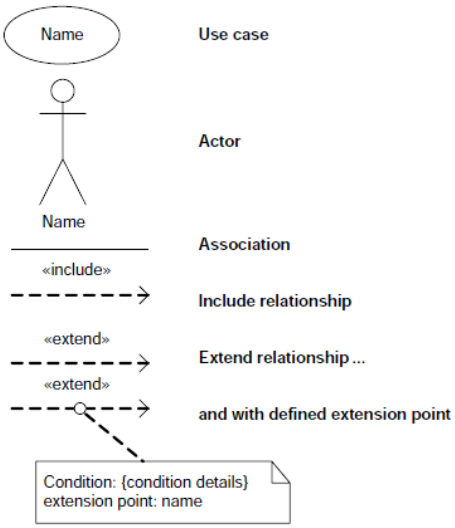


Figure 1.3 Graphical representation of elements of an Use Case Diagram [6].

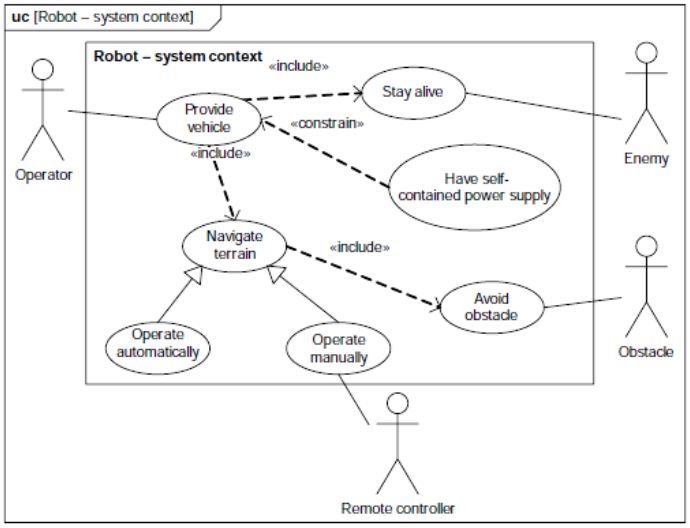


Figure 1.4 Generic example of a Use Case Diagram [6].

It is interesting glancing deeper at the special type of relationships among the elements: to characterize the Stakeholders, the Generalization[2] link is used, while to characterize the different interests the Association link "include" has been chosen, to indicate a relationship between a secondary objective requirement and primary objective requirement: this is a kind of Aggregation-style relation derived from the more general "Association[3]" one [6].

[2] Generalization shows a 'has types' relationship that is used to show "parent and child" blocks.

[3] Association is a simple connection between one or more *Blocks*, characterized by two different specializations: "Aggregation" means "is made up of" while "Composition" means "is composed of".

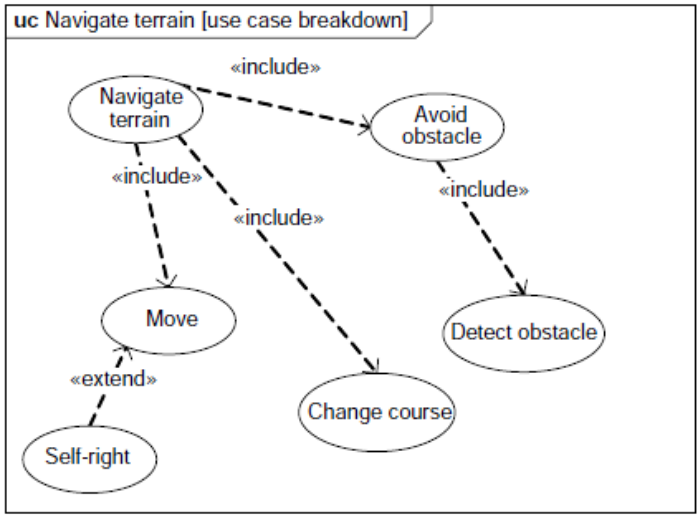


Figure 1.5 Relationship between requirements in a Use Case Diagram [6].

All the data elaborated are gathered into specific diagrams in order to guarantee traceability during the entire product life cycle. The Model-Based approach is also useful to underline the relationships and connections among the elements of the design project: a proper database that records all the relevant statements is created, therefore that formalization allows to immediately verify if requirements are satisfied or not and, in which case it is necessary to think over different choices.

Once this analysis is done, it is time to elaborate the functionalities which best-fit with the mission objectives realization. In fact, the next step is to generate the Functional Tree and to derive Functional Requirements which have to be based on the already declared mission objectives.

The first list of requirements can be populated with particular attention to their semantic [7]. As mentioned before, a Functional Tree can be created using the SysML Block Definition Diagram, as a tool typical of the MBSE approach, to connect the different functions (blocks) graphically and trace them during the design steps: it is an iterative and recursive process, which means each step is a sort of revision of the all procedure.

During this brainstorming, it is important also to reflect on which are the most relevant systems that could satisfy each requirement: in fact, each requirement is *allocated* to a specific product that can fulfil the requisite itself. The next step of the process is to identify indeed the potential products able to perform the previous outlined functions.

To guarantee the optimization, every product can be able to perform more than one function but no vice versa, also because it avoids to mix different hierarchical levels [1]. Moreover, in this phase *functions/products Matrix* can be a usefull tool: this is helpful to allocate each requirement to the expected device. After the development of this matrix, it is easy to draw the Products Tree in parallel to the Functional Tree: the hierarchical level must be the same. The outcome of this step is another diagram, known as Products Diagram, that shows which are the devices involved and which functions is a commitment of which element.

The most significant diagram at this level remains the Functional Tree, not only because it allows deducing which are the products (the equipment and components) that fulfil the requirements, but also because the blocks of the tree contain the input for the following analysis: the Functional Hazard Assessment[4].

This tool is useful to classify the failure conditions related to the functional architecture at the proper level of study and diversify the risk associated to the loss of those functions, according to some considerations (such as the consequences of the failure and the phase of the mission in which it occurs. This is an important aspect because it is the starting point to derive the lower level Safety Requirements. As said above, the FHA is carried out to classify all the potential failure conditions related to each outlined function that the aerospace product has to perform. Looking at all the functions at system level, the process consists of gathering the hazardous circumstances for each mission phase, evaluating the effects on the product and then, linking the cited level of risk to each case. This level of risk is given in order to identify which are the most dangerous events.

Generally, there are two levels of FHA: the first is performed at system level and the latter at sub-system level but the procedure is approximately the same. Each identified condition in the FHA becomes the starting point to perform the Fault Tree Analysis, FTA[5] : this means that each failure is the top event of a Fault Tree.

The whole Fault Tree is the result of a deductive approach of thinking. The idea is to investigate which could be the causes of the top event, focusing on a functional point of view, following the research of potential intermediate events and then concluding with components basic events. The relevant aspect of a Fault Tree is that it offers and displays immediate qualitative information about combinations of undesired events.

[4] For more details, see Appendix A.
[5] For more details, see Appendix A.

From the failure events is then possible to derive new lower level functions and then, a parallel with the Products Tree can be done, before sketched, to obtain a new point of view on these failure conditions and their relation with the way the system operates. The result will be a FT focused on device failures point of view.

The basic events of the Fault Tree become the one's complement of the functionalities of a lower level of study and the process restarts with a lower level FHA.

The final step consists in performing the Failure Modes, Effects and Criticality Analysis, FMECA[6]: this tool is useful for listing the potential critical events to the system due to failures or malfunctions at components level.

In the same way explained above, it is possible to deduce the potential causes of each hazard and, with an iterative procedure, to evaluate the severity of the whole system from the equipment failure events. The process ends when the failure effects derived with FMECA are the basic events of the final FT. In this sense, it would be useful to reach a proper level of structural and functional decomposition up to components in order to allow to assign numerical probabilistic values (as failure rates λ is) to each element and then to estimate the aircraft level failure rate, proceeding with the bottom-up approach.

This activity is the first part of the quantitative approach described in the following section.

1.2.1.2 The Quantitative Bottom-up Approach

The main purpose of this approach is deriving the value of the failure rate at aircraft level, starting from the likelihood of malfunctions of the basic components identified during the previous analysis. This aim is allowed only performing an accurate research through statistical databases about the potential failure events of the equipment: each failure rate must be associated to the specific component depending on its feature.

After having elaborated the probability equation and having solved it, it is possible to proceed with the bottom-up procedure starting with the data previously gathered and to evaluate the failure rate of the top event of the FTA up to aircraft level [4]. The quantitative bottom-up approach is highlighted in Figure 1.6 with the red colour.

[6] For more details, see Appendix A.

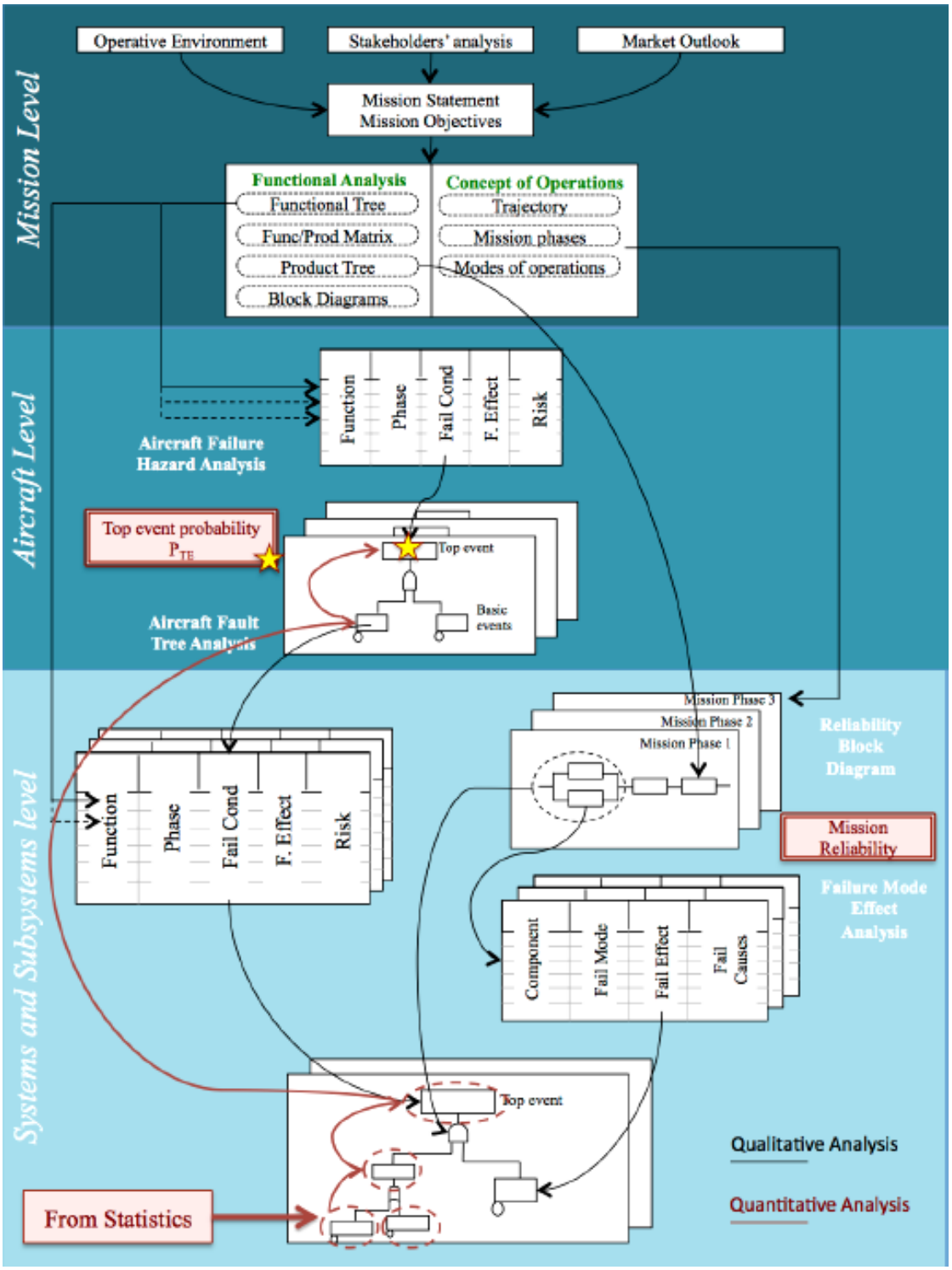


Figure 1.6 Scheme of whole methodology [4].

The explanation of the whole methodology as it has been already pointed out, is proposed within the preliminary design of a hypersonic vehicle, in particular evaluating the Safety level of an innovative Thermal Management System that will be installed on the aircraft described in Chapter 2.

2 Case of Study: the Lapcat Project and the MR2 vehicle

In this context, the Long-Term Advanced Propulsion Concepts and Technologies Project, known as the European LAPCAT II Project (2008-2013), promoted, as principal objective, the research about new kinds of transportation vehicles able to sustain hypersonic flight, in order to reduce long distance civil routes.

Figure 2.1 The symbolic logo of the project. [8]

Achieving this goal means new flight regime for commercial transport, and in other words, operations across *new* speeds and *new* altitudes. Hence, traditional turbo-jet engines are not usable and they must be replaced by innovative air-breathing technologies: the point of the project was, therefore, the realization of a new propulsion unit appropriately integrated with the whole aircraft system [8].

In fact, the LAPCAT II project aim was to design a hypersonic transportation vehicle able to fly at Mach 8 and board at least 300 passengers across antipodal routes in less than 3 hours.

According to this purpose, there are a lot of challenges to face:

- Reaching an appropriate aero-propulsive balance;
- Achieving sufficient engine performance for critical phase such as acceleration and cruise;
- Multi-cycle propulsion system to operate across the full speed range;
- Efficient structural design (robust high temperature materials and fluid thermal structural interactions to manage);
- Innovation of control system at hypersonic speed;
- Economic viability.

This context includes the MR2 vehicle which is foreseen to overcome these strict hurdles.

Figure 2.2 The MR2 vehicle [9].

The MR2 concept is based upon the optimization of systems integration and performance, in particular between propulsion unit and aerodynamic efficiency, guaranteeing volume for tanks and storage fuel, payload and all the required subsystems. It is important to underline that, the final vehicle is the result of multiple iterative procedures of optimizations and in the following pages its relevant features are introduced [10].

2.1 MR2 Concept

The fundamental idea is that the vehicle can perform hypersonic flight from Europe to Australia, that means approximately an antipodal route, over the North Pole, following the Bering Strait and avoiding inhabited lands. This is one of the main characteristic of this vehicle: in fact, it cannot fly over classical trajectories because it generates a relevant sonic boom (that is a critical point that acts as constraint for the project).

It is also interesting to know that the phases before the hypersonic cruise consume around 45% of the fuel mass: the first part of the route is constituted of climb, subsonic cruise and two acceleration phases that require considerable fuel mass [9]. It is expected, the flight Brussels-Sydney consumes all the available propellant; on the other side, landing in a closer airport, such as Tokyo or Los Angeles means less flight time and also less propellant consuming but clearly, these routes are not optimized [9].

Figure 2.3 View of the complete trajectory [10].

2.1.1 Mission profile

The entire scenario is divided in specific phases characterized by different speed, altitude and manoeuvres and here will be discussed the fundamental features.

The horizontal take-off is performed at 150m/s to ensure lift-off speed, lift-off manoeuvre and acceleration. It is probable that new airport will be necessary to guarantee the take-off and they will have to be located approximately 400km far from the coast. To face this constraint, the design has envisaged a second phase that consists in a subsonic cruise at Mach 0.95 for around 240km in order to distance the coast plus to reach proper altitude and speed to start the acceleration phases. In fact, next step is the turbojet first acceleration phase up to Mach 4, followed by the second acceleration phase, that is a ramjet acceleration up to Mach 8 using Dual Mode Ramjet (and deactivating Air Turbo Ramjet): the acceleration is limited to $3m/s^2$ to guarantee passengers comfort. As mentioned above, avoiding inhabited lands, the hypersonic cruise is performed over arctic regions and across the Bering Strait to reach Sydney International Airport, which distances 15200km at an altitude of 32-35km. The final unusual phase is an unpowered descent, without consuming fuel, and a final horizontal landing: the profile mission is shown in Figure 2.4 [10].

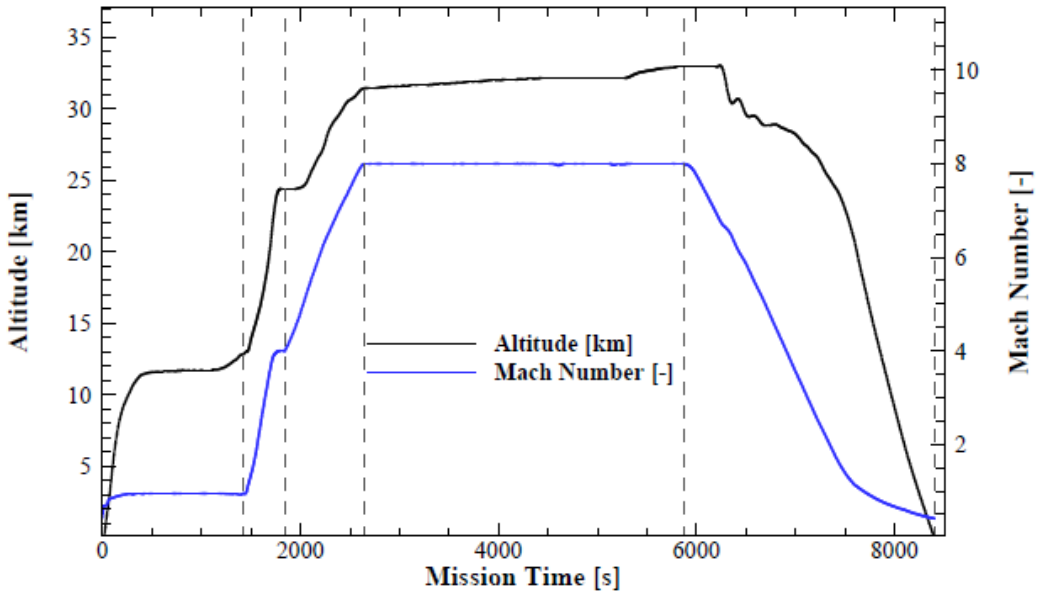


Figure 2.4 Flight Altitude and Flight Mach Number vs. Mission Time [10].

In conclusion, here the mission phases are summarized:

- Take-off in Brussels and subsonic cruise;

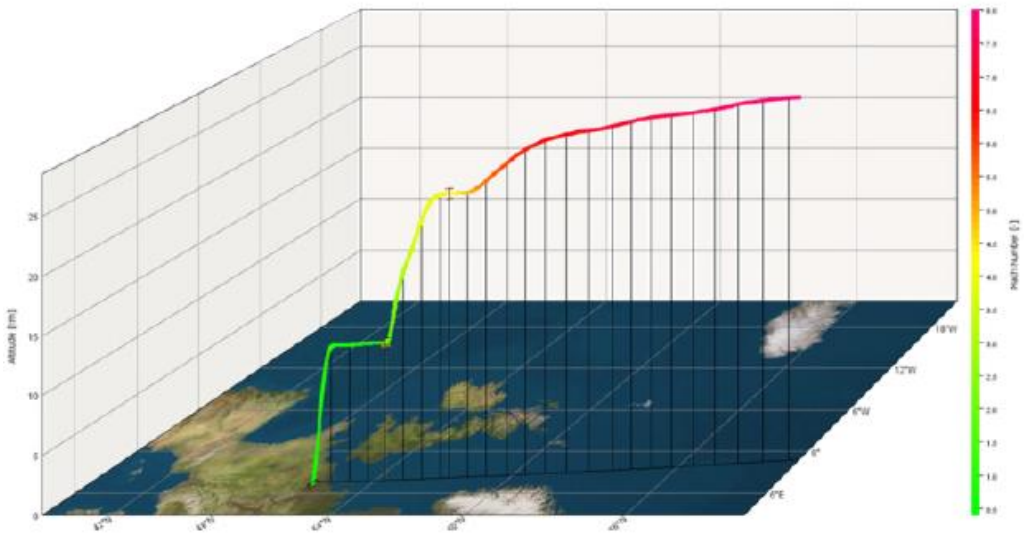


Figure 2.5 Take-off in Brussels and initial subsonic cruise between Norway and Britain [10].

- First and second acceleration up to Mach 8;
- Hypersonic cruise across arctic regions;

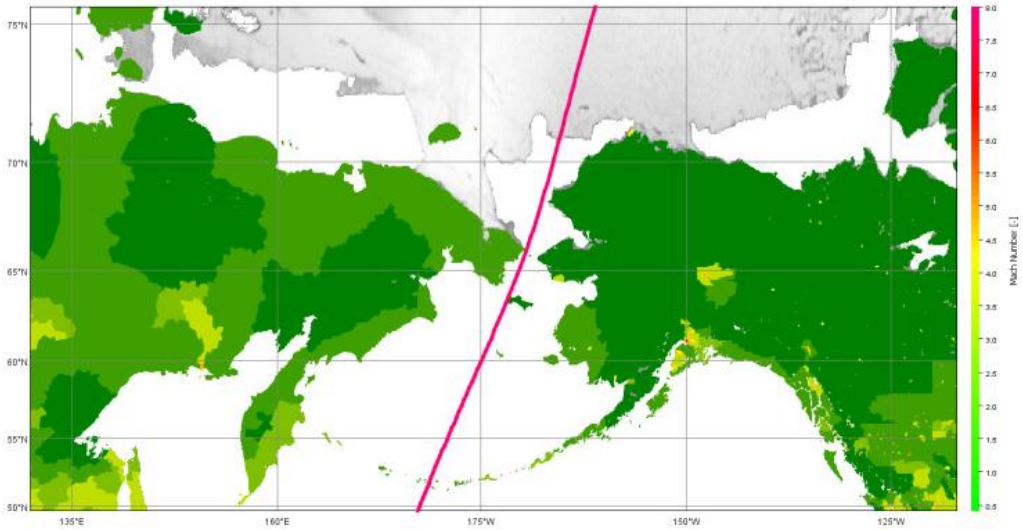


Figure 2.6 Bering Strait passage at Mach 8 [10].

- Descent and landing in Sidney.

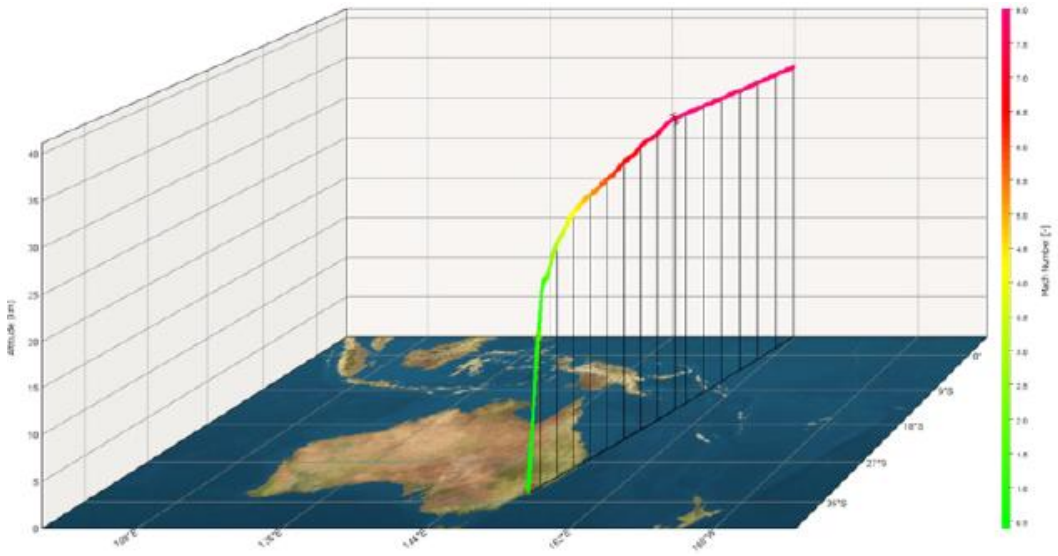


Figure 2.7 Landing in Sidney [10].

It is clear that, the simulations are based upon the Brussels-Sydney trajectory seen as the antipodal relevant route; hence, the design of the vehicle is focused on that flight.

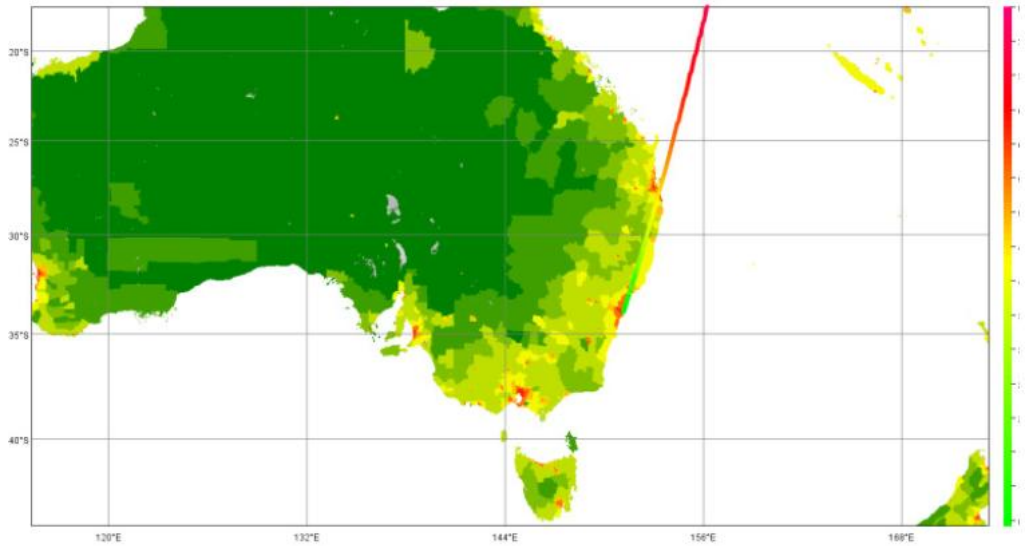


Figure 2.8 Detail of the landing in Sidney [10].

Obviously, if the analysis are carried out evaluating available but different landing airport (Los Angeles, Tokyo, ...) the project is not optimized (Figure 2.9) [10].

Trajectory	Distance Flown [km]	Great Circle distance [km]	Total Flight Time	Fuel consumed acceleration [ton]	Fuel consumed cruise [ton]	Fuel consumed [ton]	Fuel Remaining [ton]	TO mass [ton]	Consumed KgFuel/ 100km/ PAX
BRU-SYD[1]	18734	16734	2h47	81.5	99.5	181	0.25	400	3.23
BRU-SYD[2]	18734	16734	2h42	68.5	103.25	171.75	9.5	400	3.06
BRU-LAX[3]	12845	9075	2h20	82.8	54	136.8	44.5	400	3.55
BRU-NRT[3]	11843	9483	2h13	83.4	47.7	131.1	50.2	400	3.69
BRU-NRT	11843	9483	2h13	75.4	43.6	119	21	359.75	3.35
BRU-JFK[4]	5901	5901	1h30	63.3	7.6	70.9	9.1	298.75	4.00
BRU-MIA[4]	7472	7472	1h37	65.7	16.9	82.6	12.4	313.75	3.68

Figure 2.9 Overview of the simulated trajectories [10].

Figure 2.10 Final part of the mission in LAX (left) and NRT (right) [10].

The MR2 vehicle has to be characterized by an innovative shape in order to perform this kind of "unusual" mission scenario. The inspiration comes from other already-known supersonic vehicle such as Concorde or Valkyrie XB-70. The result of the study is a *waverider configuration* in order to increase L/D, thanks to compression lift, using shock waves, that the high speed flight generates against suitable lifting surfaces. In Figure 2.11 is shown the final layout of the MR2 with a detail of the inside, displayed in Figure 2.12.

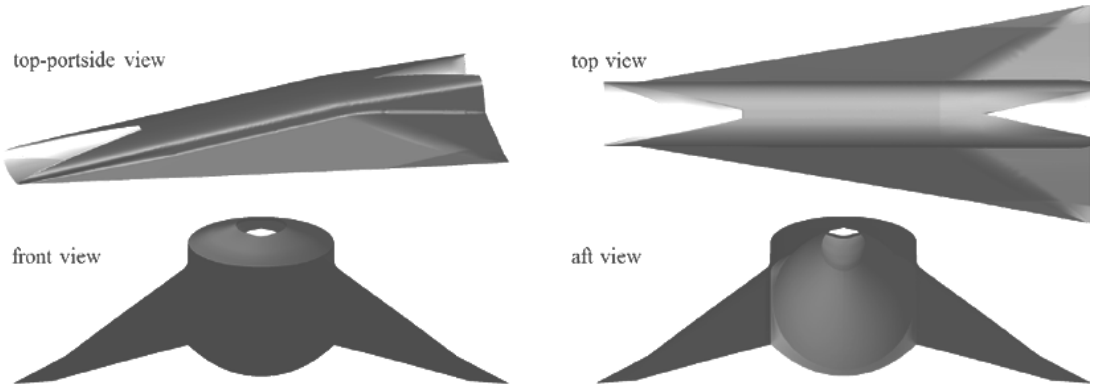


Figure 2.11 CAD overview of the MR2 vehicle [11].

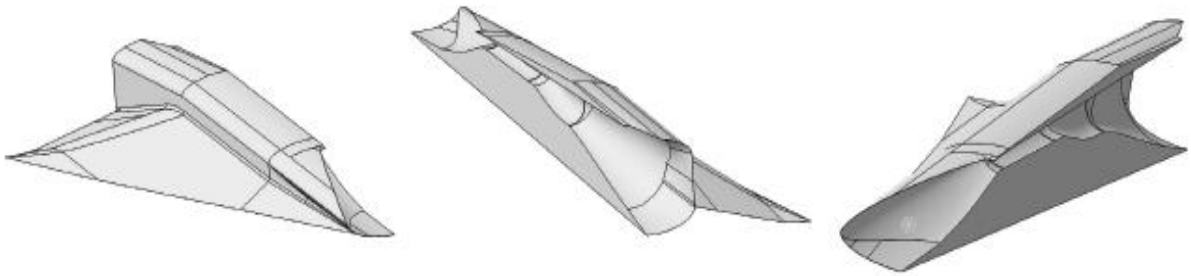


Figure 2.12 CAD Internal cut view of the MR2 [12].

2.2 Layout and Engines integration

This vehicle has a «*waverider*[7] *form based upon a rigorous osculating cone method, enabling to construct the vehicle from the leading edge while diminishing integration problems between the aerodynamics and the intake*» [9]. After different trade-off analyses, the final 2D shape of the intake is elliptical conceived to feed a DMR, Dual Mode Ramjet (or Scramjet, see Figure 2.13), combustion chamber: this technology is expected to operate up to Mach 8.

Clearly, two different kind of engines are required: one has to be able to operate at low speed, the latter has to perform acceleration and hypersonic cruise; the challenge is to successfully design the integration of both the propulsion unit.

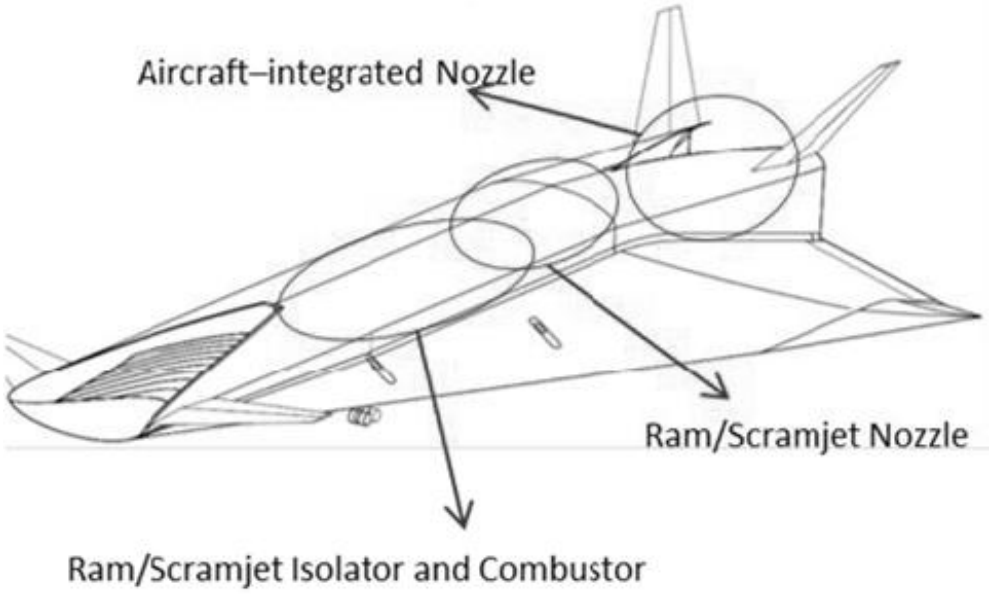


Figure 2.13 Location and integration of engines in the vehicle [13].

The first kind of technology, installed to perform subsonic and supersonic phases, is based on an ATR (Air Turbo Rocket) engine (inspired by the XB-70), where a retracting door panels system is placed linked with intake, characterized by sliding or movable ramps, to provide the necessary flow for the operations in the useful direction.

[7]For "waverider design" see http://www.aerospaceweb.org/design/waverider/waverider.shtml.

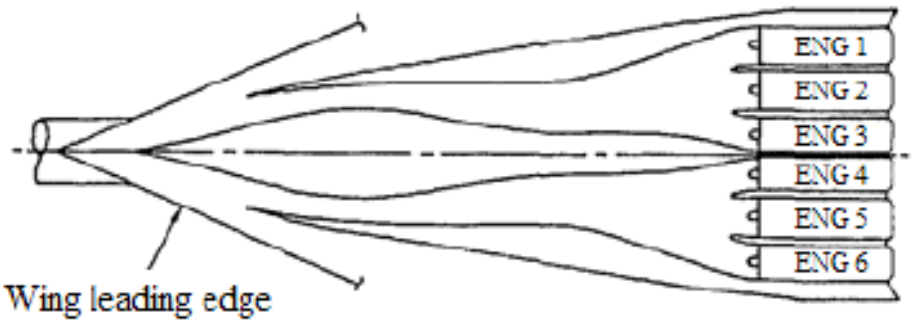


Figure 2.14 XB 70 Engines and Air induction system Configuration [13].

At the end, a two sections nozzle is installed: the first sector is an isentropic 2D nozzle with an area ratio of 3. After reaching a contraction ratio of 10, that nozzle works as combustor chamber to guarantee supersonic expansion in the second nozzle; that shape is relevant because it guarantees minimization of wetted area but maintains appropriate and efficient the fuel injection. The second section of the nozzle has the particularity that, it was designed with a too long length, so in the final design, it was truncated to perfectly fit the suitable design as Figure 2.15 shows [9].

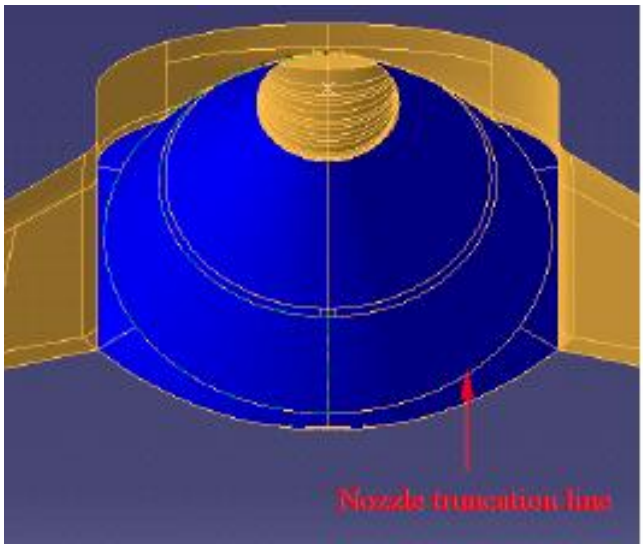


Figure 2.15 Detail of the truncation of the second nozzle: in blue the thrust surface is highlighted [9].

As mentioned at the beginning of the chapter, the purpose is to design a vehicle with an optimized configuration that could guarantee a "L/D factor greater than 6", in order to achieve the expected flight Mach number approximately of 8.

Introducing the layout, the engines are installed on the dorsal upper side of the MR2 vehicle; after a significant expansion at the end of the intake, the combustion chamber is located and it feeds the Dual Mode Ramjet (or Scramjet) [9].

This is foreseen to operate at Mach 4-4.5 and subsequently at Mach 8. Clearly, it is necessary to reach suitable speed to start the operations of the DMR engine, therefore an ATR is installed to provide the proper acceleration phases before the hypersonic cruise: this engine is integrated into the DMR and it is accessible by sliding doors, that make the flow path change direction as is shown in Figure 2.16. From take-off to Mach number of around 4, the ATR works: this system consists of 6 engines divided in 2 bays of 3 of each engine (as example see Figure 2.14) installed in parallel and integrated with the airframe.

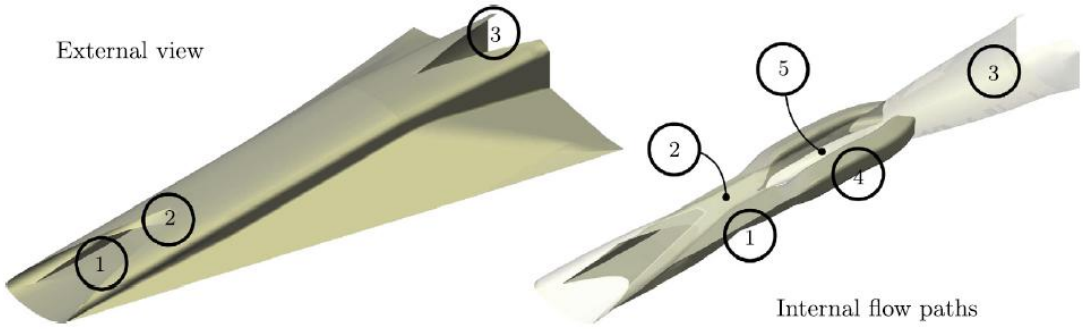


Figure 2.16 CAD of external and internal view of the vehicle:1 low speed intake, 2 high speed intake, 3 nozzle, ATR duct, 5 DMR duct [14].

The operations are based on an expander cycle where the DMR duct is not used (Figure 2.17). To reach the expected hypersonic speed, the vehicle operates with the DMR system, able to step up and get to the cruise phase. This engine is characterized by the already seen nozzle with a first 2D isentropic expansion followed by a second 3D expansion: the latter one is 43m long (it was expected to be 75m long) because it has had to fit with the vehicle structure. This truncation is permitted by the fact that the last part of the nozzle does not contribute significant thrust [9].

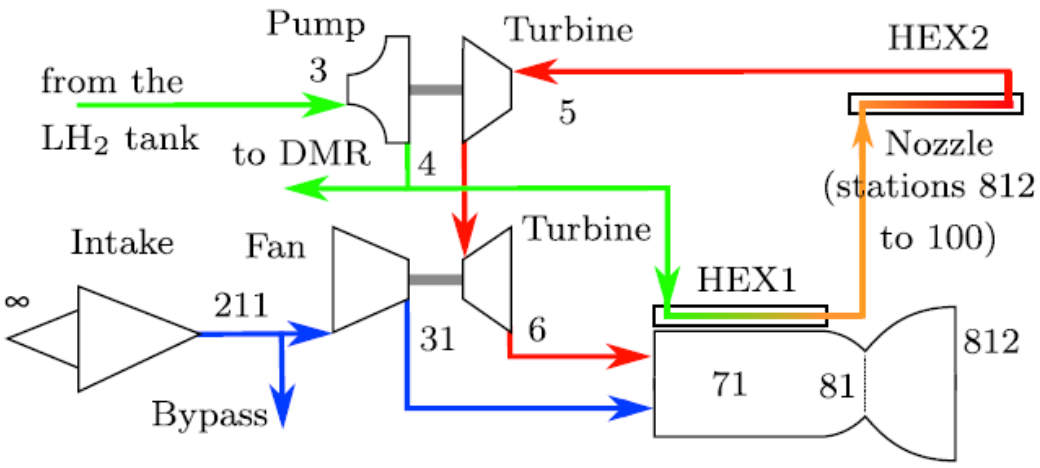


Figure 2.17 Operation of the expander cycle [14].

The scheme of the expander cycle is here no further discussed[8] (because the engines operation is not the focus of this Thesis). However, it is considerably useful to introduce the general concept in order to understand TEMS system interfaces such as turbine, pump, tanks and intake and their behaviour during the mission. TEMS system is analysed in detail in the following sections.

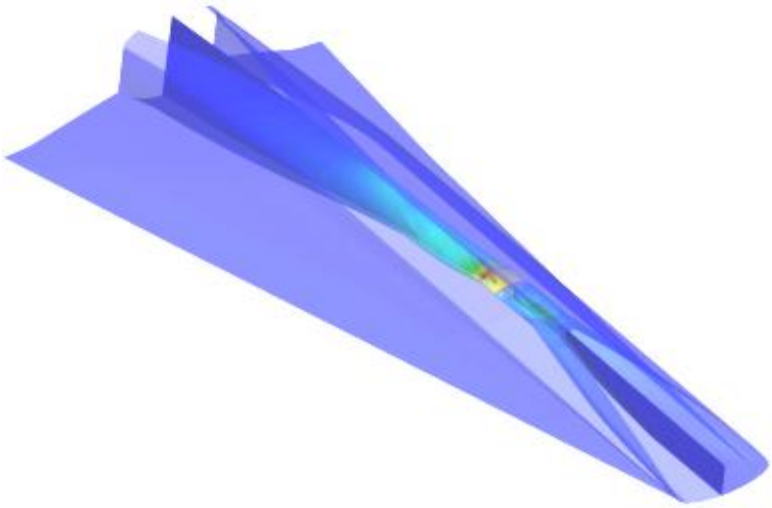


Figure 2.18 CFD detail of the combustion inside the DMR [14] .

[8] For more details, see [14].

2.3 Thermal and Energy Management System

As already mentioned, one of the most significant technology embedded in the on-board system of this vehicle is an innovative and efficient thermal management. In this context, the implementation refers to as a Thermal Management System responsible to provide the need of cooling for passengers and crew (to guarantee comfort in strict margins to maintain human habitability) but also to protect all the systems (and subsystems) against high temperatures, due to propulsion system and external heat fluxes derived from hypersonic speed.

In fact, the purpose of designing an innovative TEMS, Thermal and Energy Management System, for hypersonic transportation vehicle is to optimize the capability to sustain thermal loads but also to try covering the on-board energy needs. This kind of aircraft is exposed to high temperature fluxes, in particular during cruise phase, from the external of the fuselage and wings (high friction due to hypersonic speed) but also from the inside because of the propulsion system. It is clear that, a management of this thermal condition is essential to protect equipment and provide cooling for airframe and cabin: if this energy is well-managed, it could be also useful to provide on-board power [15].

There is also another relevant aspect: during the acceleration phases and the hypersonic cruise, that means when the DMR is active, there is no power supply (electrical or mechanical) to provide on-board needs and operations. In this context, the goal has been achieved studying an unexpected "new" cold source, that is the boil-off. The vehicle boards indeed 180tons of liquid hydrogen: this absorbs some part of heat, therefore a percentage is converted in gaseous phase. Designing a suitable system integrated into the structure and, consequently, a proper thermodynamic cycle, it is possible to further reuse the fuel boil-off to cool down equipments before injecting it into the combustion chamber and to balance thermal loads during the entire flight mission.

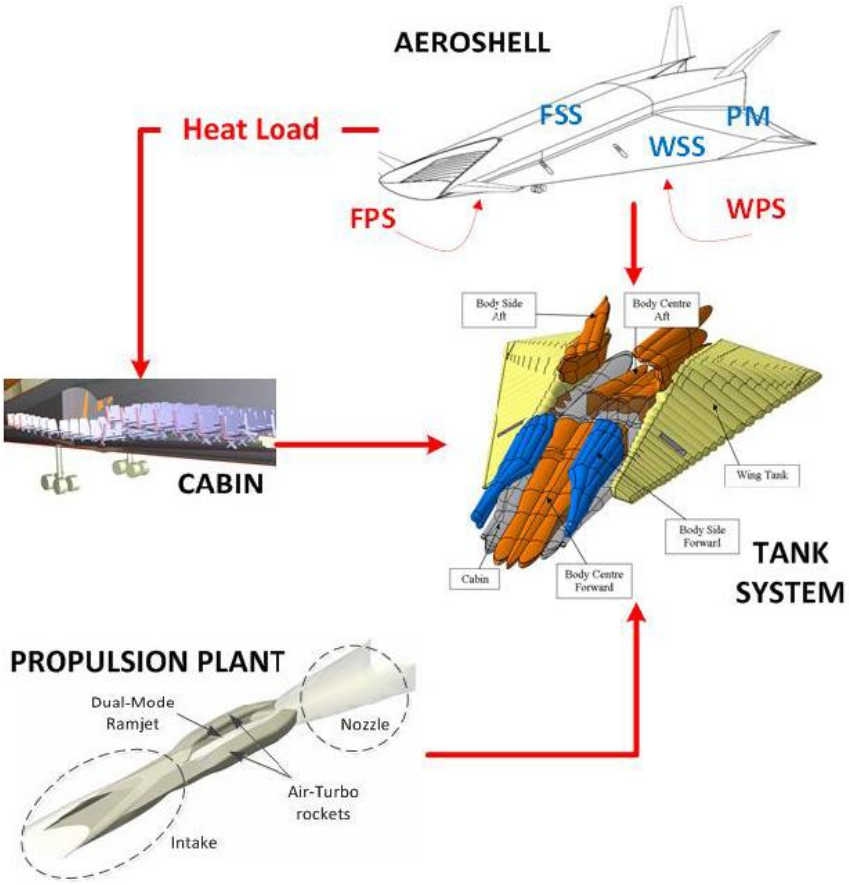


Figure 2.19 Thermal interaction between the vehicle subsystems [16].

The TEMS is further characterized by a high level of complexity: different systems interface with it (as Figure 2.19 highlights[9]) and its innovative way of working will be revealed in the following pages.

The heat loads (from external or propulsion plant) penetrate and generate boil-off in the cryogenic tanks and then the path is divided in two parts:

- A fraction is used to cool the cabin and systems;
- A fraction remains unspoilt and is sent to the compressor.

Before reaching the compressor, there is a mixing of the two fractions.

[9] For more details, see [16].

The propulsion plant and the air pack are then cooled down by the compressed fuel obtained: the cycle ends with an expansion through a turbine that provides mechanical energy for the whole aircraft system. The final step is to inject the fuel into the combustion chamber. There is a spillage system in the intake to create an air inflow inside the cabin: an air-recirculation system and an insulation system are then installed in the cabin, therefore the cooled air coming from the spillage in continuously changed and proper conditions are guaranteed for passengers.

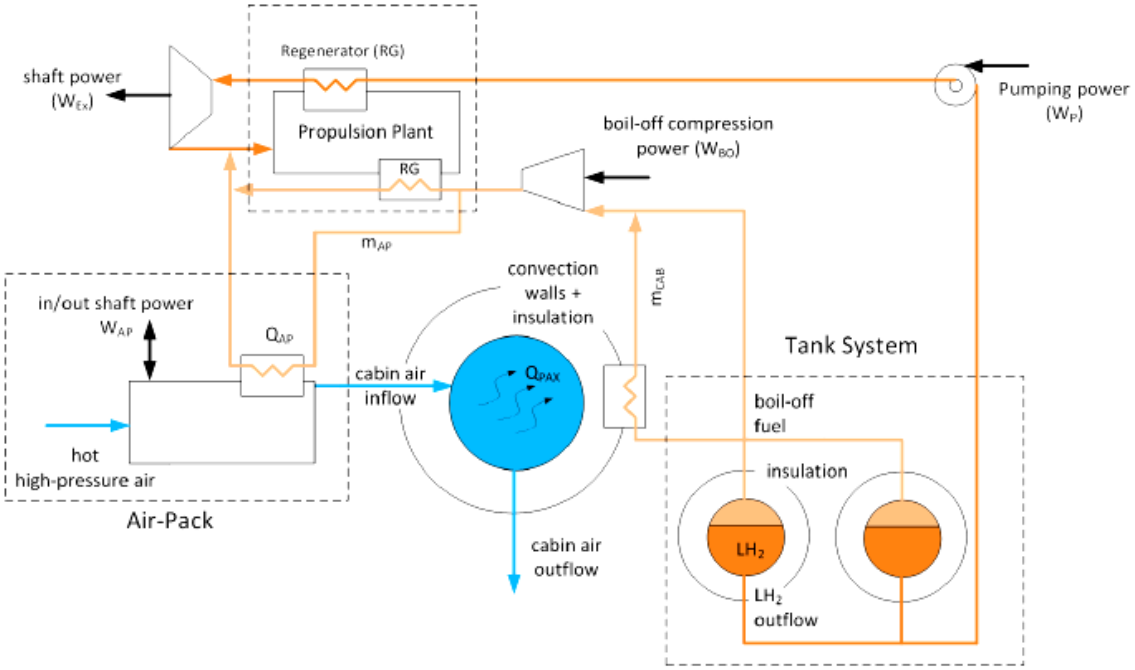


Figure 2.20 Overview of the thermodynamic cycle of the designed TEMS for MR2 vehicle [15].

As shown in Figure 2.20, there is also another flow path for liquid hydrogen. This fraction of fuel is the main cooling source for the propulsion plant walls: the fuel is properly compressed through a pump and then it is used as refrigerant in a heat exchanger in contact with the combustion chamber walls.

The active system has been designed for cabin, because the operations margin of the ECS are quite demanding and a passive one does not guarantee a proper reliable human habitability. For what concerns the propulsion plant since the passive cooling is not applicable for high temperatures regimes, which are reached during acceleration and hypersonic cruise phases [15].

Eventually, a traditional Thermal Protection and Shielding System for the aeroshell (the reached temperatures can be faced by usual insulation materials such as C/C/SiC, the purpose is to perfect this sector) has been envisaged.

In Figure 2.20, Passive Thermal System and Thermal Protection and Shielding System are not displayed but they have been cited here because they will be useful to guarantee an appropriate analysis.

This introduction of the main characteristics and operation of the MR2 vehicle will be now followed by the description of the application of the MBSE methodology to perform the Safety and Reliability Assessment on this specific case of study focusing the analysis on the innovative TEMS.

3 Application of the MBSE methodology to the MR2 vehicle

In this Chapter, the step-by-step, formalized methodology introduced in Chapter 0 is illustrated, starting from the market analysis, proceeding with the Functional Analysis and concluding with the allocation of the different functions to the proper product.

3.1 The stakeholders analysis

This project is attractive for the research world because it involves a lot of different study fields: from the already cited aerodynamics, to materials engineering, up to propulsion system and structure sector. Apart from the academia, also plenty of public and private agencies could be interested in developing an innovative type of transportation system plus people would be interested as passengers to exploit long-haul hypersonic missions because of the reduction of route duration.

To sum up and contextualize the product, here the Mission Statement related to this case of study has been reported, followed by the gathered objectives.

The Mission Statement could be written as follows:

The aim of Lapcat project is to design a hypersonic reusable transportation vehicle to reduce antipodal flight time. The vehicle shall board at least 300 passengers, flying at Mach 8 and at high altitude set at 35km. A multidisciplinary optimization is required as well as high level of integration in subsystems.

The vehicle shall perform an horizontal take-off, an initial cruise, different acceleration phases to reach Mach 8, the hypersonic cruise and an unpowered and horizontal landing.

The mission shall withstand all the flight regulations: in particular the expected trajectory shall not be over inhabited lands because of the sonic boom.

In the near future the vehicle shall be able to operate efficiently in air traffic management therefore it shall be a competitive and affordable new way of travelling.

The primary objective of the project is *to provide a long-haul hypersonic transportation service*.

Finally, the secondary objectives, derived from the primary one, are related to the actors, who could be interested in it:

- *To maintain Europe competitive in long-term studies.*
- *To gain good position in emerging markets.*
- *To provide an antipodal flight capability.*

- *To develop faster transportation system concepts.*
- *To develop, produce and commercialize hypersonic transportation systems.*
- *To test innovative layout.*
- *To test new technologies.*
- *To develop regulatory framework for hypersonic flight service.*
- *To enhance public consensus in a future way of travelling.*
- *To turn high speed transport into a business.*
- *To promote the application of space technologies in other sectors.*
- *To diminish the flight time on antipodal routes.*
- *To verify the reusability of new hypersonic transportation system.*
- *To enhance the TRL of the system.*

It is necessary to underline that each purpose has to be linked with at least one actor. In this case, three significant sponsors have been identified, with their specific aims:

- European Community;
- ESA;
- Private Agencies.

Sponsors	Objectives
EC	To maintain Europe competitive in long-term studies
	To gain good position in emerging markets
	To enhance public consensus in a future way of travelling
ESA	To provide an antipodal flight capability
	To enhance public consensus in a future way of travelling
Private Enterprises	To develop, produce and commercialize hypersonic transportation systems
	To develop faster transportation system concepts
	To enhance public consensus in a future way of travelling

Table 3.1 Sponsors and related objectives.

On the other side, two relevant entities have been outlined as operators:

- European Industries or Companies;
- Airline Operators.

Operators	Objectives
European Industries	To turn high speed transport into a business
	To provide an antipodal flight capability
	To enhance public consensus in a future way of travelling
Airline Operators	To provide an antipodal flight capability
	To enhance public consensus in a future way of travelling

Table 3.2 Operators and related objectives.

The End-users are obviously from the research world as:

- ESA;
- Scientific Community.

End-users	Objectives
ESA	To enhance the TRL of the system
	To develop faster transportation system concepts
	To test innovative technologies
	To test innovative layout
Scientific Community	To verify the reusability of new hypersonic transportation system
	To promote the application of space technologies in other sectors
	To test innovative technologies
	To test innovative layout
	To enhance the TRL of the system
	To develop, produce and commercialize hypersonic transportation systems

Table 3.3 End-users and related objectives.

Finally, the passengers are pointed out as customers.

Customers	Objectives
Passengers	To diminish the flight time on antipodal routes

Table 3.4 Customers and related objectives.

The result of this analysis can be graphically illustrated in a Use Case Diagram (see Attachment A), where the Stakeholders are represented by the actors and the connections among actors and use-cases are highlighted to show the relationship in a more immediately way. The diagram is sketched in a proper language: in particular, in order to express the stakeholders categorizations, generalization links have been adopted, while to express the interest of each single stakeholder, the association link is more advisable. Moreover, the rule to express hierarchical relationship between primary and secondary elements has been respected: e.g. the secondary objectives are related to the primary one by a dependency link with a specific stereotype "include". As mentioned before, the generation of a first list of mission and programmatic requirements is significant. Each requirement, that will be generated all along the product life cycle, can be written in a established database, allowing the storage, the access and the management step-by-step.

The importance of elaborating a Model-Based approach is not only to think over and write statements in databases, but also to generate classifications, connections and relationships among them, in order to trace each step and obtain a formalization of all the selections and choices made during the conceptual design. In this sense, it will be immediately investigated and verified if requirements are satisfied, and in negative case, the counteraction is to quickly modify and elaborate a new design to accomplish the mission purpose.

Subsequent to the focus on this innovative approach inserted at the beginning of the "traditional" MBSE method, the specific Safety Assessment starts in the already discussed way. At this level is valuable to list the Mission Requirements, the final product has to satisfy.

The Mission Requirements are gathered here, followed by the constraints (international regulations) and the Programmatic Requirements[10]:

Mission Requirements

- *The transportation system shall allow antipodal hypersonic flight service.*
- *The vehicle shall be able to transport at least 300 passengers and crew.*
- *The vehicle shall perform a hypersonic cruise at high altitude set at 35km.*
- *The vehicle shall perform a hypersonic cruise at Mach 8 .*
- *The vehicle shall be conceived to perform an horizontal take-off.*
- *The vehicle shall perform multiple acceleration phases to reach Mach 8.*

[10] To remind the meaning, see chapter 1.

- *The vehicle shall be able to perform unpowered descent.*
- *The vehicle shall be conceived to perform an horizontal landing.*
- *The vehicle shall verify high and proper safety level.*
- *The transportation system shall guarantee higher level of integration.*
- *The transportation system shall ensure a competitive new way of travelling.*

Constraints

- *The vehicle shall cover a trajectory over uninhabited lands.*
- *The passengers shall experience acceleration limited in the range -1g to 2,5g.*

Programmatic Requirements

- *The mission shall be performed by the 2030-2040.*
- *The mission shall maintain Europe competitive.*
- *The mission shall lead in a new transport market.*
- *The mission shall be envisaged to enhance the state of art technologies.*

According to the performed analysis at Mission Level (see Figure 1.6) of the previous pages, the next step is to begin the Functional Analysis at lower levels.

3.2 Functional Analysis

The Functional Analysis is used to consider the product from a different point of view: this sight permits to derive the Functional Requirements related to the objectives the system has to fulfil: this procedure has to be applied and repeated until the proper level of study will be achieved [4]. In addition, it is useful to identify the products, which have to guarantee the operations previously elicited. Proceeding with this study, the outcome will be firstly the Functional Tree, graphically reflecting the functionalities breakdown and allowing to immediately show the system from the "functional point of view"; as well as the functions/devices Matrix, which is derived to match and allocate the functions to the correct components. The Products Tree finally collects and summarizes the required equipment.

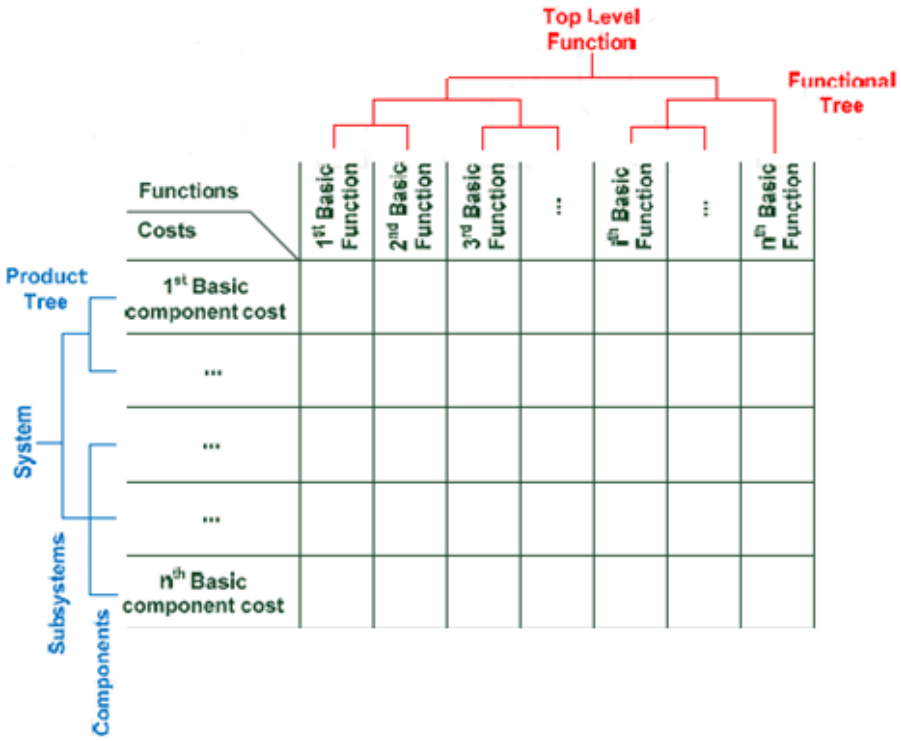


Figure 3.1 Example of a Functions/Devices&Costs Matrix [7].

These steps allow deriving, in a second moment, the functional and the physical block diagrams [5].

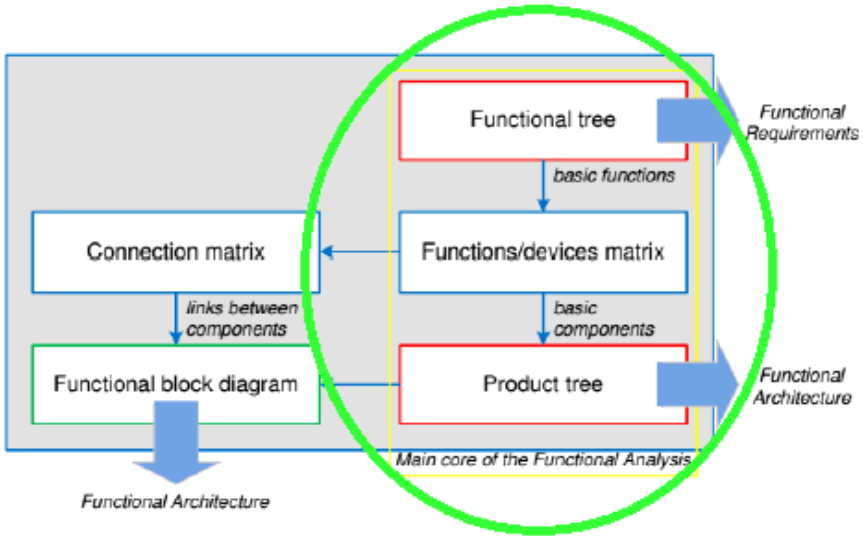


Figure 3.2 Functional Analysis scheme [7].

3.2.1 Application of the Functional Analysis to the MR2 vehicle

In this specific case the Functional Tree is characterized by different levels of requirements: the top level is the highest level and most general, the segment level is the one related to the flight segment, the system level, certainly, regarded all the systems and lastly all the subsystems levels are pointed out. The result of this reasoning is a top level requirement, a list of requirements associated to the segment level and a list of different system and subsystems level requirements.

The top level requirement is expressed as "*the product shall perform antipodal hypersonic flight service"*, the segment level requirements are split in two different statements, the one related to the Ground Control System ("*the ground segment shall support the flight service and operations"*) and the one linked to the Flight Segment ("*the flight segment shall transport passengers"*).

The system level requirements are listed here and gathered in the Functional Tree in Figure 3.3:

- *The system shall maintain thermal equilibrium.*
- *The system shall board propellant.*
- *The system shall perform horizontal take-off.*
- *The system shall support horizontal take-off.*
- *The system shall perform horizontal landing.*
- *The system shall support horizontal landing.*
- *The system shall perform the acceleration phases.*
- *The system shall support the acceleration phases.*
- *The system shall perform the initial subsonic cruise.*
- *The system shall support the initial subsonic cruise.*
- *The system shall perform a hypersonic cruise at 35km.*
- *The system shall perform a hypersonic cruise at Mach 8.*
- *The system shall sustain structural loads.*
- *The system shall safely accommodate passengers and attendants.*
- *The system shall guarantee communication.*
- *The system shall guarantee navigation and guidance.*
- *The system shall perform surveillance and identification.*
- *The system shall control system in atmospheric environment.*

- *The system shall perform unpowered descent.*
- *The system shall support unpowered descent.*
- *The system shall accommodate the crew.*
- *The system shall guarantee human habitability.*
- *The system shall supply electrical power.*

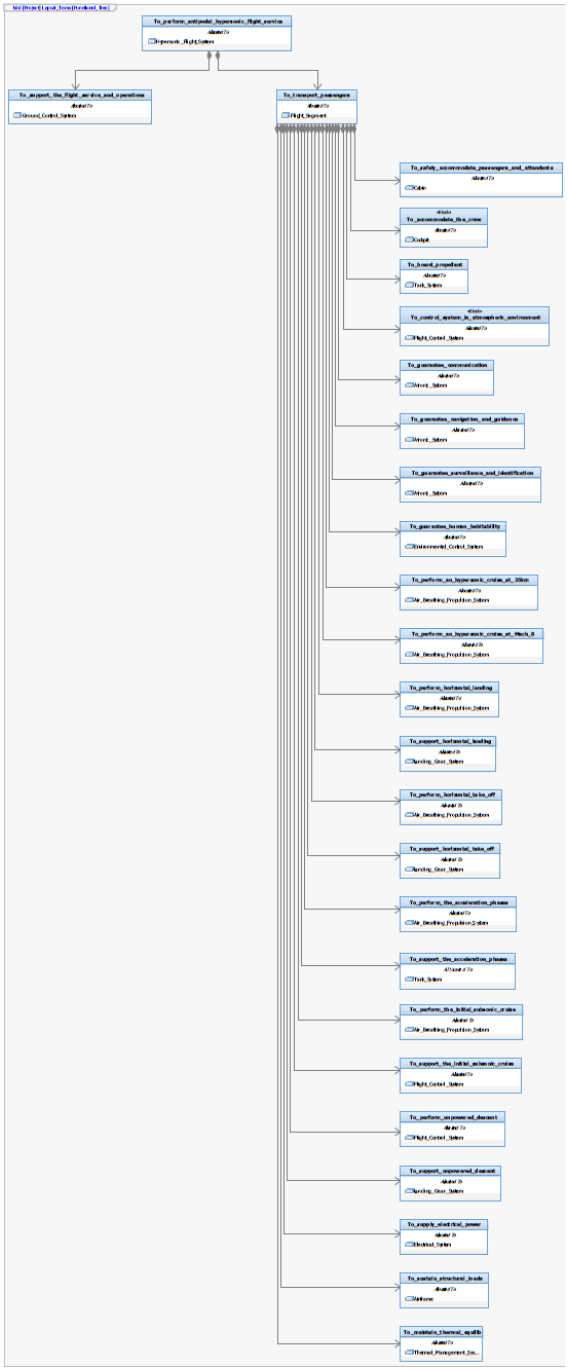


Figure 3.3 Functional Tree (top-level, segment-level and system level).

The subsystems level requirements will be discussed in chapter 4.2.3. In parallel with the Functional Tree[11] , the Products Tree[12] is developed (see Figure 3.4).

To obtain an accurate Products Tree is necessary to build the functions/devices Matrix in order to allocate each function to the sub-systems (up to concrete components) able to perform those functions [4]. Observing Table 3.5, to complete the matrix, it is sufficient to tick the proper correspondence between rows and columns and gather the equipment in the tree.

Here, the devices/functions Matrix (Table 3.5) and the Products Tree (Figure 3.4) are shown, where it is highlighted that, to achieve optimization, each component could perform more than one functionalities.

[11] Attachment D.
[12] Attachment F.

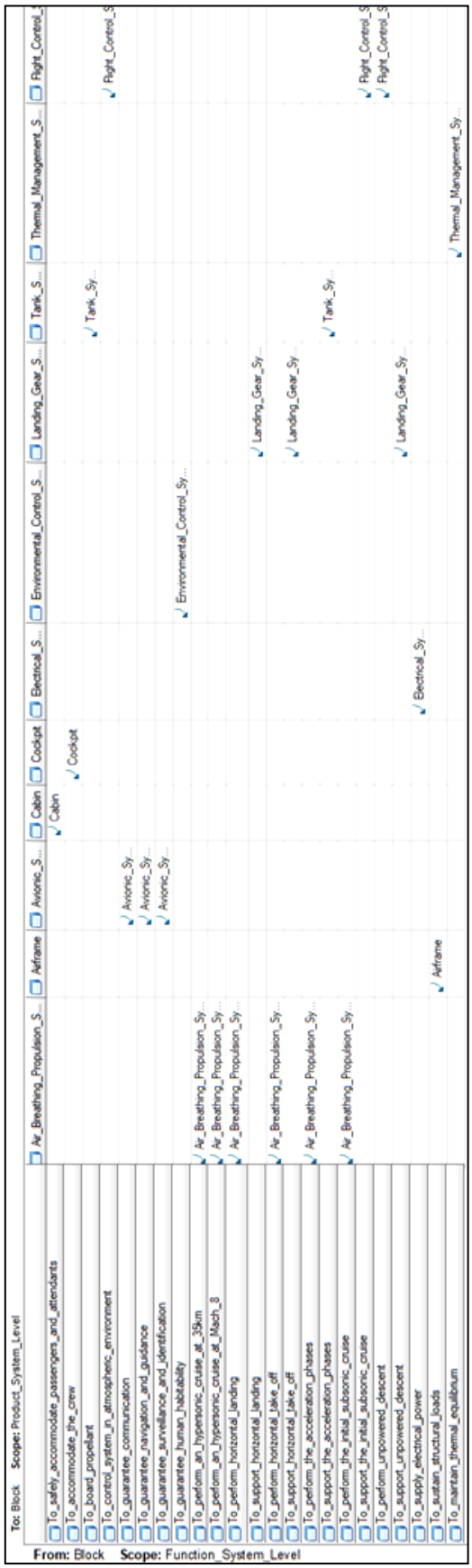


Table 3.5 Table view of the Functions/Devices Matrix at Systems Level.

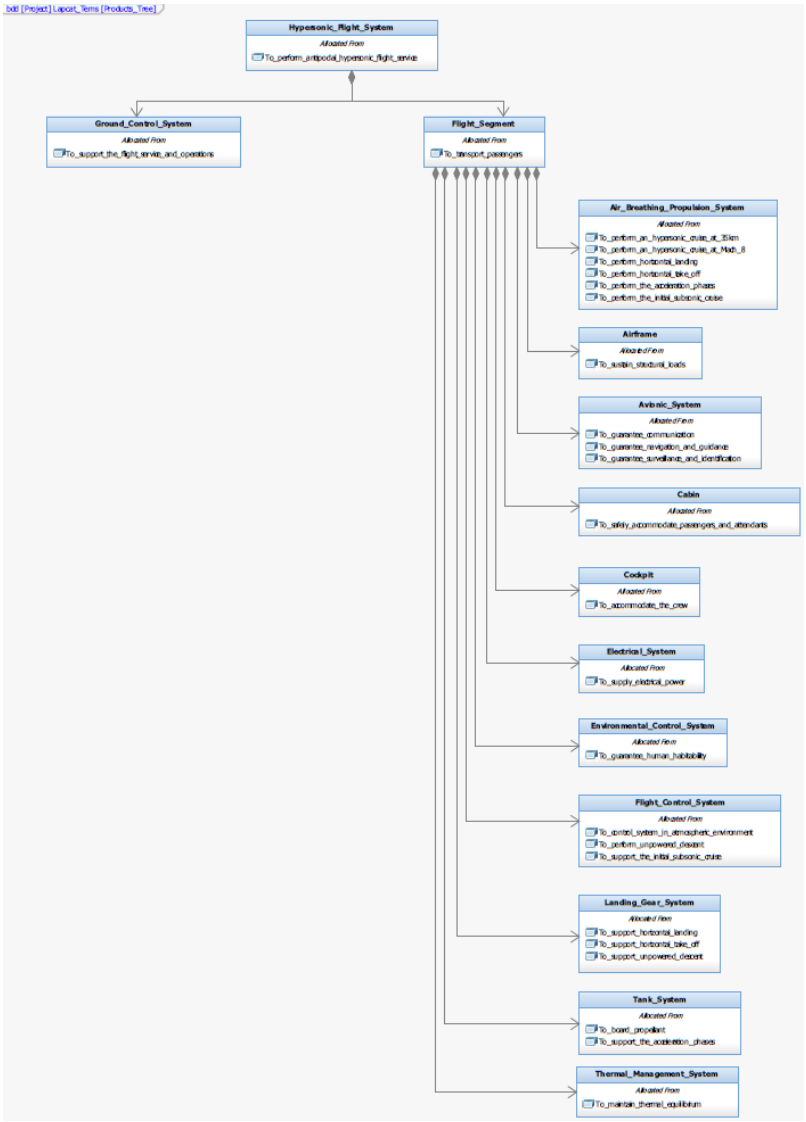


Figure 3.4 Products Tree (top-level, segment-level and system level).

4 Qualitative Safety and Reliability Assessment

Next to the preliminary analysis performed in chapter 3, the following step is the iterative and recursive procedure related closely to the Safety Assessment. In this process, the preliminary Functional Tree and Products Tree obtained in the previous analysis will be developed at lower levels.

4.1 Functional Hazard Assessment (FHA)

The outlined functions could be exploited to perform the FHA and to carry out this analysis at aircraft and systems/sub-systems level. As it has been already explained in chapter 1.2, the main purpose of this kind of assessment is to examine, identify and classify the failure conditions linked to the single function at each level of study. The relevant aspect is to derive malfunctions for every mission phase because the severity of the failure is different according to the sort of operation: each function has been evaluated indeed attempting to underline what could happen, if that function is unavailable during the flight phases.

Clearly, the FHA[13] is an iterative and recursive process that must be performed until the design process is complete, consequently, each failure condition is useful to generate lower level requirements [4].

In this reasoning, to carry out the FHA, it is required to derive functions related to the operation of the hypersonic vehicle, considering at the same time the potential failure conditions that could happen; in particular, the effects caused against the vehicle during a specific mission phase. It is necessary to classify the different failure conditions according to five different risky levels formalized and labelled with these marks:

- catastrophic (A),
- hazardous (B),
- major (C),
- minor (D),
- no safety risk (E).

A =Catastrophic
B=Hazardous
C=Major
D=Minor
E=No safety effect

Table 4.1 Risk classification

[13] For more details, see Appendix A.

4.1.1 Functional Hazard Assessment (FHA): Application to the MR2 vehicle

Functional Hazard Assessment has to be accomplished for each Function previously listed: specific failure conditions are associated to each functions (and consequently also to each requirement) and organized in a table view (see Attachment B). In the following pages, the methodology to elaborate the FHA is illustrated.

Reminding the outlined requirements list in chapter 3.2.1, the first considered function to develop the FHA at system level is the one concerning the Thermal Management System: if the function to *maintain thermal equilibrium* is lost, during climb and cruise (when it is reached hypersonic speed), the vehicle can risk overheating causing *unsustainable thermal loads* and the *incapability to cool the structure, the engines and all the systems*.

FUNCTION	FAILURE CONDITION	PHASE	CLASSIFICATION
To maintain thermal equilibrium	loss of the capability to sustain thermal loads	climb, cruise	A
	loss of the capability to cool engines	climb, cruise	A
	loss of the capability to cool the vehicle primary structure	climb, cruise	A
	loss of the capability to cool systems	climb, cruise	A

Table 4.2 FHA of the function "To maintain thermal equilibrium".

All these events have been classified as catastrophic, because they can elicit the worst and most dangerous effects to passengers: the Thermal Management System is one of the most relevant system for this case study and it has to guarantee best performances through a high level of innovation architecture.

The functionalities associated to the storage of liquid hydrogen can cause risky events when proper conditions during propellant transfer operation are not guaranteed: during flight phases, the event could become catastrophic, if the proper flow rate is not maintained inside the propulsion unit. Moreover, hydrogen must constantly be in circuit both for engines and for cooling capability: when DMR is active, the fuel flow rate is essential because the turbine operation is the only source of power apart from batteries.

FUNCTION	FAILURE CONDITION	PHASE	CLASSIFICATION
To board propellant	loss of the capability to storage the required propellant	taxi	E
	loss of the capability to transfer fuel at a proper rate	take off	C
	loss of the capability to transfer fuel at a proper rate	climb/cruise/descent	A
	loss of the capability to transfer fuel at a proper rate	landing	C
	unable to maintain the correct relative pressure	all	B
	loss of the capability to supply a continuous fuel at proper temperature	all	B
	loss of the capability to refuel the tanks	taxi	E
	loss of the capability to refuel the tanks	cruise	B
	loss of the capability to ensure sufficient fuel in the main tanks to perform an emergency landing	all	B

Table 4.3 FHA of the function "To board propellant".

The function concerning the performance of horizontal take off can cause several kinds of effects according to the mission phase: during the taxi phase, there is no safety risk because the vehicle is on ground; if the failure occurs during the take off phase, the risk increases because the aircraft cannot accelerate appropriately to lift off. A more dangerous condition happens, if the vehicle can accelerate but not enough to reach the lift-off speed: in this case it is difficult to brake and stop safely in time.

FUNCTION	FAILURE CONDITION	PHASE	CLASSIFICATION
To perform HTO	loss of the capability to perform take-off	taxi	E
	loss of the capability to generate thrust on ground	take off	C
	loss of the capability to perform taking off acceleration	take off	B

Table 4.4 FHA of the function "To perform HTO".

Moreover, the support of take-off manoeuvre is essential: if the vehicle is unable to reach the position on the runway, it could be an inconvenience for the airport traffic with a "minor" risky level; the most hazardous event happens, if the system cannot perform the proper rotation manoeuvre because it has already reached a high speed to be stopped without risky consequences. In the other considered cases, the level of risk is classified as "major", it means a medium risk.

FUNCTION	FAILURE CONDITION	PHASE	CLASSIFICATION
To support HTO	unable to reach the proper position on the runway	taxi	D
	unable to perform straight taking off running on the ground	take off	C
	unable to support the taking off manoeuvre	take off	B
	unable to retract the landing gear	take off	C

Table 4.5 FHA of the function "To support HTO".

During the climb phase the incapability of the vehicle to perform and support the two different acceleration phases to reach Mach 8 has been outlined. If this does not happen because the propulsion system fails or the fuel mass flow rate is not guaranteed, the impact will be not so risky: the vehicle can follow a mission profile different from the one expected, without compromising considerably the safety, even if the mission may be aborted..

FUNCTION	FAILURE CONDITION	PHASE	CLASSIFICATION
To perform the acceleration phases	loss of the capability to perform the acceleration phases	climb	D
To support the acceleration phases	unable to guarantee the desired fuel mass flow rate	climb	C

Table 4.6 FHA of the function "To perform/support the acceleration phases".

Moreover, referring to the constraints of this project, before the reach of hypersonic conditions, the vehicle must keep distance from the airport and the inhabited zones (because of the sonic boom.

The level of risk is classified as "minor" for the performance of this phase; the operation becomes more dangerous if the support of the cruise is threatened: as a matter of fact, the risk is high if the vehicle loses its primary surfaces becoming uncontrollable. On the other side, the condition in which some control surfaces remain active, is classified as "major" because the controllability of the vehicle is guaranteed, thanks to the redundancies of the surfaces.

FUNCTION	FAILURE CONDITION	PHASE	CLASSIFICATION
To perform the initial subsonic cruise	loss of the capability to perform the initial subsonic cruise	cruise	D
To support the initial subsonic cruise	loss of all the flight primary surfaces	cruise	B
	loss of any flight primary surfaces	cruise	C

Table 4.7 FHA of the function "To perform/support the initial subsonic cruise".

In parallel, performing and supporting the landing can cause undesired conditions, when the vehicle cannot brake properly during the on-ground landing phase. The other events are identified as a "major" level of risk because the vehicle cannot carry out a fair approach and cannot be accurately controlled.

FUNCTION	FAILURE CONDITION	PHASE	CLASSIFICATION
To perform HL	loss of the capability to perform the approach for hl	descent	C
	loss of the capability to decelerate	landing	B
To support HL	unable to perform braking	landing	C
	unable to perform steering	taxi	C

Table 4.8 FHA of the function "To perform/support horizontal landing".

If the aircraft cannot reach the expected operational conditions in cruise, the risk is low, marked out as "minor" because the whole system can nevertheless work.

FUNCTION	FAILURE CONDITION	PHASE	CLASSIFICATION
To perform a cruise at 35km	loss of the capability to perform a cruise at 35km	cruise	D
To perform a cruise at Mach 8	loss of the capability to perform a cruise at Mach 8	cruise	D

Table 4.9 FHA of the function "To perform cruise at 35km" and "To perform cruise at Mach 8".

One of the most dangerous conditions appears when the structure cannot bear mechanical and aerodynamic loads: if this circumstance happens, the level of risk is the highest.

FUNCTION	FAILURE CONDITION	PHASE	CLASSIFICATION
To sustain structural loads	loss of the capability to bear weight and aerodynamic forces	take off/climb/cruise/landing	A

Table 4.10 FHA of the function "To sustain structural loads".

Another parallelism could be related to the function regarding the accommodation of passengers and crew. Clearly, the crew has a more remarkable role, because it is composed by trained pilots who can manage and face emergency conditions: if the crew is not well-equipped, the potential circumstances are hazardous or catastrophic (in nominal conditions and in emergency respectively); on the other side, the level of risk is lower, if the passengers are not well-equipped during nominal operations.

FUNCTION	FAILURE CONDITION	PHASE	CLASSIFICATION
To safely accommodate passengers and attendants	loss of the capability to accommodate passengers and attendants	taxi	D
	loss of the capability to accommodate passengers and attendants	take off/climb/cruise/ descent/landing	A
	loss of the capability to accommodate passengers and attendants	take off/climb/cruise/ descent/landing	C
To safely accommodate the crew	loss of the capability to accommodate the crew	taxi	E
	loss of the capability to accommodate the crew	take off/climb/cruise/landing	A
	loss of the capability to accommodate the crew	take off/climb/cruise/landing	B

Table 4.11 FHA of the function "To safely accommodate passengers and attendants" and "To safely accommodate the crew".

The next considered functions concerns the avionic system: to maintain the correct level of study, more details were added as a sort of "sub-functions" to specify.

The first one is to guarantee communications with ground station and passengers. The communication system is one of the most significant system in a vehicle: if it does not work, the effects can be catastrophic or hazardous during any phases. The loss of inner communications is not as relevant as the loss of communications with ground station: if passengers are not informed by the pilots about the flight, dangerous conditions do not occur. The most alarming event happens, when the crew is unable to be informed, if failures occur inside the vehicle. Conditions classified as hazardous instead, are related to information missing between crew and ground station about authorizations and assistance.

FUNCTION	FAILURE CONDITION	PHASE	LASSIFICATIOI
To guarantee communication			
To transmit/receive signals	loss of the capability to transmit/receive signals to/from ground station	taxi	E
	loss of the capability to communicate the authorization	take off	D
	loss of the capability to transmit/receive signals to/from ground station	climb, cruise, descent	B
	loss of the capability to communicate the authorization	landing	B
	loss of the capability to reach the correct gate	taxi	E
To store data	unable to memorize data	all	E
To transmit emergency signal to be localized	loss of the capability to transmit emergency signal	all	B
To inform in case of system failure	unable to warn in case of system failure	all	A
To guarantee inner communication	loss of the capability to guarantee inner communications during flight	all	E

Table 4.12 FHA of the function "To guarantee communication".

In parallel with the communication system, the navigation and guidance is another main field: the key difficulty happens when it is not possible to acquire data from the external environment and elaborate navigation outcomes to calculate the state vector, speed and altitude.

It means, the vehicle cannot follow the best route and the crew cannot identify essential information about the flight to control the aircraft and perform manoeuvres: the worst case comes about if distances are undetectable during take-off and landing, therefore the crew cannot perform appropriate manoeuvres and is forced to execute emergency operations.

FUNCTION	FAILURE CONDITION	PHASE	CLASSIFICATION
To guarantee navigation and guidance			
To acquire navigation data	loss of the capability to acquire navigation data	take off/landing	B
	loss of the capability to acquire navigation data	climb/cruise/descent	C
To acquire environmental data	loss of the capability to acquire environmental data	climb/cruise/descent	C
To acquire flight data	loss of the capability to acquire flight data	all	C
To store and process data	loss of the capability to determine the state vector	all	C
	unable to have a database and to upgrade new data	all	D
To manage navigation data	loss of the capability to guarantee automatic guidance	cruise	C
	loss of the capability to guarantee manual guidance	all	C
	loss of the capability to activate a radionavigation	landing	C
To inform the crew	loss of the capability to guarantee guidance and navigation	all	C

Table 4.13 FHA of the function "To guarantee navigation and guidance".

Last functions of the avionic system is related to the identification and surveillance. In case of failure of this sector, the level of risk is not so harmful: the classification is a "major" level of risk. The danger consists of the failures that involve the capability of the vehicle to identify other airplanes or to be recognised and be tracked by ground station.

FUNCTION	FAILURE CONDITION	PHASE	CLASSIFICATION
To perform surveillance and identification			
To carry out identification by ground station	loss of the capability to be identified on the runway	taxi	C
	loss of the capability to be interrogated by radars	take off	D
	loss of the capability to be interrogated by radars	climb, cruise, descent	C
	loss of the capability to be interrogated by radars	landing	C
To carry out identification by other airplanes	loss of the capability to be interrogated by radars	take off	D
	loss of the capability to be interrogated by radars	climb, cruise, descent	C
	loss of the capability to be interrogated by radars	landing	D
To carry out surveillance in the airspace around	loss of the capability to carry out surveillance	climb, cruise, descent	C

Table 4.14 FHA of the function "To guarantee surveillance and identification".

The operations of the flight control system are essential: if it does not work, the failure conditions and the effects are catastrophic in account of the vehicle is uncontrollable and the crew cannot perform any kind of manoeuvres.

FUNCTION	FAILURE CONDITION	PHASE	CLASSIFICATION
To control the system in atmospheric environment	loss of the capability to control the system in atmospheric environment	take off/landing	A
	loss of the capability to control the system in atmospheric environment	climb/cruise/descent	A
	loss of the capability to guarantee control in case of emergency	take off/climb/cruise/ descent/landing	A

Table 4.15 FHA of the function "To control system in atmospheric environment".

Before the landing, the vehicle must perform and support an unpowered descent: any failures during this phase can cause hazardous events because the aircraft cannot actually decelerate, but overall, it cannot extend the landing gear earlier than the landing phase, therefore an emergency landing (which is a risky event) must be accomplished.

FUNCTION	FAILURE CONDITION	PHASE	CLASSIFICATION
To perform unpowered descent	loss of the capability to perform unpowered descent	descent	B
To support unpowered descent	unable to support unpowered descent	descent	B

Table 4.16 FHA of the function "To perform/support unpowered descent".

The environmental control system must not fail in order to guarantee proper human environmental conditions in the cabin and cockpit. In case of danger, the risk is obviously classified as catastrophic.

FUNCTION	FAILURE CONDITION	PHASE	CLASSIFICATION
To guarantee human habitability	loss of the capability to guarantee human need of temperature pression and oxygen concentration	all	A

Table 4.17 FHA of the function "To guarantee human habitability".

Finally, the electrical system is another one of the vital and essential elements of the project: if it does not work, all the users cannot be guaranteed.

The level of risk is high, in particular if the vital users are lost because there is no power distribution, no possibility to face emergency conditions plus if it loses the essential user to be controllable (to supply electrical power to actuators of the surfaces); the other identified level of risk have been decreased to hazardous, apart from the one concerning non-essential user.

To supply electrical power			
To supply electrical power to vital users	loss of the capability to supply electrical power to vital users	all	A
	loss of the capability to supply electrical power to vital users	all	A
	loss of the capability to supply electrical power to vital users	all	A
	loss of the capability to activate emergency devices	all	A
To supply electrical power to essential users	loss of the capability to supply electrical power to actuators	all	A
	loss of the capability to supply electrical power to on board computers	all	B
	loss of the capability to supply electrical power to essential users	take off/landing	B
To supply electrical power to non-essential users	loss of the capability to supply electrical power to non-essential users	all	E

Table 4.18 FHA of the function "To supply electrical power".

4.2 Fault Tree Analysis (FTA)

The next step is to proceed with the development of the Fault Tree Analysis with the assistance of the FHA. Each failure condition is the top event of a Fault Tree used to deduced the causes of the undesired event with a top-down approach. Thanks to the connections and relationships shown in the Fault Tree is possible to derive not only qualitative results but also information related to the probability of the events, applying the rules of the Boolean Algebra[14].

At this point, the process clearly shows its iterative and recursive baseline: each basic event of the Fault Tree becomes a failure condition of a lower level FHA.

In this case of study, this step has been developed exclusively for the TEMS because is the only system of the MR2 vehicle that is almost well-designed up to components level.

In this Chapter some details concerning the Fault Tree are disclosed, the whole models are in Attachment C.

4.2.1 Fault Tree Analysis (FTA): Application to TEMS of the MR2 vehicle

The only considered system is the Thermal Management System, therefore, here a review of its main features is displayed.

The purpose of designing an innovative TEMS, Thermal and Energy Management System, for hypersonic transportation vehicle is to optimize the capability to sustain thermal loads but also to attempt to cover the on-board energy needs. Actually, these kind of aircrafts are exposed to high temperature fluxes, in particular during cruise phase, from the external of the fuselage and wings (high friction due to hypersonic speed) but also from the inside because of the propulsion system.

[14] For more details, see Appendix A.

It is comprehensible that, a management of this thermal condition is necessary to protect equipment and provide cooling for airframe and cabin: if this energy is well-managed, it could be also useful to provide on-board power.

In the case of MR2, the TEMS has a high level of complexity because it must regulate the temperature during critic phases and supply mechanical and electrical power, when the propulsion system has to operate as DMR. In this phase, the applied technology is the one exploiting the cryogenic fuel boil-off. The optimization is within the boil-off indeed, that can be further reused in a cooling circuit for components.

The innovative way of working of this specific system is based upon heat loads which make the fuel boil-off in the cryogenic tanks. This gas is used as refrigerant and it follows a path through the aircraft components and passengers' cabin. Subsequent to have mixed the remaining gaseous hydrogen, the fluid is compressed to cool down the propulsion plant and the air pack; at the end of the process, it is expanded through a turbine to provide mechanical power and eventually, injected into the combustion chamber. In parallel, there is second path dedicated to the liquid hydrogen circuit: here, the liquid is compressed by a pump and before the expansion, it is flown into the specific regenerator to refrigerate the propulsion plant.

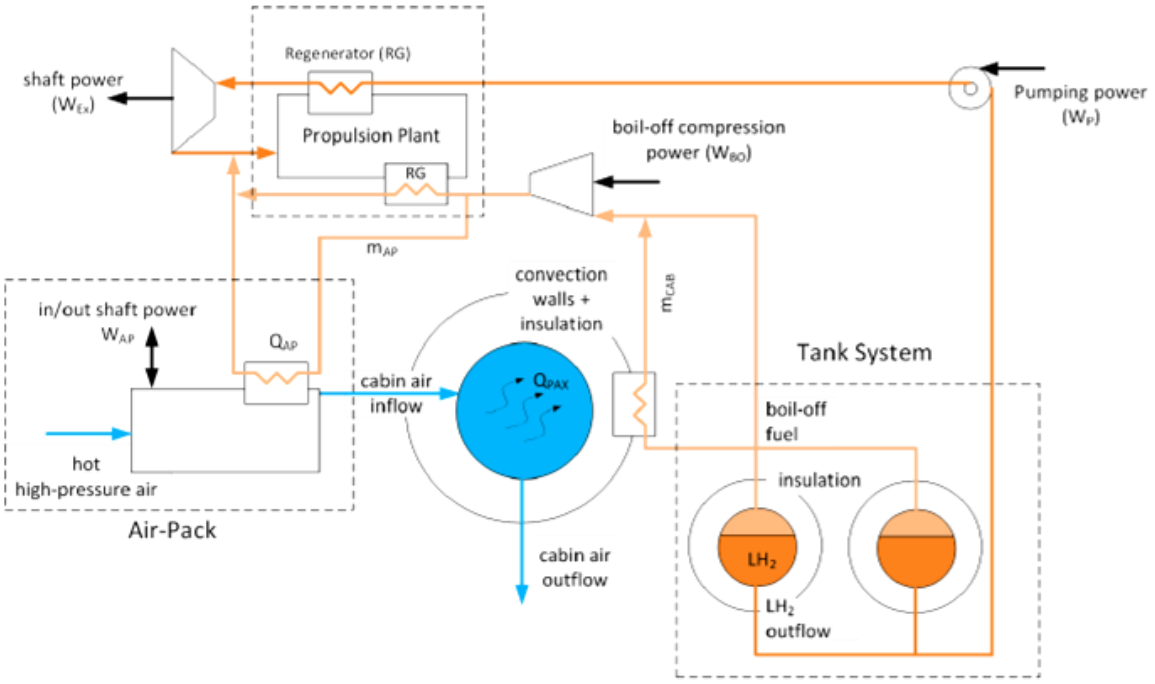


Figure 4.1 Scheme of the TEMS in MR2 vehicle [16].

Next stage consists in collecting the outlined failure conditions from the FHA and selecting each single circumstance to become the top event of a Fault Tree.

The four significant conditions, concerning the TEMS, are summarized here:

- Loss of the capability to sustain thermal loads (Figure 4.2);
- Loss of the capability to cool engines (Figure 4.3);
- Loss of the capability to cool systems (Figure 4.4);
- Loss of the capability to cool the primary structure (Figure 4.5).

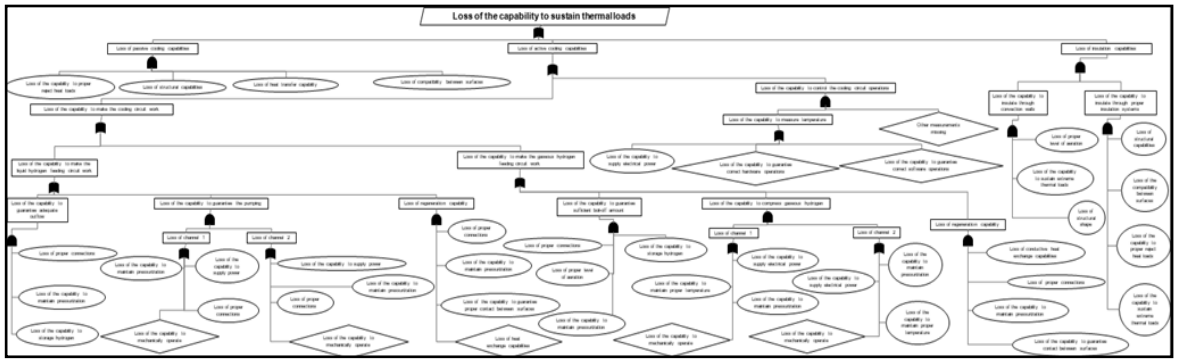


Figure 4.2 Loss of the capability to sustain thermal loads.

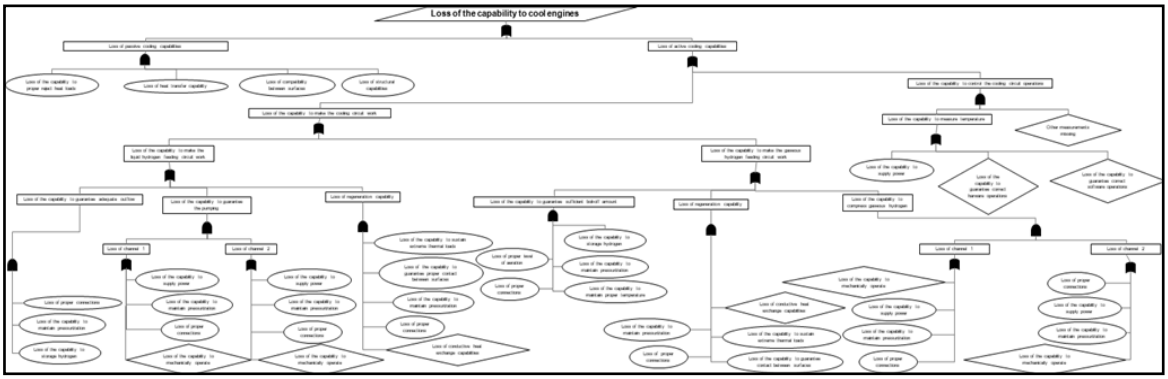


Figure 4.3 Loss of the capability to cool the engines.

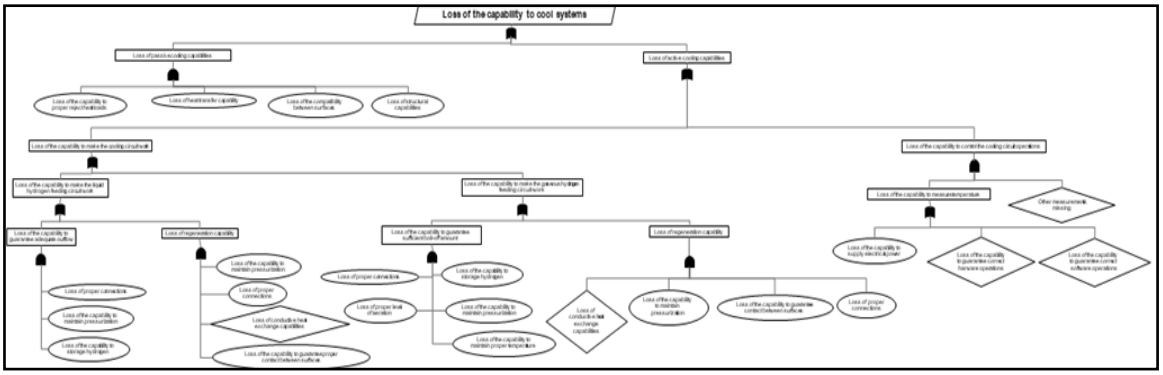


Figure 4.4 Loss of the capability to cool the systems.

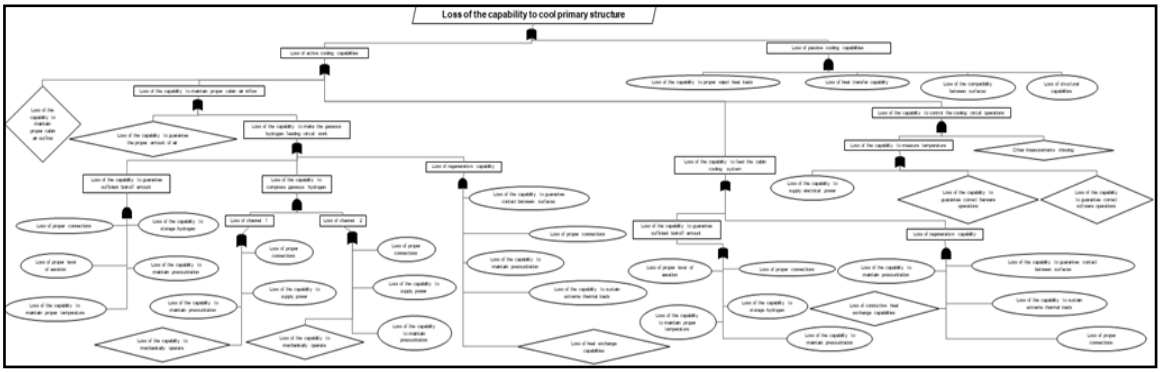


Figure 4.5 Loss of the capability to cool the primary structure.

A space Thermal Control System is normally composed of two sectors: the first one is the active cooling system, the latter is the passive one, linked, for example, with insulating materials or refrigerant phase-change fluids installed in heat pipes.

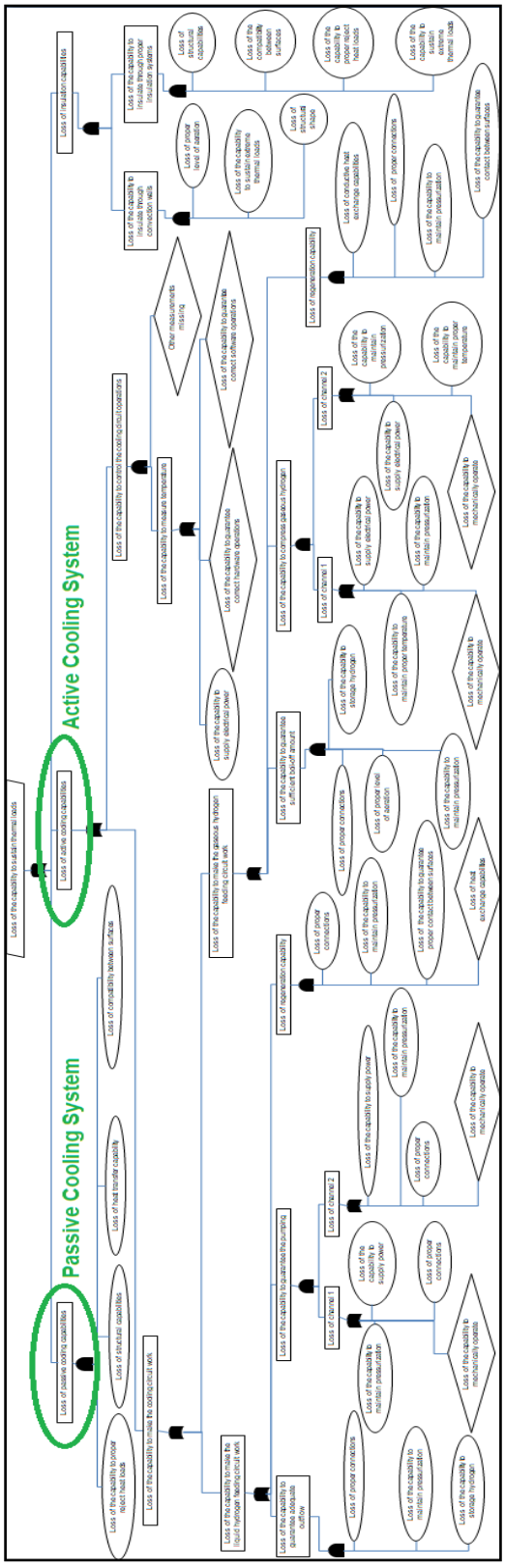


Figure 4.6 Detail of the active and passive system in the FT.

The first aim is to analyse, step by step, the suitable low level causes of the upper event. An "inefficient cooling capability" is due to the loss of active or passive thermal system. The case of losing the passive system concretely means that materials (coatings, mirrors, radiators, ...) or refrigerant fluids cannot guarantee the capability to insulate from thermal loads and to perform a "partial" refrigeration; on the other side, an active system will lose its functionalities, if its components (pumps, electric heaters, electric coolers, ...) do not operate to assure the cooling capabilities. The next phase is to accomplish, to find intermediate events and to perform the analysis up to the bases, i.e. until the outlined events that are considered the lowest for this phase of study.

Checking each single failure condition, here is an example of the way of reasoning to develop and obtain the basic events[15] of the FTA is here discussed.

The first failure event is the most complete of those outlined before, and it consists of the loss of all the possible way to maintain thermal equilibrium inside the aircraft: differently to the other conditions, it includes a reference to the thermal protection and shielding sector of the Thermal Management System. In particular, this condition is the one referring to the capability of the whole hypersonic vehicle to sustain thermal loads, which it must face during acceleration phases and cruise. Actually, the most dangerous thermal loads from the inside have a risky impact on the vehicle, while it is performing the hypersonic cruise, because DMR engines is active; other significant high thermal loads come from the external space, they are caused by friction due to the high reached speed.

In the diagram of this failure condition all the characteristics of the Thermal and Energy Management System are mostly summarized. As early discussed, the main aspect is to divide the functionalities between an active and a passive system: the active one starts to work in case of loss of efficiency of the passive one. The active one is, then, divided in two sectors: the loss of the circuit functionalities and the loss of Thermal Control System. Examining deeper, the whole cooling circuit is built by the liquid hydrogen path and the gaseous one.

It shall be highlighted that the active part (in the cooling circuit there is a compressor or a pump) involves a process that is spontaneous as well: the boil-off of the liquid hydrogen.

[15] All the identified events which are not close-connected to the Thermal System have been classified as "undeveloped events" because their analysis involves mechanical and/or computer science, that is not the purpose of this document.

Starting with a pressurized tank of liquid propellant, a piping system conducts gaseous hydrogen to a compressor and, subsequently, to the exchanger in contact with the engine walls. In parallel, a path for the liquid hydrogen is installed, being characterised by using the same pump of the propellant system. Three relevant aspects are considered for pump and compressor:

- the regeneration capability,
- the compression/pumping capability,
- the capability to guarantee the proper fluid flow.

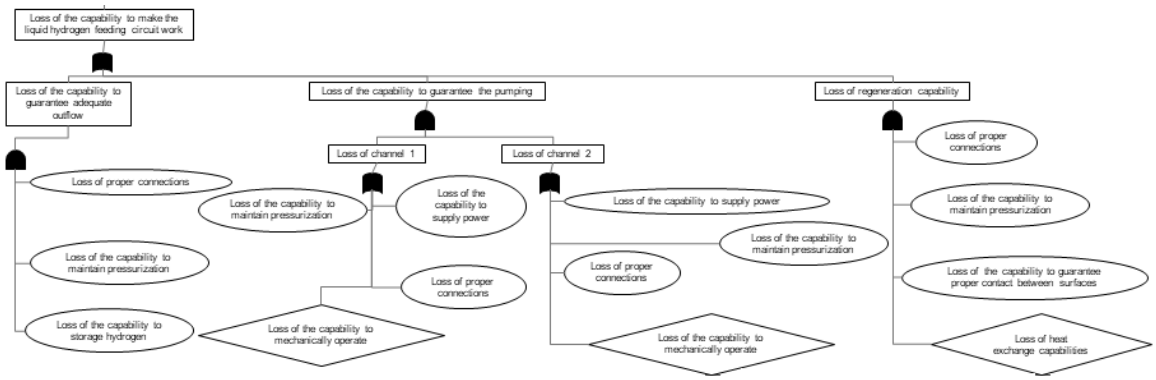


Figure 4.7 Details of the liquid circuit in the FT.

Concerning the Thermal Control System, the loss of the possibility to monitor temperatures is highlighted because of the lack of electrical power or malfunctions in the measure equipment; the assistance of other measures, such as data from level sensors or flow sensors, are evaluated as undeveloped event.

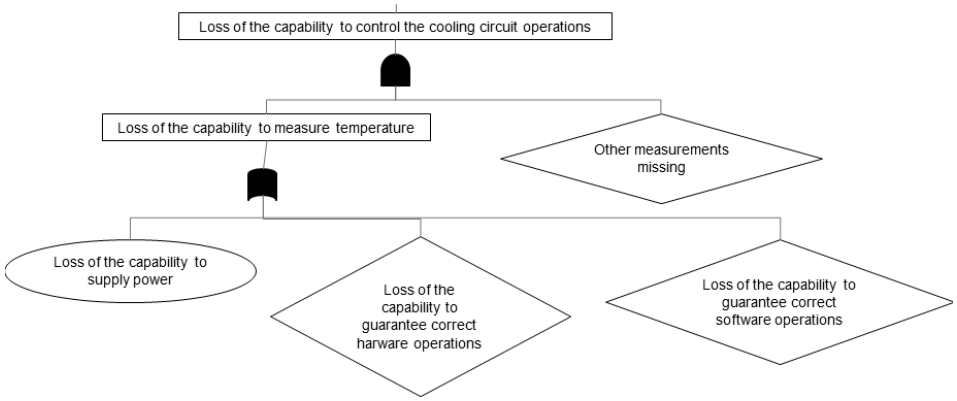


Figure 4.8 Detail of TCS in the FT.

In parallel, a sector dedicated to the passive system and to the protection system have been stressed. The TPS is related to the capability to insulate the aeroshell from the external environment, which could fails, if convection walls systems or shielding panels do not maintain their properties. In this diagram this part is linked to the top event as third main branch (Figure 4.9).

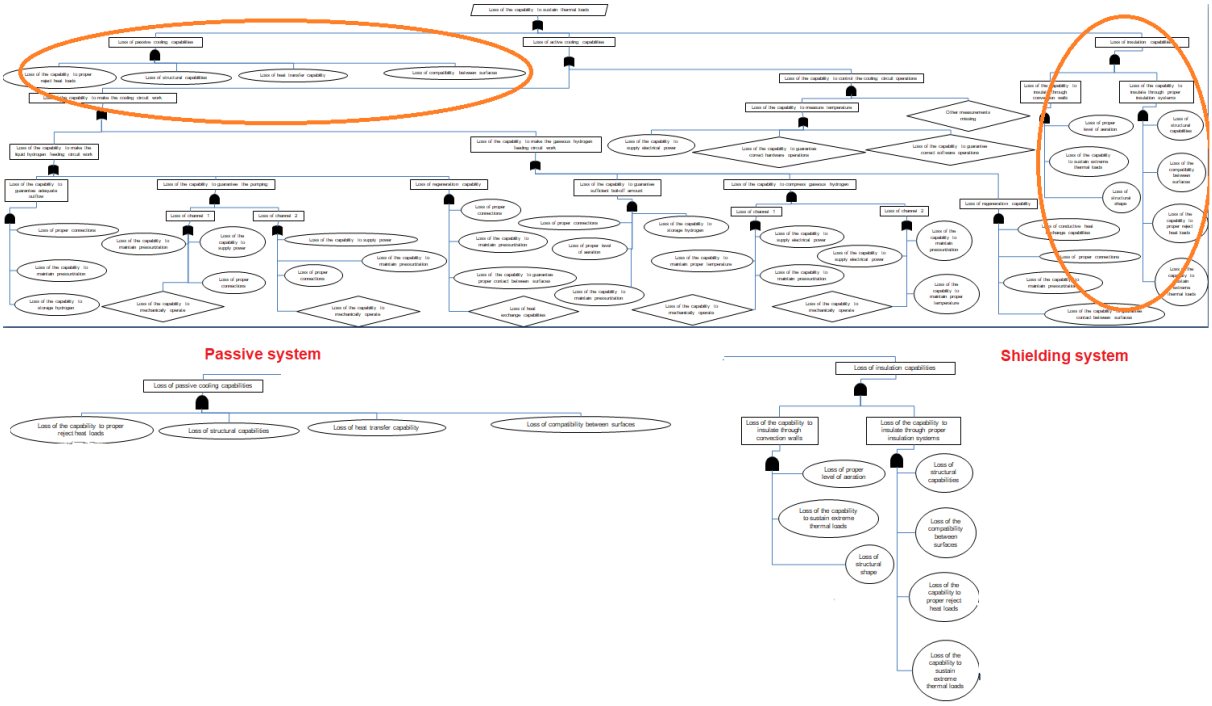


Figure 4.9 Detail of passive cooling system (left) and Thermal Protection and Shielding System (right) in the FT.

The second condition concerns the capability to effectively cool the engines (and air intake) during hypersonic cruise and acceleration phases. Here, the active system shall be exploited because the passive one cannot satisfy the Safety Requirements: as a matter of fact, the materials can bear maximum 1500°C but the temperature reached could overcome 2000°C (see air pack temperature [14]). At this point, to derive the FTA, the way of reasoning is almost equivalent as the one already exposed. The sector dedicated to the cooling circuit (liquid and gaseous) is the same displayed above, where the two different paths, with their three main elements, have been identified. Eventually, the part dedicated to the Thermal Control System and the specific sector of the passive cooling capabilities correspond to the previous paragraph.

Moreover, the third condition is similar but lighter than the second one because, in order to cool down the systems, the cooling power of the boil-off as it is created or the refrigerant capability of liquid hydrogen is sufficient. Here-hence, the main difference with the previous diagram consists in the absence of concrete active devices: however, as it can be noticed from the diagram, this part is classified as active cooling system because the cooling circuit is integrated in the more extended one and the operations are guaranteed with the assistance of equipment which, in any case, needs electrical power, such as pressure or temperature sensors.

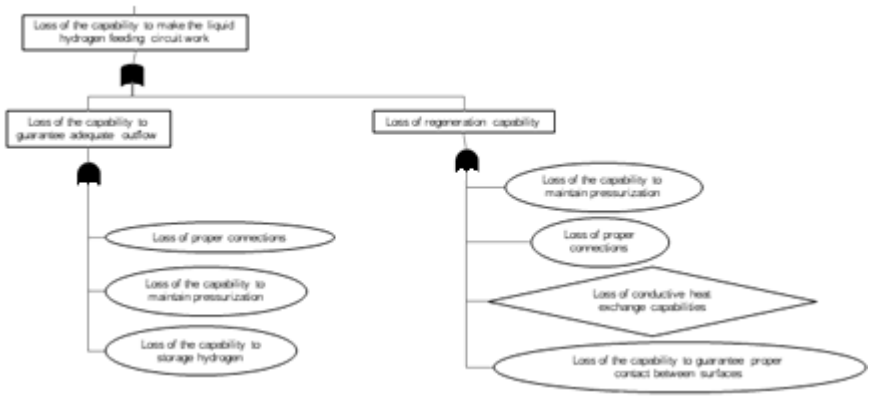


Figure 4.10 Detail of the liquid circuit of the FT: it is evident the lack of "real" active devices.

The last condition regards the cooling capability of the primary structure in order to maintain proper temperature inside the cockpit and the passengers' cabin. In this case, the liquid path is unnecessary, therefore only the boil-off hydrogen circuit is considered relevant. The presence of an inflow from the outside air with the possibility to take a spillage from the intake is the most significant point. This airflow is hot and at high pressure, for that reason, an heat exchanger is required before the amount of air is led into the cabin: the regenerator system exploits, as refrigerant, the compressed boil-off hydrogen to face extreme typical conditions of the air pack.

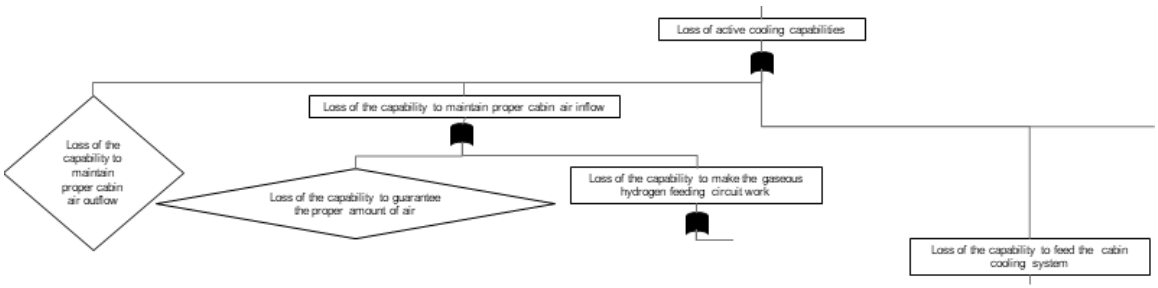


Figure 4.11 Detail of the FT of the failure condition "Loss of capability to cool the primary structure": it is underlined the introduction in cabin of new air and the recirculation.

On the other side, the "pure" boil-off hydrogen is used to cool down the convection walls of the cabin cooling system (Figure 4.12). Eventually, it is relevant to notice that, the amount of air into the cabin is continuously changed thanks to an outflow system[16] , here not further discussed [16].

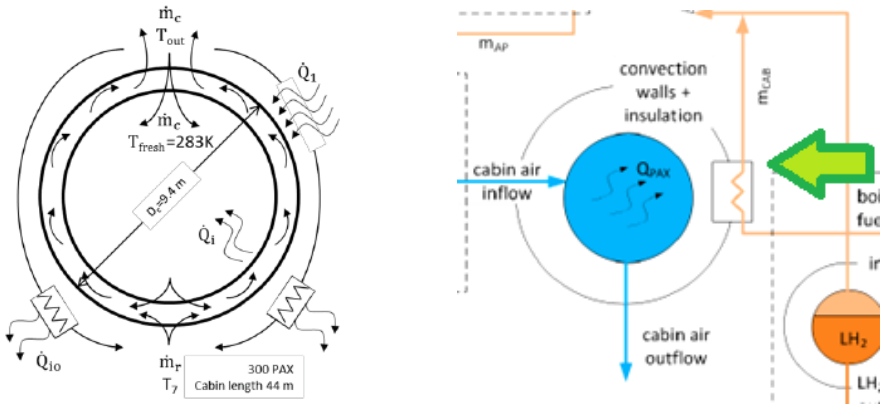


Figure 4.12 Recirculation of air inside the cabin (left) and regenerator for convection walls (right) [16].

It is interesting to observe that, the "active functionalities" , in other words, the capability to guarantee pumping and compression operation, are characterized by a "double channel": each channel is independent of the other one. The double channel provides a natural redundancy that will be further discussed: the loss of that capability occurs only if both channels fail.

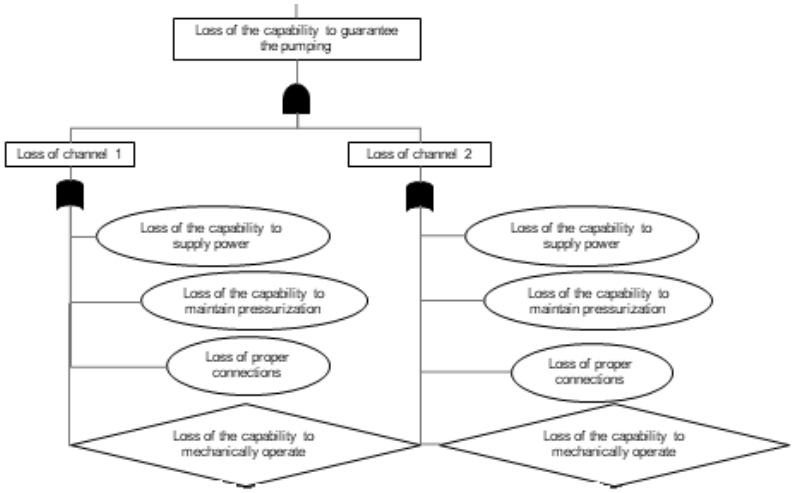


Figure 4.13 Detail of the redundancy in the FTA.

[16] For more details, see [16].

The final step at this level of the analysis is to derive, from the basic failure events, firstly new lower Functional Requirements: as example, if the failure event consists in *the loss of the capability to cool the engines*, the Functional Requirement will be *the system shall cool the engines*. This process has to be applied to all the outlined failure conditions identified during the development of the FTA for each top level event: at the end, the conclusive step is to further develop the Functional Tree (see Attachment D).

Successively, the lower level Function-Products Matrix and the specific lower components are derived: beginning with the physical scheme of the Thermal and Energy Management System, the already outlined lower functionalities are allocated to the proper component with the assistance of the specific tool, the functions-products matrices for each level of study. In this way, a list of equipment is gathered and, similarly to the process applied to the Functional Tree, the Products Tree must be further developed (see Attachment F).

The Products Tree is also useful to specify the Functional Requirements, this implies an higher level of accuracy, because instead of using the generic stereotype "system", the requirement could be written more precisely as, for example, *the* ***Tems*** *shall cool the engines*.

In this way of thinking, the significant outcomes are four parallel FTA related to products failures rather than loss of functions (see Attachment G).

In conclusion, the specific device failure is useful in the following bottom-up analysis, in order to have a quantitative reference related to the potential failure rate of that component: this value will be compared with the probability to happen (considered as Safety Requirement) that will be allocated to each failure event, after the procedure described in the next Section.

4.2.2 Failure rate allocation with a top-down approach

To accomplish the top-down approach, the next phase is to allocate the established top-level requirement to the lower levels event until the basic ones.

The four catastrophic events must be extremely improbable conditions, so their probability to happen has to be of *$1*10^{-9}$ failure/FH or less* [11].

Starting from the top event, which has to satisfy the requirement already cited, the following step is to allocate the probability to the lower event, until the bases, in order to obtain new requirements, as numerical probability, in accordance to the lower failure conditions.

The top-down allocation process has been performed following the diagram branches, evaluating the relevance (as a sort of weighted average) that each single outlined event of the tree has to the upper one and, at the end, applying the Boolean Algebra rules related to the AND/OR gates[17].

In the following sections the allocation process for each Fault Tree is summarized. The complete diagrams characterized by the final allocated values are gathered in Attachment C.

❖ **Loss of the capability to sustain thermal loads**

In this condition, the top-level probability has to be divided into three branches: it has been estimated that Passive and Thermal Protection and Shielding System have equal importance, three times lower than the active system, therefore the relation among the system is numerically represented as 1:1:3 for the active one.

In the same way, a "weighted ratio" per each branch has been derived and has been evaluated the probability of each event to happen. Here, all the significant weights are collected.

Taking into account, firstly, the passive system, the lower failure events have been estimated to have the same relevance; the Thermal and Protection System has been evaluated equally, therefore each event has the equivalent importance as the other conditions at the corresponding level.

[17] For more details, see Appendix A.

The active system is more sophisticated. The first branch has a ratio of 5:1 related to the active circuit, in comparison with the Thermal Control System; in the ramification of the Thermal Control System, the temperature sensor has five more importance (5:1) than the other sensors (level or flow sensors) and the loss of electrical power has double relevance compared with the loss of hardware or software operation (2:1:1). Considering the active circuit, liquid and gaseous circuit have equal weight. The liquid circuit is uniformly divided in three conditions:

- The capability to guarantee adequate outflow is composed of three events, where the capability to storage hydrogen in the tank has three times less importance than the other events (1:1:1/3);
- The capability to guarantee the pump operation is composed of four events, where the mechanical failure condition has half relevance than the others (1:1:1:1/2);
- The capability to refrigerate through liquid hydrogen concerns four events, where the loss of proper connections and loss of pressurization inside the circuit have half weight in comparison with the loss of proper contact between the regenerator surfaces; loss of heat exchange capabilities is related to mechanical rupture, so has four times lower weight (1:1/2:1/2:1/4).

Almost in parallel, the gaseous circuit is equally divided in three conditions:

- The capability to guarantee proper boil-off is composed of five events, in which the capability to guarantee proper connection and pressurization have identical weight, the capability to storage gaseous hydrogen is three times less relevant, the capability to guarantee aeration is five times lower and the capability to maintain proper temperature has been estimated half significant (1:1:1/3:1/5:1/2);
- The capability to guarantee compression has twin branches as the pumping capability;
- The gaseous regenerator is parallel to the liquid one.

❖ **Loss of the capability to cool engines**

The function "to cool engines" is similar to the previous one except for protection system, which is not involved here. In addition, the passive system acquires more relevance: the first branch between active and passive system is here characterized by a four times higher value for the active one (4:1).

In parallel, there is a new essential capability regarding the regenerators: actually, the regeneration system has to bear extreme thermal loads originated from engines or intake: it has been estimated that this event must have half probability to happen in comparison with the most dangerous event, concerning the loss of the capability to maintain contact between the regenerator surfaces (the numerical relation is thus formalized 1:1/2:1/2:1/2:1/4).

❖ **Loss of the capability to cool primary structure**

In this case study, the capability to cool down the cabin and to maintain acceptable internal conditions has been considered. The passive system acquires more significance, therefore it has been weighted as 2/3 important in comparison with the active one (there is no thermal protection system also here).

The other relevant aspect is, the subdivision of the active system in four branches[18]:

- Loss of the capability to maintain proper cabin air outflow;
- Loss of the capability to maintain proper cabin air inflow;
- Loss of the capability to feed the cabin cooling system;
- Loss of the capability to control the cooling circuit operations.

The value of these conditions have been weighted as 1/4:1:1:3/4. Moreover, the second event is divided into two branches, where it has been estimated that the undeveloped event "the loss of the capability to guarantee the proper amount of air" weights three times less than the event "loss of the capability to make the gaseous hydrogen feeding circuit work". The other relations are corresponding to the already discussed (the reference is the condition "Loss of the capability to sustain thermal loads", p. - 61 -) .

❖ **Loss of the capability to cool systems**

This capability is less sophisticated. The weights are similar to those already established; the passive system has 2/3 of significance in comparison with the active one. Eventually, there are no real active component, therefore liquid and gaseous circuits are constituted only by the outflow path and liquid regenerator as well as boil-off path and gaseous regenerator respectively; the importance is equally distributed.

[18] For more details, see Chapter 4.2.1.

At this point, considering step-by-step the previous estimated weights, the value of the rate related to all the possible failures has been computed, starting from the main requirement of the top level events, whose likelihood to occur must be less than 10^{-9} failures/FH.

4.2.3 Subsystems Functional Requirements

Performing this phase, Functional Tree has been further developed and deepened on the requirements that TEMS has to satisfy. Each failure condition has been used to derive a lower level function and, thanks to the assistance of a lower level functions/products matrix, Functional Requirements could be written in a more detailed way: this step is relevant because allows to identify lower level specifications.

The derived functions have been gathered in the proper tree[19] and allocated to the suitable device.

It is coherent that, the Products Tree will be further developed (see Attachment F).

The whole functional diagrams are available in Attachment E but here, some details concerning the function allocated to Thermal and Energy Management System "*The Tems shall cool the engines*" have been collected to illustrate the main branches.

The tree branches start from the system level function concerning the Thermal Management System "*to maintain thermal equilibrium*". The following phase is to derive, from the outlined FHA, lower functionalities to obtain new specifications: in these details, only the failure condition "*Loss of the capability to cool the engines*", allocated to TEMS and developed as "*the TEMS shall cool down the engines*" is discussed.

The second level of the sub-system functions is illustrated in the Functional Tree in Figure 4.14, where from the function "*to cool engines*", have been improved into two sub-functions, "*to guarantee engines active cooling*" and "*to guarantee engines passive cooling*".

Figure 4.14 Detail of the first sub-system level (Functional Tree).

Figure 4.15 shows passive cooling "level" and its lower level sub-functions.

[19] see Attachment D for the whole diagram and E for the details of the Functional Trees related to the four main failure conditions.

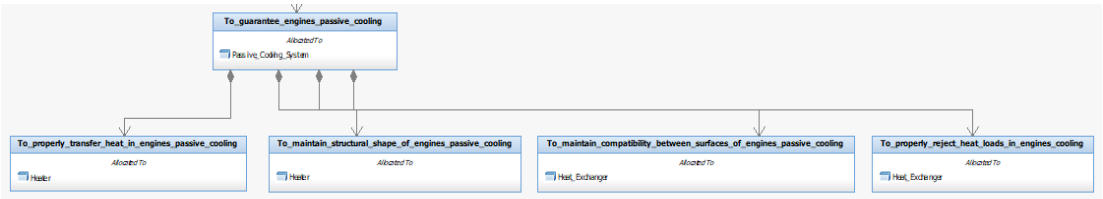


Figure 4.15 Detail of the passive cooling branch (Functional Tree).

The Figure 4.16 displays the third sub-function level, specifying the branch related to the active cooling: it has been divided into the cooling circuit and the cooling control system.

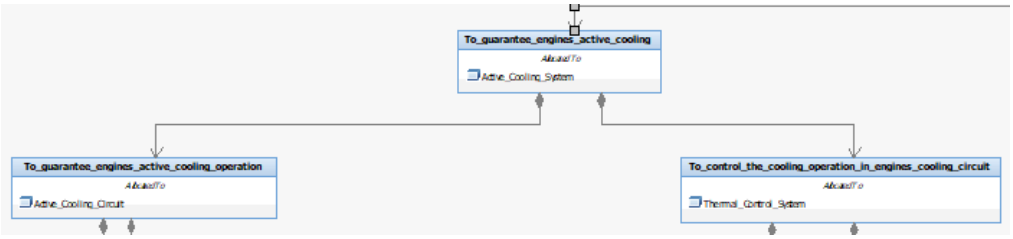


Figure 4.16 Detail of the active cooling branch (Functional Tree).

In Figure 4.17 , the next level based upon the function related to the cooling control system is highlighted: the diagram has been further developed from the previous cited function "*to control the engines cooling operation*".

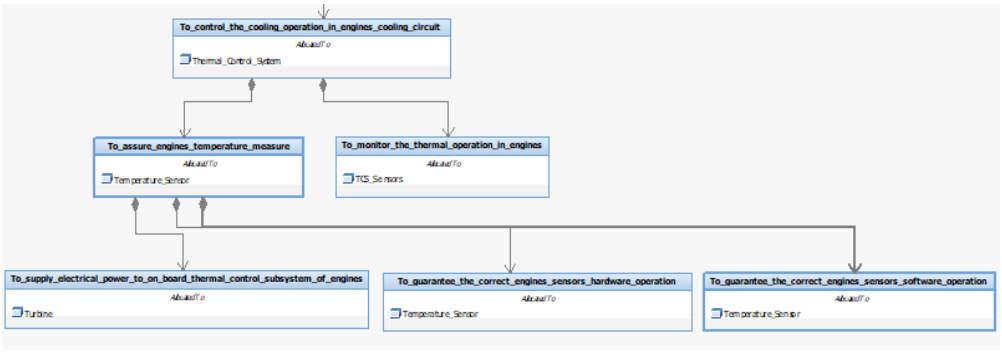


Figure 4.17 Detail of the Thermal Control System branch (Functional Tree).

Figure 4.18 instead, exhibits the fourth level connected to the cooling circuit. The functions have been developed focusing on the cooling circuit operation.

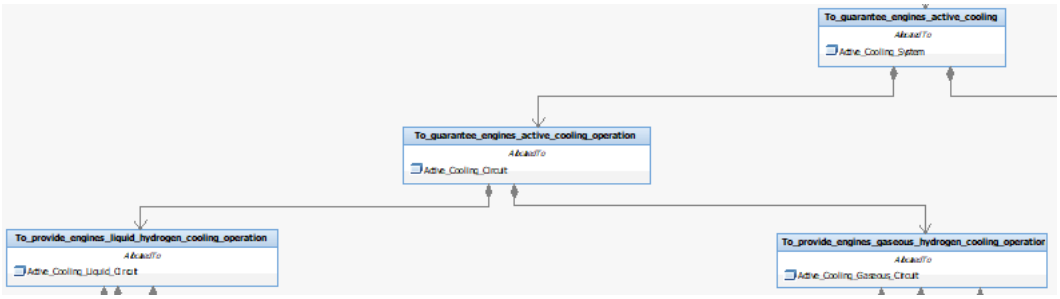


Figure 4.18 Detail of the active cooling circuit branch (Functional Tree).

Next figures illustrate in a closer way, the details of the cooling operation divided in liquid (Figure 4.19) and gaseous circuits (Figure 4.20), in which the three branches related to the outflow circuit (or boil-off circuit), the pumping/compression system and the regeneration system and their lower functionalities appear.

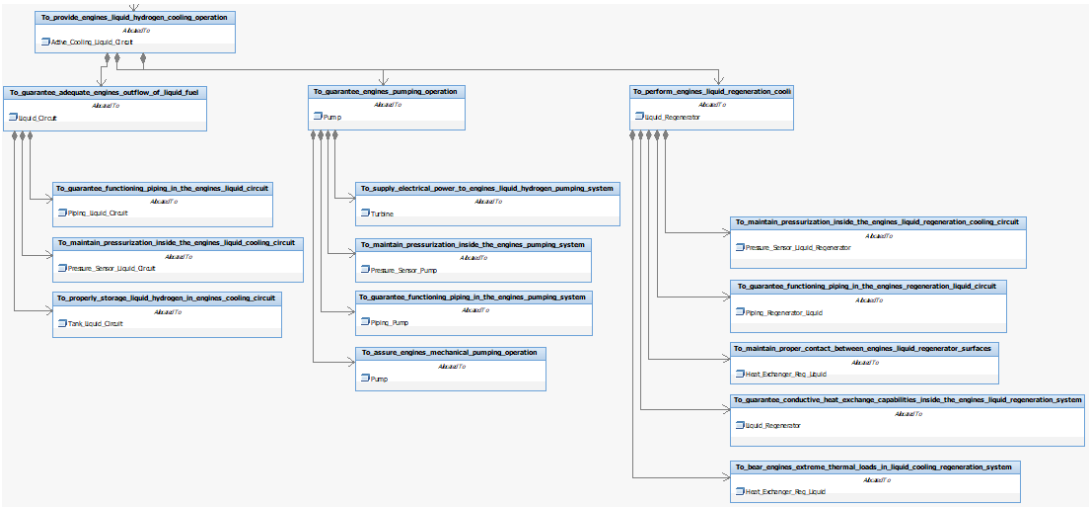


Figure 4.19 Detail of the active liquid cooling circuit branch (Functional Tree).

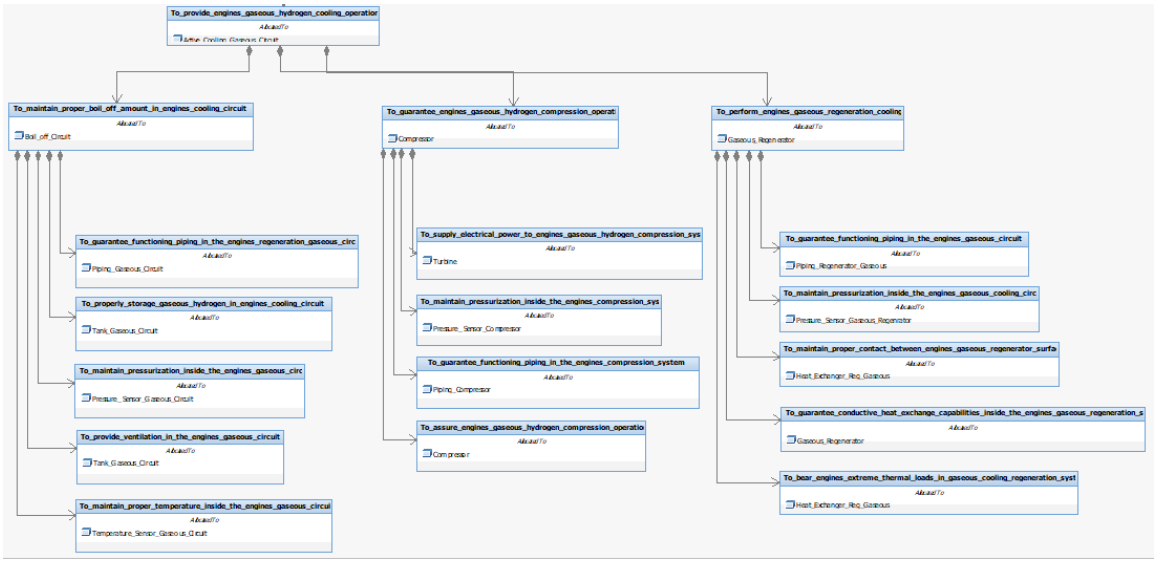


Figure 4.20 Detail of the active gaseous cooling circuit branch (Functional Tree).

Here, some example of the Products Tree have been grouped: each device could perform different functions as Figure 4.22 clearly shows. Each box of the Products Tree contains the functions, which the specific device has to accomplish: evidently, the allocation has to respect the design level as Figure 4.21 shows.

The Products Tree is a valuable tool because it allows immediately identifying which are the relevant components in the project and which tasks they have to perform.

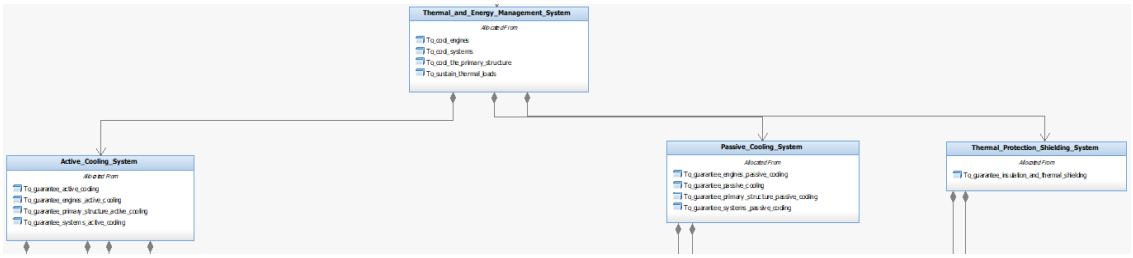


Figure 4.21 Detail of TEMS level (Products Tree).

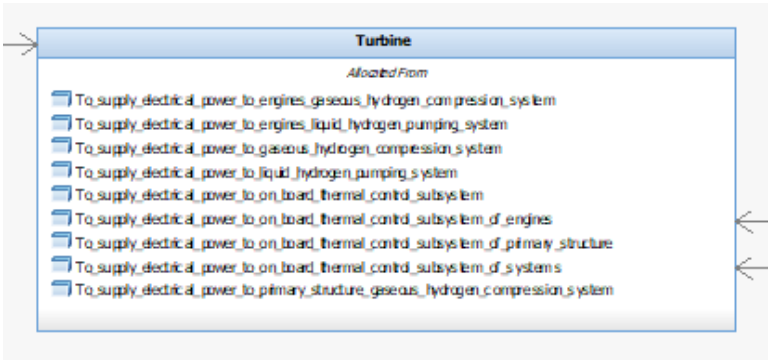


Figure 4.22 Example of the allocation of functions to the suitable device, in this case the turbine accomplish the function "to supply electrical power to..." (Products Tree).

4.2.4 Safety Requirements

The final outcomes of the top-down analysis are the Safety Requirements, stating the probability to happen of each single and independent event. They are placed beside the sub-systems level Functional Requirements and gathered into a well-organized list, in order to trace the steps and to immediately find relevant data. In actual fact, the real significance of this list is to have a numerical value of a requirement, which acts as a sort of constraint: Safety Requirement is associated to each Functional Requirement and every event must occur with a probability less than the one established. In this way only, the specification is satisfied. The numerical value of the Safety Requirements comes from the allocation operation previously performed and, subsequently, the safety specification could be clearly formalized.

The list of the Functional Requirements related to the Thermal Management System and the respective Safety Requirements is included in Attachment H.

4.3 Evaluation of RBD of TEMS

Beside the numerical results which attest the satisfaction of the requirements, it could be also carried out, evaluating the Reliability Block Diagram.

Components that are part of system must operate and cooperate each other to guarantee suitable integration and reach the mission. The interface among components could be physical or logical and they could be underlined in different flowcharts. The conceptual difference between a physical diagram and the functional one is that, the first shows how the equipment or system components are installed; on the other side, the RBD highlights, coherently, the system from a reliability point of view, it means, focusing on the influence that a failure could have to the functionalities of other components or to the whole system. The most "famous" connection models are series or parallel links among devices in order to point out how the whole system works.

For example, considering a system composed by two other subsystems:

- The subsystems are linked in series, if the failure of one of them causes the loss of the functionalities of the system;

Figure 4.23 Series scheme: if x2 fails, the system will not work.

- The subsystems are linked in parallel, if the failure of one of them does not cause any other malfunctions because one active element guarantees the functionality.

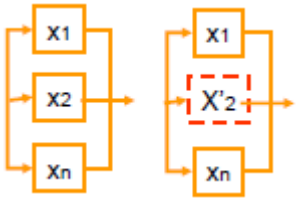


Figure 4.24 Parallel scheme: if x2 fails, the system will work.

Figure 4.25 displays the already seen scheme of the physical installation of the devices that constitute the TEMS; on the other side, in Figure 4.26 the functional diagram of the Thermal Management System of MR2 related to the failure condition "*Loss of the capability to sustain thermal loads*" is illustrated.

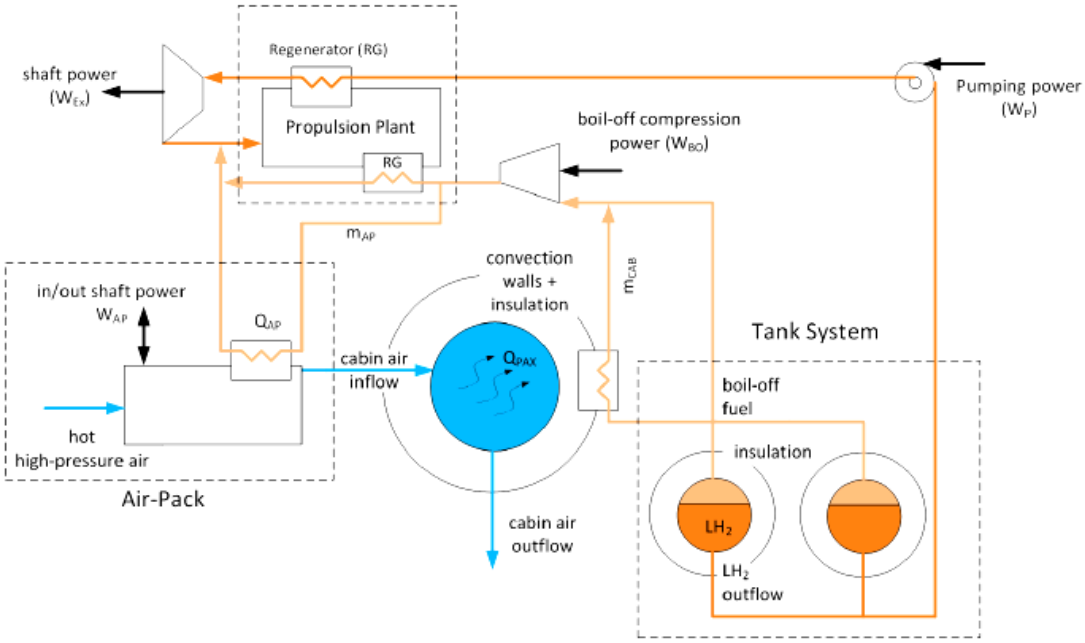


Figure 4.25 Physical scheme of MR2's TEMS [15].

At first glance, it is noticeable that the two kind of diagrams are completely dissimilar, therefore any sort of parallelization is unsuitable.

However, it is worth looking into several points which merit consideration: they will be underlined indeed in the following pages.

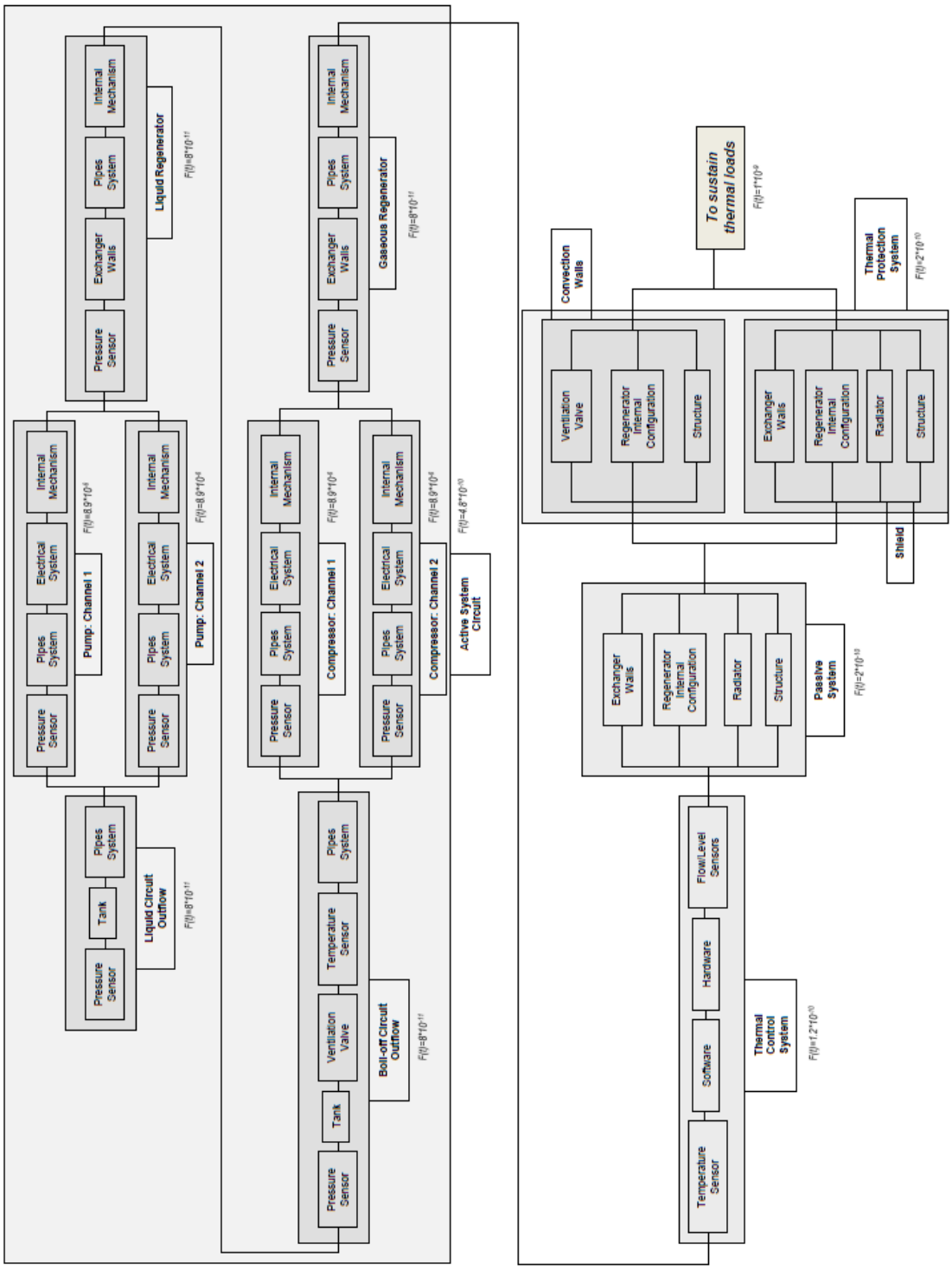


Figure 4.26 RBD of TEMS: "Loss of the capability to sustain thermal loads".

Reminding the failure conditions "*Loss of the capability to sustain thermal loads*" is the most "comprehensive" event, its FTA and consequently its RBD in Figure 4.26 has been useful to make the most appropriate comparisons with the physical scheme; in the next pages the RBDs concerning the other failure conditions are displayed all along.

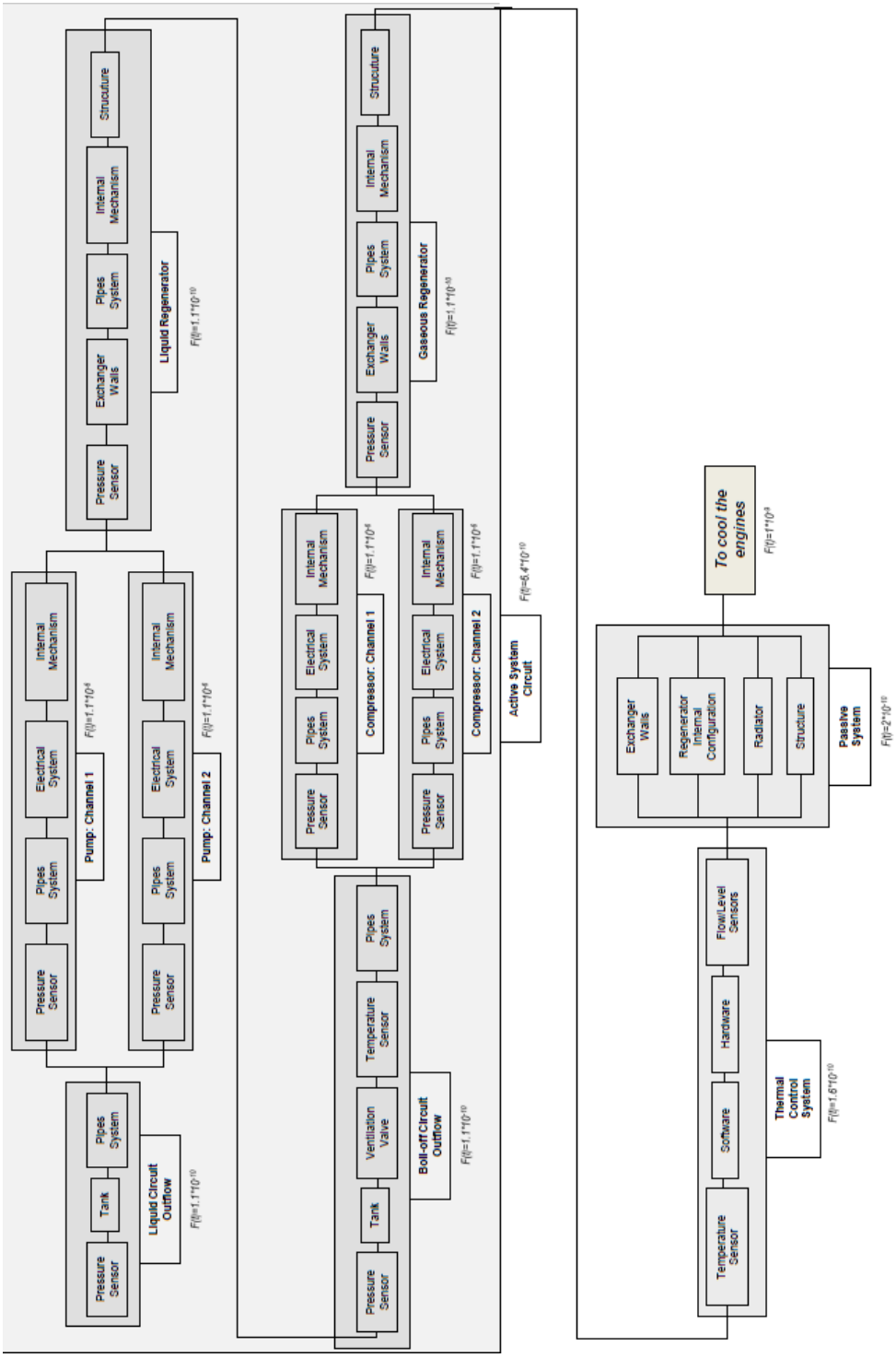


Figure 4.27 RBD of TEMS: "Loss of the capability to cool the engines".

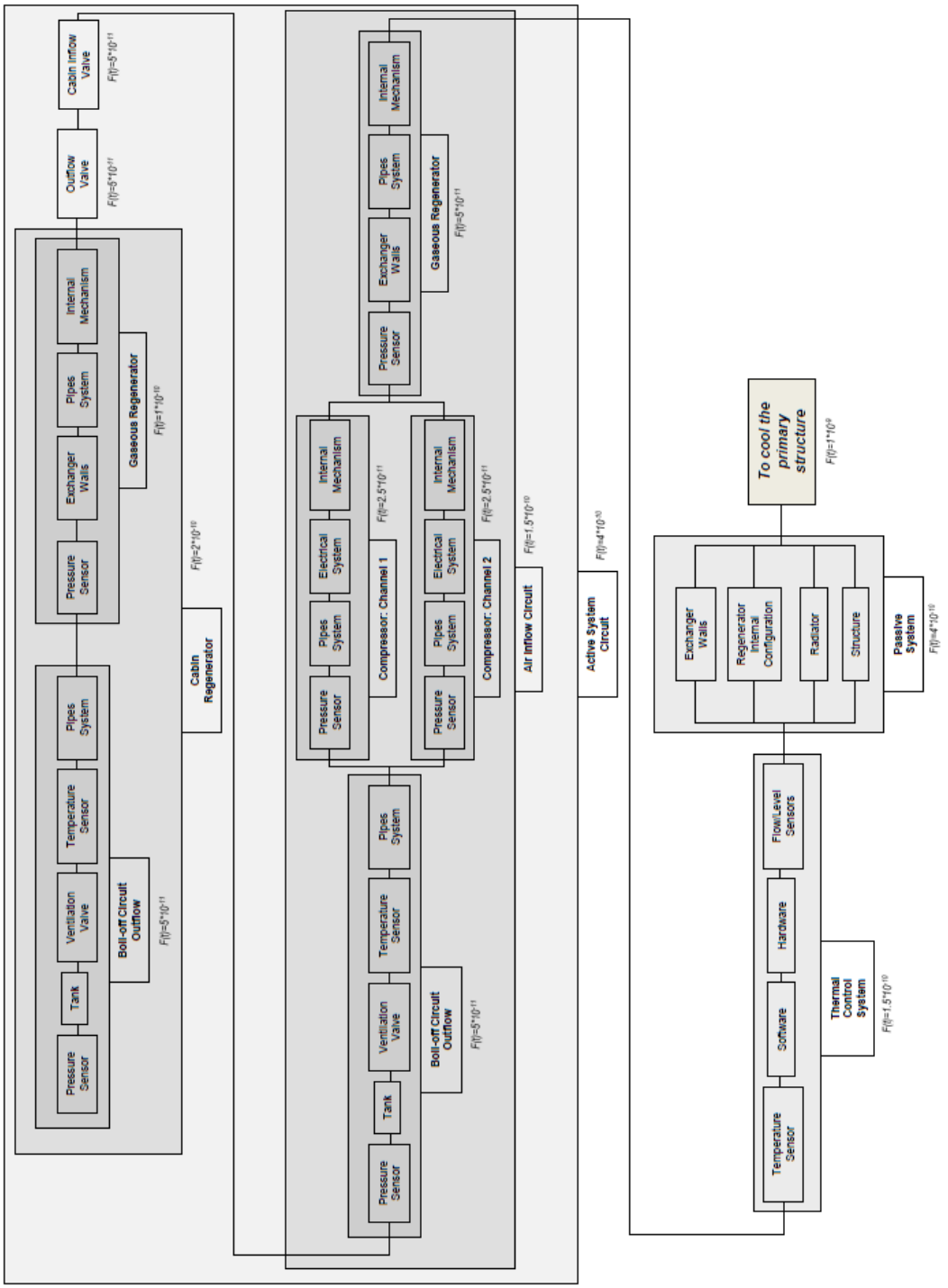


Figure 4.28 RBD of TEMS: "Loss of the capability to cool the primary structure".

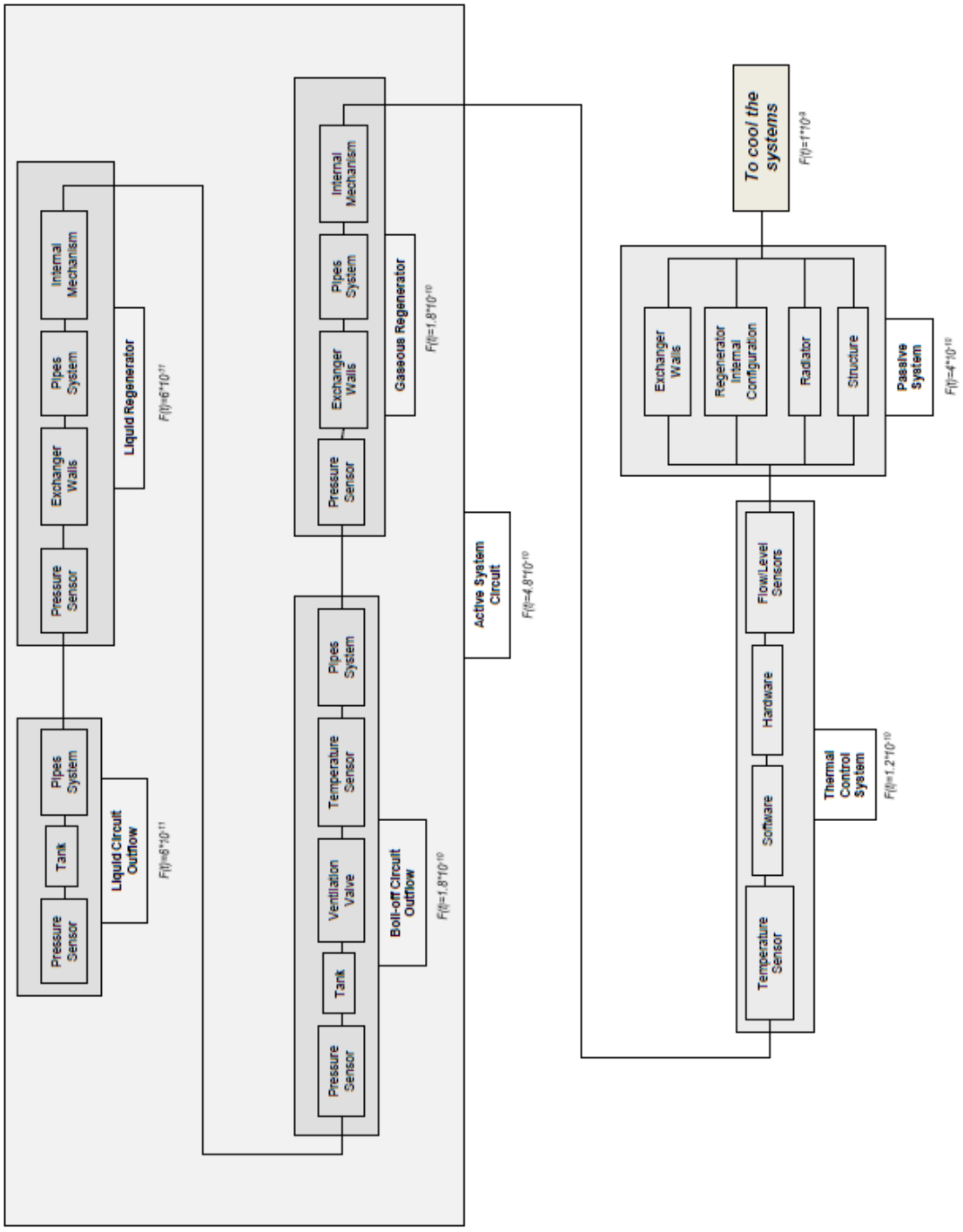


Figure 4.29 RBD of TEMS: "Loss of the capability to cool the systems".

In this specific case, there are lots of useful information according to the TEMS operation that are missing in the physical diagram if the point of view of the study is the Reliability.

Firstly the RBD shows, the whole Thermal Management System operates if all its parts work: this means, Thermal Active System, Thermal Passive System and Thermal Protection and Shielding System are linked in series, therefore they have not to be damaged because the failure of one of them could compromise the mission. This fact could not be compared with the physical scheme because it is focused on underlining only the specific TEMS section and not all the Thermal Management System. Passive and Thermal Protection and Shielding Systems are more reliable in comparison with the active one because they are envisaged as constituted of parallel links. In this case, there are not comparable point with the designed physical scheme.

Looking closer at the active system instead (in the RBD), it is mostly characterized by series connections. In this sense, the probability of failures due to the active system is higher because the failure of one device causes the failure of the whole system. From the Safety Analysis, it has been established nonetheless that, the majority of the equipment must be sufficiently reliable to satisfy the requirements: the riskiest devices are the pump and the compressor. In the Reliability Block Diagram, these two elements lay in parallel to highlight the redundancy previously envisaged and set (see Figure 4.31).

Observing the physical scheme in Figure 4.30, the series link is not immediately noticeable: in fact, the liquid and the gaseous circuit "seem to be in parallel", that means, it is not necessary both circuit work to accomplish the requirement but, nowadays, it is even physically and technologically impossible to realize.

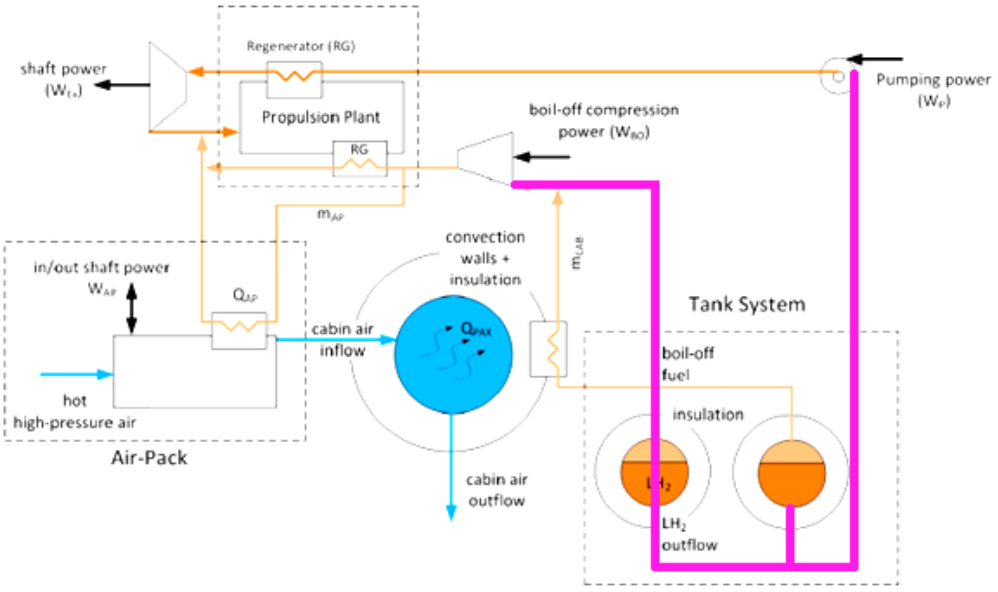


Figure 4.30 Detail of liquid circuit and boil-off circuit in the physical scheme.

There also another aspect, in the physical scheme redundancies are not highlighted as it is shown in Figure 4.31; in the functional graph the redundancies have been realized with a parallel link between the redundant elements.

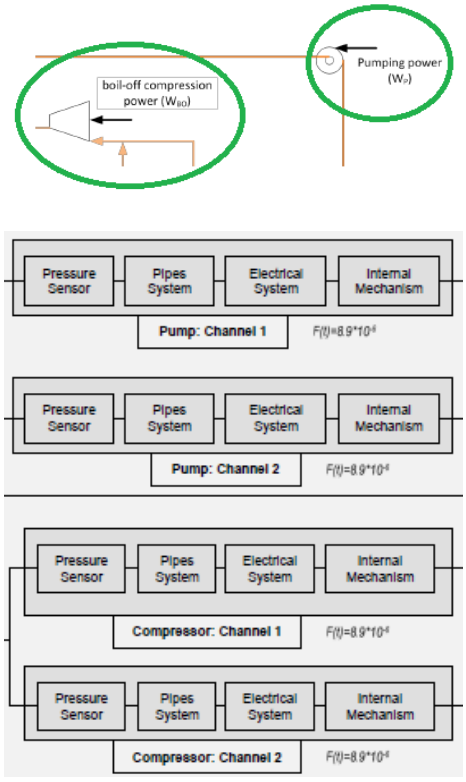


Figure 4.31 Comparison of physical (above) scheme and functional scheme with the detail of the redundancies of pump and compressor (below).

The same connection appears in the RBD concerning the TPS and the Passive System: it is intended to underline that, in this case, the aim is to show the system could work if only one sub-system works but it is not properly a redundancy because they are, actually, different devices.

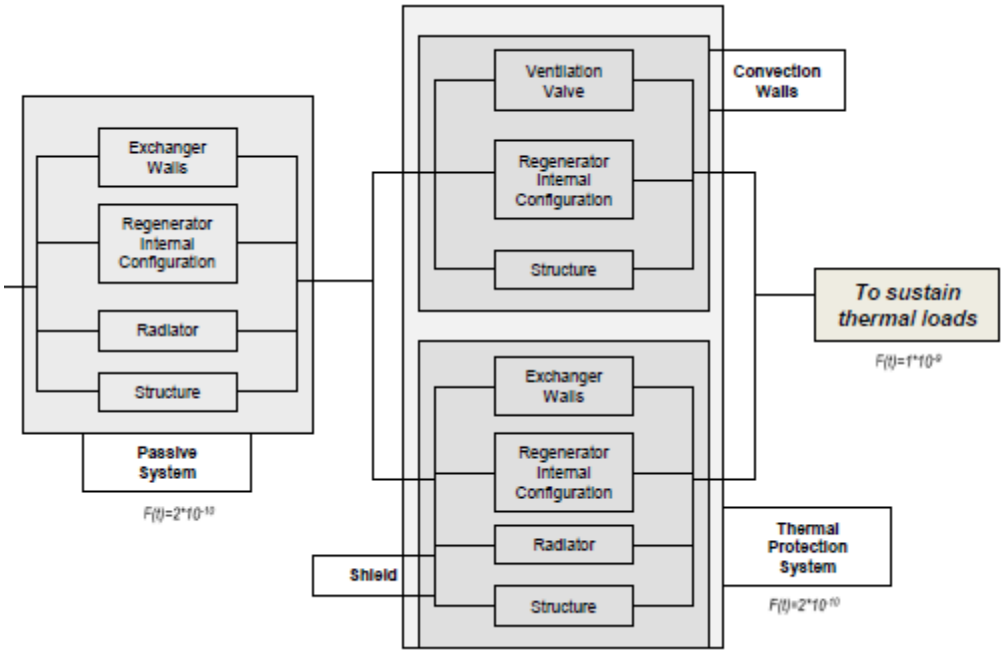


Figure 4.32 Parallel link inside the Passive System and the TPS.

In conclusion, pinpointing the numerical value settled in the RBDs, that is the failure rate expressed in *failures per flighthours*, it could be stressed the Reliability of that specific functionality, reminding that it is equal as the complement to 1 of the allocated failure rate [17]:

$$R = 1 - F(t).$$

In this way, it is possible to associate to each function its failure rate but also to have a reference of the reliability rate and to establish immediately that the system has to guarantee high level of Safety.

5 Quantitative Reliability and Safety Assessment

The following step is the procedure that is based upon the bottom-up approach: after having identified typical failure rates of devices collected in database, the main purpose is to follow backwards the levels, from bases to the higher ones, and evaluate the probability of the top event. This could be accomplished calculating the Reliability Equation, that is a logic expression which indicates the MCS (Minimal Cut Set). The MCS is the set of events that causes the system failure, if they happen simultaneously: if the values of the failure rates are substituted to the specific element in the equation and the equation is solved, the result is the likelihood of the top event. In the case that the probability evaluated from the MCS is less than the imposed safety constrain, the requirement is satisfied, conversely, some features have to be modified.

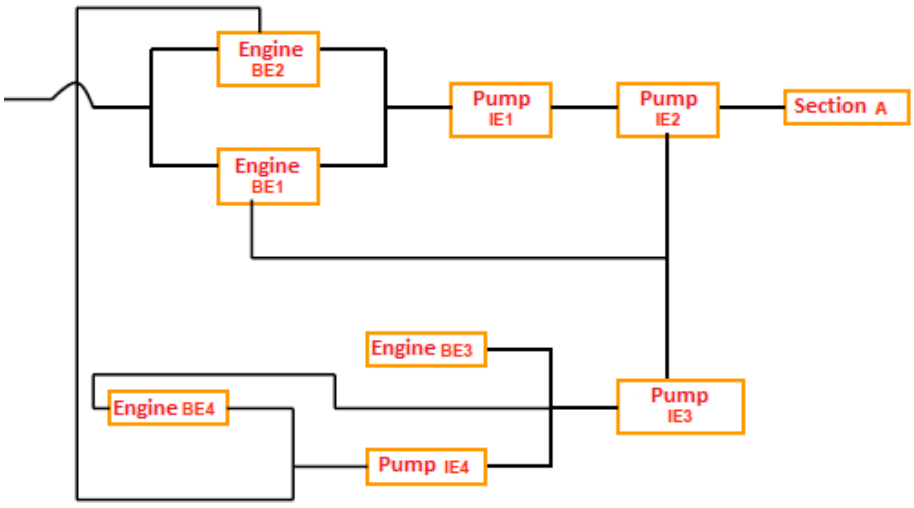


Figure 5.1 Example of a functional scheme of an hydraulic system architecture.

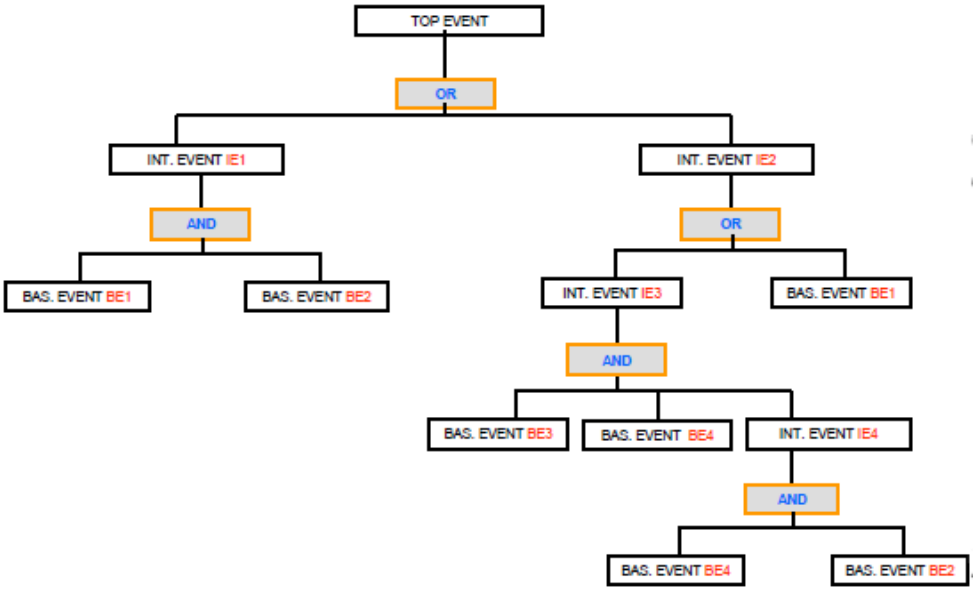


Figure 5.2 FT of the example of an hydraulic system architecture.

STEP	Boolean Expression
1	T= IE1+IE2
2	T= (BE1xBE2) + (BE1+IE3)
3	T= BE1xBE2 + BE1 + (BE3xBE4xIE4)
4	T= BE1xBE2 + BE1 + (BE3xBE4xBE4xBE2)
5	T= BE1 + BE1xBE2 + (BE3xBE4xBE2)
6	T= BE1 + BE3xBE4xBE2
7	**T= BE1 + BE2xBE3XBE4**

Solution: Minimal Cut Set

Table 5.1 Reliability Equation of an hydraulic system architecture.

5.1 Reliability Equations: application to TEMS of the MR2 vehicle

The steps performed in the example will be here applied to the failure conditions in order to obtain the final numerical expression to estimate the likelihood to happen of each top event. In Figure 5.3 is illustrated the FT of the first condition "*Loss of the capability to sustain thermal loads*", in a lighter shape in comparison with the one typical of the Systems Engineering. Reminding the list of abbreviations at the beginning of the document, it is possible to read the diagram and to derive the Reliability equation of the top event, constituted of the combination of basic events. The Table 5.2 shows the steps to achieve the final equation representing the MCS of the cited failure condition.

It is useful to remind that, the outlined failure conditions are:

- Loss of the capability to sustain thermal loads;
- Loss of the capability to cool the engines;
- Loss of the capability to cool the primary structure;
- Loss of the capability to cool the systems.

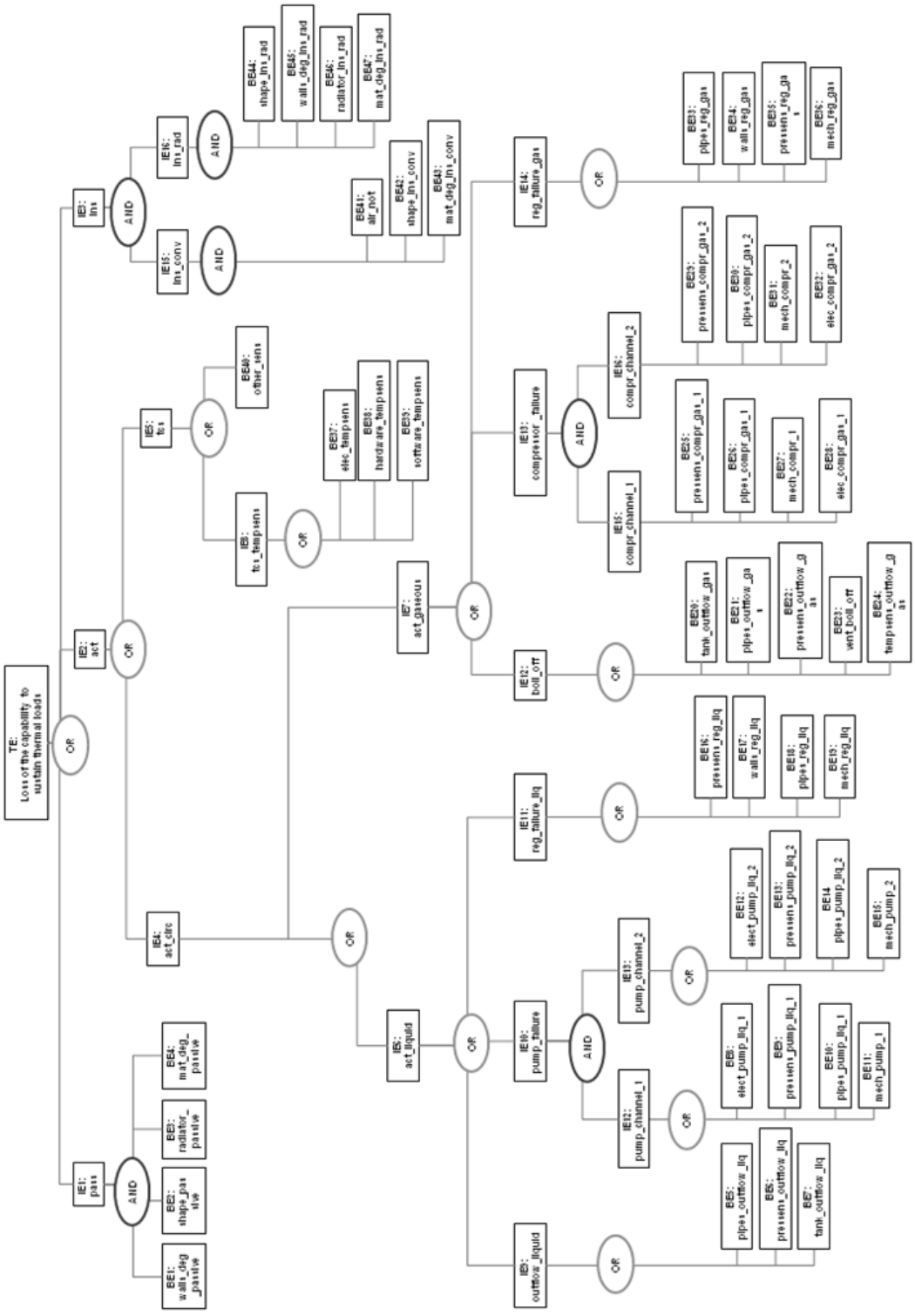


Figure 5.3 FT of the failure condition "Loss of the capability to sustain thermal loads".

STEP	BOOLEAN EXPRESSION
1	T=IE1+IE2+IE3
2	T=(BE1*BE2*BE3*BE4)+(IE4+IE5)+(IE19*IE20)
3	T=(BE1*BE2*BE3*BE4)+((IE6+IE7)+(IE8+BE40))+ +((BE41*BE42*BE43)*(BE44*BE45*BE46*BE47))
4	T=(BE1*BE2*BE3*BE4)+(((IE9+IE10+IE11)+ +(IE12+IE13+IE14))+((BE37+BE38+BE39)+BE40))+ +((BE41*BE42*BE43)*(BE44*BE45*BE46*BE47))
5	T=(BE1*BE2*BE3*BE4)+((((BE5+BE6+BE7)+ +(IE15*IE16)+(BE16+BE17+BE18+BE19))+ +((BE20+BE21+BE22+BE23+BE24)+ +(IE17*IE18)+(BE33+BE34+BE35+BE36)))+ +((BE37+BE38+BE39)+BE40))+ +((BE41*BE42*BE43)*(BE44*BE45*BE46*BE47))
6	T=(BE1*BE2*BE3*BE4)+((((BE5+BE6+BE7)+ +((BE8+BE9+BE10+BE11)*(BE12+BE13+BE14+BE15))+ +(BE16+BE17+BE18+BE19))+((BE20+BE21+BE22+BE23+BE24)+ +((BE25+BE26+BE27+BE28)*(BE29+BE30+BE31+BE32))+ +(BE33+BE34+BE35+BE36)))+((BE37+BE38+BE39)+BE40))+ +((BE41*BE42*BE43)*(BE44*BE45*BE46*BE47))

Table 5.2 Resolving steps to evaluate the MCS of the failure condition "Loss of the capability to sustain thermal loads".

Logically resolving that expression with the assistance of the typical Boolean rules and properties[20], the expression at the sixth step will be simplified and will become the following equation.

TE (To sustain thermal loads)=

other_sens*(elec_tempsens+hardware_tempsens+software_tempsens)+(elect_pump_liq_1+mech_pump_1+pipes_pump_liq_1+pressens_pump_liq_1)*(elect_pump_liq_2+mech_pump_2+pipes_pump_liq_2+pressens_pump_liq_2)+(elec_compr_gas_1+mech_compr_1+pipes_compr_gas_1+pressens_compr_gas_1)*(elec_compr_gas_2+mech_compr_2+pipes_compr_gas_2+pressens_compr_gas_2)+pipes_outflow_liq*pressens_outflow_liq*tank_outflow_liq+mech_reg_gas*pipes_reg_gas*pressens_reg_gas*alls_reg_gas+mech_reg_liq*pipes_reg_liq*pressens_reg_liq*walls_reg_liq+mat_deg_passive*radiator_passive*shape_passive*walls_deg_passive+pipes_outflow_gas*pressens_outflow_gas*tank_outflow_gas*tempsens_outflow_gas*vent_boil_off+air_not*mat_deg_ins_rad*mat_deg_ins_conv*radiator_ins_rad*shape_ins_rad*shape_ins_conv*walls_deg_ins_rad

[20] For more details, see Appendix A.

As early discussed, the same approach has to be followed for the other failure conditions, indeed, here there are the other three main equations, in which the values of the devices failure rates will be substituted.

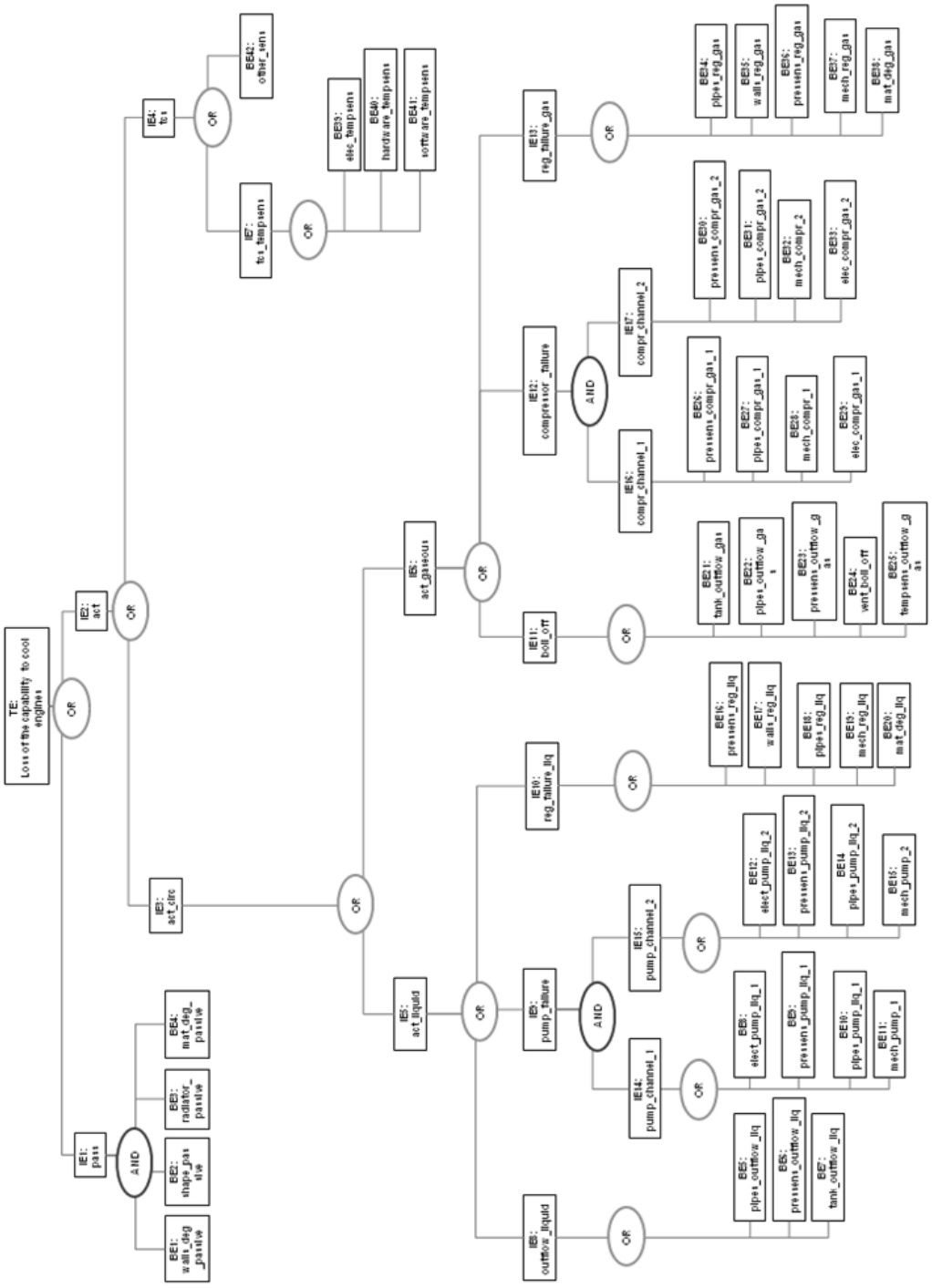


Figure 5.4 FT of the failure condition "Loss of the capability to cool the engines".

STEP	BOOLEAN EXPRESSION
1	T=IE1+IE2
2	T=(BE1*BE2*BE3*BE4)+(IE3+IE4)
3	T=(BE1*BE2*BE3*BE4)+((IE5+IE6)+(IE7+BE42))
4	T=(BE1*BE2*BE3*BE4)+(((IE8+IE9+IE10)+ +(IE11+IE12+IE19))+((BE39+BE40+BE41)+BE42))
5	T=(BE1*BE2*BE3*BE4)+((((BE5+BE6+BE7)+ +(IE12*IE13)+(BE16+BE17+BE18+BE19BE20))+ +((BE21+BE22+BE23+BE24+BE25)+ +(IE16*IE17)+(BE34+BE35+BE36+BE37+BE38)))+ +((BE39+BE40+BE41)+BE42))
6	T=(BE1*BE2*BE3*BE4)+((((BE5+BE6+BE7)+ +((BE8+BE9+BE10+BE11)*(BE12+BE13+BE14+BE15))+(BE16+BE17+BE18+BE19+BE20))+ +((BE21+BE22+BE23+BE24+BE25)+((BE26+BE27+BE28+BE29)*(BE30+BE31+BE32+BE33))+ +(BE34+BE35+BE36+BE37+BE38)))+((BE39+BE40+BE41)+BE42))

Table 5.3 Resolving steps to evaluate the MCS of the failure condition "Loss of the capability to cool the engines".

TE (To cool engines)=

other_sens*(elec_tempsens+hardware_tempsens+software_tempsens)+(elect_pump_liq_1+mech_pump_1+pipes_pump_liq_1+pressens_pump_liq_1)*(elect_pump_liq_2+mech_pump_2+pipes_pump_liq_2+pressens_pump_liq_2)+(elec_compr_gas_1+mech_compr_1+pipes_compr_gas_1+pressens_compr_gas_1)*(elec_compr_gas_2+mech_compr_2+pipes_compr_gas_2+pressens_compr_gas_2)+pipes_outflow_liq*pressens_outflow_liq*tank_outflow_liq+mech_reg_liq*pipes_reg_liq*pressens_reg_liq*walls_reg_liq+mat_deg_passive*radiator_passive*shape_passive*walls_deg_passive+mat_deg_gas*mech_reg_gas*pipes_reg_gas*pressens_reg_gas*walls_reg_gas+pipes_outflow_gas*pressens_outflow_gas*tank_outflow_gas*tempsens_outflow_gas*vent_boil_off

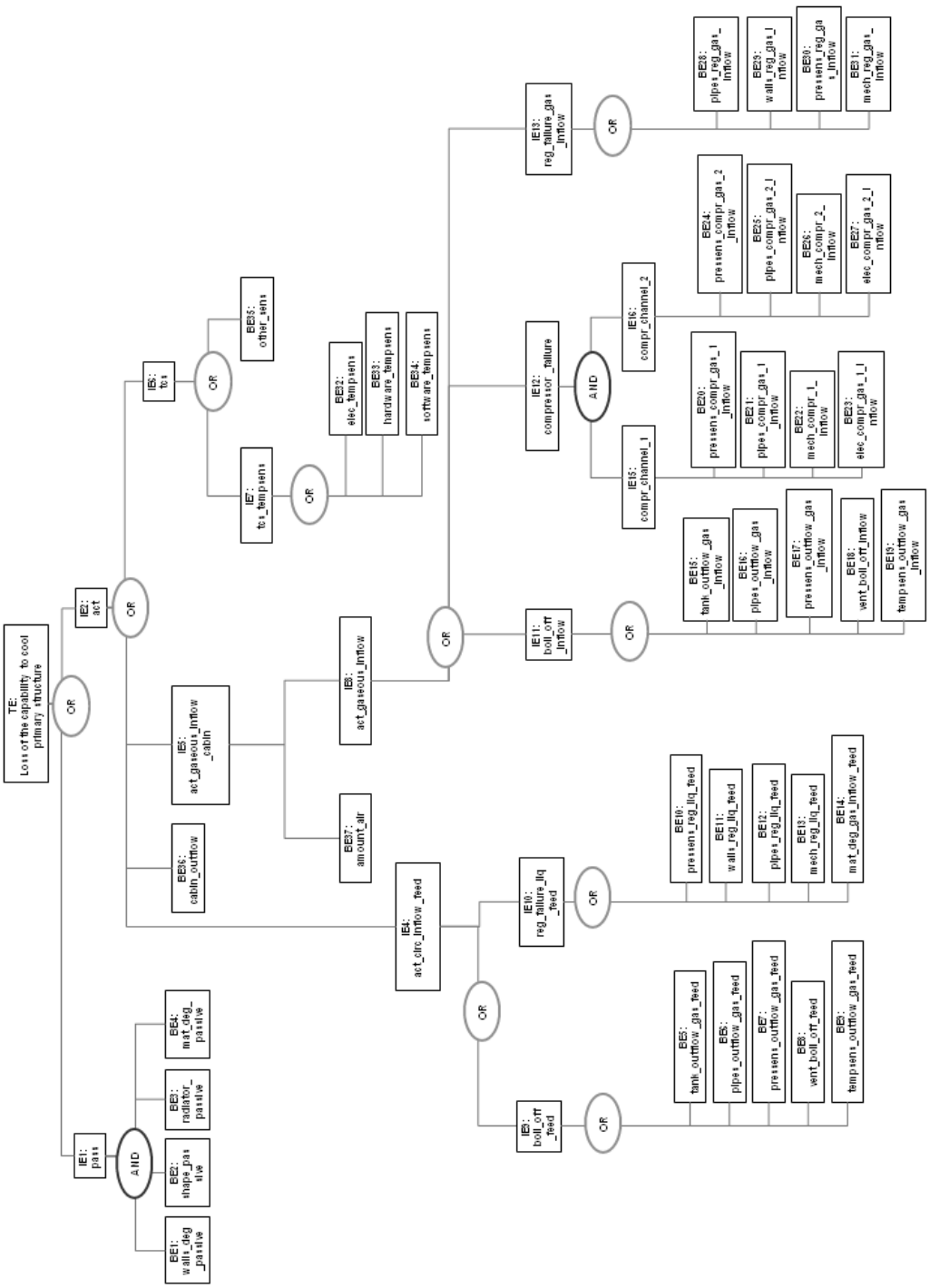


Figure 5.5 FT of the failure condition "Loss of the capability to cool the primary structure".

STEP	BOOLEAN EXPRESSION
1	T=IE1+IE2
2	T=(BE1*BE2*BE3*BE4)+(IE4+IE5+IE6+BE36)
3	T=(BE1*BE2*BE3*BE4)+((IE9+IE10)+(IE8+BE37)+BE36+(IE7+BE35))
4	T=(BE1*BE2*BE3*BE4)+(((BE5+BE6+BE7+BE8+BE9)+(BE10+BE11+BE12+BE13+BE14))+((IE11+IE12+IE13)+BE37)+BE36+(BE32+BE33+BE34)+BE35))
5	T=(BE1*BE2*BE3*BE4)+(((BE5+BE6+BE7+BE8+BE9)+(BE10+BE11+BE12+BE13+BE14))+(((BE15+BE16+BE17+BE18+BE19)+(IE15*IE16))+(BE28+BE29+BE30+BE31))+BE37)+BE36+(BE32+BE33+BE34)+BE35))
6	T=(BE1*BE2*BE3*BE4)+(((BE5+BE6+BE7+BE8+BE9)+(BE10+BE11+BE12+BE13+BE14))+(((BE15+BE16+BE17+BE18+BE19)+((BE20+BE21+BE22+BE23)*(BE24+BE25+BE26+BE27)))+(BE28+BE29+BE30+BE31))+BE37)+BE36+(BE32+BE33+BE34)+BE35))

Table 5.4 Resolving steps to evaluate the MCS of the failure condition "Loss of the capability to cool the primary structure".

TE (To cool primary structure)=

amount_air+cabin_outflow+other_sens*(elec_tempsens+hardware_tempsens+software_tempsens)+(elec_compr_gas_1_inflow+mech_compr_1_inflow+pipes_compr_gas_1_inflow+pressens_compr_gas_1_inflow)*(elec_compr_gas_2_inflow+mech_compr_2_inflow+pipes_compr_gas_2_inflow + pressens_compr_gas_2_inflow)+mat_deg_passive*radiator_passive*shape_passive*walls_deg_passive+mat_deg_gas_inflow*mech_reg_gas_inflow*pipes_reg_gas_inflow*pressens_reg_gas_inflow*walls_reg_gas_inflow+pipes_outflow_gas_inflow*pressens_outflow_gas_inflow*tank_outflow_gas_inflow*tempsens_outflow_gas_inflow*vent_boil_off_inflow

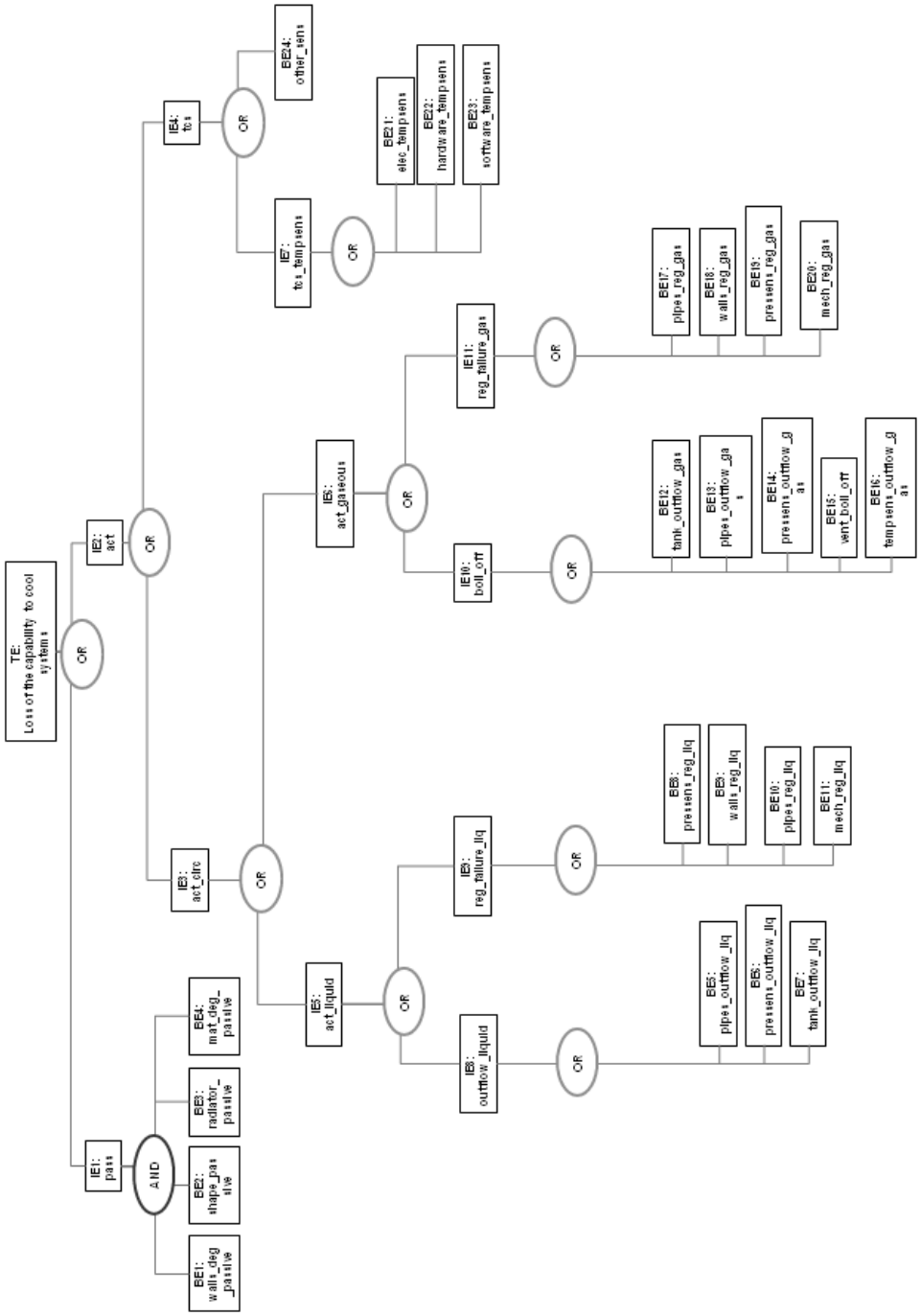


Figure 5.6 FT of the failure condition "Loss of the capability to cool the systems".

STEP	BOOLEAN EXPRESSION
1	T=IE1+IE2
2	T=(BE1*BE2*BE3*BE4)+(IE3+IE4)
3	T=(BE1*BE2*BE3*BE4)+((IE5+IE6)+(IE7+BE24))
4	T=(BE1*BE2*BE3*BE4)+(((IE8+IE9)+ +(IE12+IE11))+((BE21+BE22+BE23)+BE24))
5	T=(BE1*BE2*BE3*BE4)+((((BE5+BE6+BE7)+ +(BE8+BE9+BE10+BE11))+ +((BE12+BE13+BE14+BE15+BE16)+ +((BE17+BE18+BE19+BE20)))+ +((BE21+BE22+BE23)+BE24))

Table 5.5 Resolving steps to evaluate the MCS of the failure condition "Loss of the capability to cool the systems".

TE (To cool systems)=

other_sens*(elec_tempsens+hardware_tempsens+software_tempsens)+pipes_outflow_liq*pressens_outflow_liq*tank_outflow_liq+mech_reg_gas*pipes_reg_gas*pressens_reg_gas*walls_reg_gas+mech_reg_liq*pipes_reg_liq*pressens_reg_liq*walls_reg_liq+mat_deg_passive*radiator_passive*shape_passive*walls_deg_passive+pipes_outflow_gas*pressens_outflow_gas*tank_outflow_gas*tempsens_outflow_gas*vent_boil_off

Considering the Fault Tree related to the devices failures[21], a concrete failure rate must be associated to the specific device failure event at the basic level.

The failure events of electrical, mechanical or electromechanical equipment are available in technical databases, papers and technical datasheets [18], [19], [20], [21], [22], [23], [24], [25], [26], [27], [28], [29] .

A methodical research has been followed to identify the most suitable failure rates for each device and its malfunctions. The choice of the most appropriate failure rate has been firstly addressed, approximately, in the way of an average value.

Some failure rates of crucial equipment have been replaced with a more stringent value, for example, selecting them as advance components database (military sector, naval field, nuclear studies, etc, ...); this could have been accomplished because of the high complexity and innovation of this case of study.

[21] See Attachment G.

After an in-depth research and having allocated the specific failure rate to the single device failure event per each Fault Trees, every Reliability Equation has been solved, applying the logic rules of the Boolean Algebra[22].

Each top failure condition has its own Reliability Equation, therefore there are four expressions useful to evaluate the top level event likelihood and make a comparison with the expected value.

In the following tables have been gathered all the practical of use and adopted data divided according to the failure conditions.

[22] See Appendix A.

To sustain thermal loads		
	Basic Event	**FR (failures/FH)**
Liquid outflow	Pipes leakages	$3*10^{-10}$
	Pressure sensor failure	$7*10^{-6}$
	Tank leakages	$1*10^{-8}$
Pump	Electrical system failure	$3*10^{-6}$
	Pressure sensor failure	$7*10^{-6}$
	Pipes leakages	$3*10^{-10}$
	Mechanical failure	$1*10^{-6}$
Liquid Regenerator	Pressure sensor failure	$7*10^{-6}$
	Pipes leakages	$3*10^{-10}$
	Walls degradation	$3*10^{-11}$
	Heat exchanger failure	$3*10^{-11}$
Boil-off	Pipes leakages	$3*10^{-10}$
	Pressure sensor failure	$7*10^{-6}$
	Tank leakages	$1*10^{-8}$
	Temperature sensor failure	$1,9*10^{-7}$
	Aeration not present	$1,9*10^{-6}$
Compressor	Electrical system failure	$3*10^{-6}$
	Pressure sensor failure	$7*10^{-6}$
	Pipes leakages	$3*10^{-10}$
	Mechanical failure	$1*10^{-6}$
Gaseous Regenerator	Pressure sensor failure	$7*10^{-6}$
	Pipes leakages	$3*10^{-10}$
	Walls degradation	$3*10^{-11}$
	Heat exchanger failure	$3*10^{-11}$
Convection Insulation	Aeration not present	$1,9*10^{-6}$
	Material degradation	$2*10^{-3}$
	Shape degradation	$3*10^{-4}$
Radiation Insulation	Inefficient radiator	$5,6*10^{-7}$
	Walls degradation	$3*10^{-11}$
	Material degradation	$2*10^{-3}$
	Shape degradation	$3*10^{-4}$

Table 5.6 Failure rate allocated to the devices failures related to the condition "Loss of the capability to sustain thermal loads" (part 1).

Passive System	Inefficient radiator	$5,6*10^{-7}$
	Material degradation	$2*10^{-8}$
	Walls degradation	$3*10^{-11}$
	Shape degradation	$3*10^{-4}$
TCS	Electrical system failure	$3*10^{-6}$
	Hardware errors	$7,4*10^{-7}$
	Software errors	$7,1*10^{-7}$
	Sensors errors	$2,5*10^{-6}$

Table 5.7 Failure rate allocated to the devices failures related to the condition "Loss of the capability to sustain thermal loads" (part 2).

To cool engines		
	Basic Event	**FR (failures/FH)**
Liquid outflow	Pipes leakages	$3*10^{-10}$
	Pressure sensor failure	$7*10^{-6}$
	Tank leakages	$1*10^{-8}$
Pump	Electrical system failure	$3*10^{-6}$
	Pressure sensor failure	$7*10^{-6}$
	Pipes leakages	$3*10^{-10}$
	Mechanical failure	$1*10^{-6}$
Liquid Regenerator	Pressure sensor failure	$7*10^{-6}$
	Pipes leakages	$3*10^{-10}$
	Walls degradation	$3*10^{-11}$
	Heat exchanger failure	$3*10^{-11}$
	Material degradation	$2*10^{-8}$
Boil-off	Pipes leakages	$3*10^{-10}$
	Pressure sensor failure	$7*10^{-6}$
	Tank leakages	$1*10^{-8}$
	Temperature sensor failure	$1,9*10^{-7}$
	Aeration not present	$1,9*10^{-6}$
Compressor	Electrical system failure	$3*10^{-6}$
	Pressure sensor failure	$7*10^{-6}$
	Pipes leakages	$3*10^{-10}$
	Mechanical failure	$1*10^{-6}$
Gaseous Regenerator	Pressure sensor failure	$7*10^{-6}$
	Pipes leakages	$3*10^{-10}$
	Walls degradation	$3*10^{-11}$
	Heat exchanger failure	$3*10^{-11}$
	Material degradation	$2*10^{-8}$
Passive System	Inefficient radiator	$5,6*10^{-7}$
	Material degradation	$2*10^{-8}$
	Walls degradation	$3*10^{-11}$
	Shape degradation	$3*10^{-4}$
TCS	Electrical system failure	$3*10^{-6}$
	Hardware errors	$7,4*10^{-7}$
	Software errors	$7,1*10^{-7}$
	Sensors errors	$2,5*10^{-6}$

Table 5.8 Failure rate allocated to the devices failures related to the condition "Loss of the capability to cool engines".

To cool primary structure		
	Basic Event	**FR (failures/FH)**
Boil-off (convection system)	Pipes leakages	$3*10^{-10}$
	Pressure sensor failure	$7*10^{-6}$
	Tank leakages	$1*10^{-8}$
Gaseous Regenerator	Pressure sensor failure	$7*10^{-6}$
	Pipes leakages	$3*10^{-10}$
	Walls degradation	$3*10^{-11}$
	Heat exchanger failure	$3*10^{-11}$
	Material degradation	$2*10^{-8}$
Outflow valve	Insufficient cabin air outflow	$1*10^{-10}$
Inflow valve	Insufficient amount of air in cabin	$1*10^{-10}$
Boil-off	Pipes leakages	$3*10^{-10}$
	Pressure sensor failure	$7*10^{-6}$
	Tank leakages	$1*10^{-8}$
	Temperature sensor failure	$1,9*10^{-7}$
	Aeration not present	$1,9*10^{-6}$
Compressor	Electrical system failure	$3*10^{-6}$
	Pressure sensor failure	$7*10^{-6}$
	Pipes leakages	$3*10^{-10}$
	Mechanical failure	$1*10^{-6}$
Gaseous Regenerator	Pressure sensor failure	$7*10^{-6}$
	Pipes leakages	$3*10^{-10}$
	Walls degradation	$3*10^{-11}$
	Heat exchanger failure	$3*10^{-11}$
	Material degradation	$2*10^{-8}$
Passive System	Inefficient radiator	$5,6*10^{-7}$
	Material degradation	$2*10^{-8}$
	Walls degradation	$3*10^{-11}$
	Shape degradation	$3*10^{-4}$
TCS	Electrical system failure	$3*10^{-6}$
	Hardware errors	$7,4*10^{-7}$
	Software errors	$7,1*10^{-7}$
	Sensors errors	$2,5*10^{-6}$

Table 5.9 Failure rate allocated to the devices failures related to the condition "Loss of the capability to cool primary structure".

To cool systems		
	Basic Event	**FR (failures/FH)**
Liquid outflow	Pipes leakages	$3*10^{-10}$
	Pressure sensor failure	$7*10^{-6}$
	Tank leakages	$1*10^{-8}$
Liquid Regenerator	Pressure sensor failure	$7*10^{-6}$
	Pipes leakages	$3*10^{-10}$
	Walls degradation	$3*10^{-11}$
	Heat exchanger failure	$3*10^{-11}$
	Material degradation	$2*10^{-8}$
Boil-off	Pipes leakages	$3*10^{-10}$
	Pressure sensor failure	$7*10^{-6}$
	Tank leakages	$1*10^{-8}$
	Temperature sensor failure	$1,9*10^{-7}$
	Aeration not present	$1,9*10^{-6}$
Gaseous Regenerator	Pressure sensor failure	$7*10^{-6}$
	Pipes leakages	$3*10^{-10}$
	Walls degradation	$3*10^{-11}$
	Heat exchanger failure	$3*10^{-11}$
	Material degradation	$2*10^{-3}$
Passive System	Inefficient radiator	$5,6*10^{-7}$
	Material degradation	$2*10^{-8}$
	Walls degradation	$3*10^{-11}$
	Shape degradation	$3*10^{-4}$
TCS	Electrical system failure	$3*10^{-6}$
	Hardware errors	$7,4*10^{-7}$
	Software errors	$7,1*10^{-7}$
	Sensors errors	$2,5*10^{-6}$

Table 5.10 Failure rate allocated to the devices failures related to the condition "Loss of the capability to cool systems".

The previous data have been used to solve each Reliability Equation and evaluate the rate of the probability of each failure event. Looking closer at the four conditions and substituting the numerical values to the appropriate term, the outcomes of the Reliability Equations are reported in Table 5.11.

Event	FR (failure/FH)
Loss of the capability to sustain thermal loads	$2{,}5*10^{-10}$
Loss of the capability to cool engines	$2{,}5*10^{-10}$
Loss of the capability to cool systems	$1{,}1*10^{-11}$
Loss of the capability to cool primary structure	$3{,}3*10^{-10}$

Table 5.11 Outcomes of the Reliability Equation.

It is intended to underline that, the previous failure rates and final outcomes have been obtained after a third analysis, this means, the first and the second iteration were not successful; therefore something has to be modified in the reliability configuration of the system.

After having analyzed the first results, it was comprehensible that, the obstacle was related to the active components because they are characterized by a high failure rate and they have nonetheless a significant importance in the operation of the system: if pump or compressor indeed fail, this will probably compromise the operation of the whole system.

Before the first iteration, a redundancy of the crucial components has been added and, in this specific case, the active elements are the most dangerous (pump and compressor): installing two independent channels for each element, the design has been satisfied.

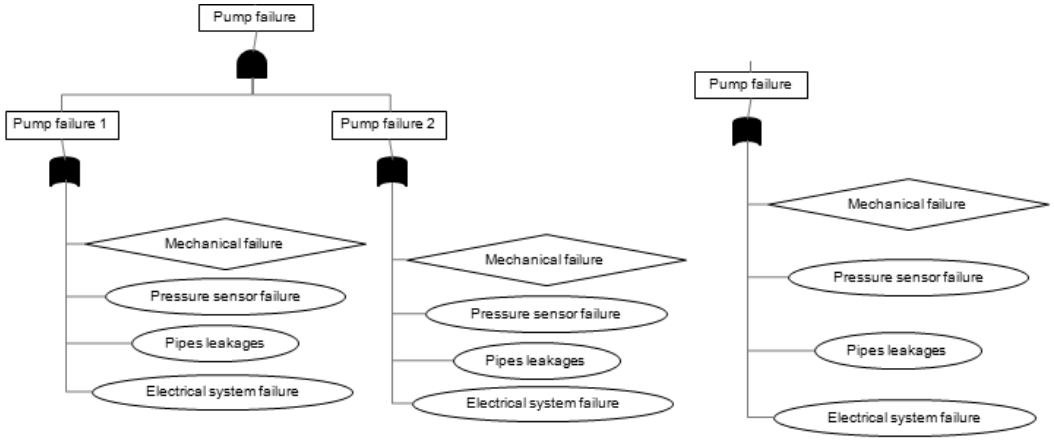


Figure 5.7 Detail of the pump redundancy (left) and single channel (right).

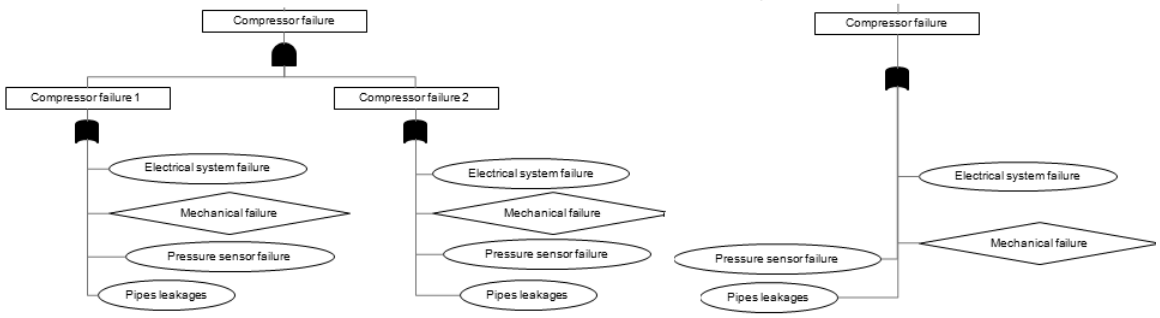


Figure 5.8 Detail of the compressor redundancy (left) and single channel (right).

Thanks to this expedient, both the channels have to fail to cause the upper pump or compressor failure event: the system on the left side of Figure 5.7 and Figure 5.8, clearly, has double weight but, the reliability of the system is considerably increased. In fact, as it is shown in Figure 5.9 and Figure 5.10, the failure rate of the pumping/compression system would have been approximately of $1.1*10^{-5}$ failure/FH without the redundancy.

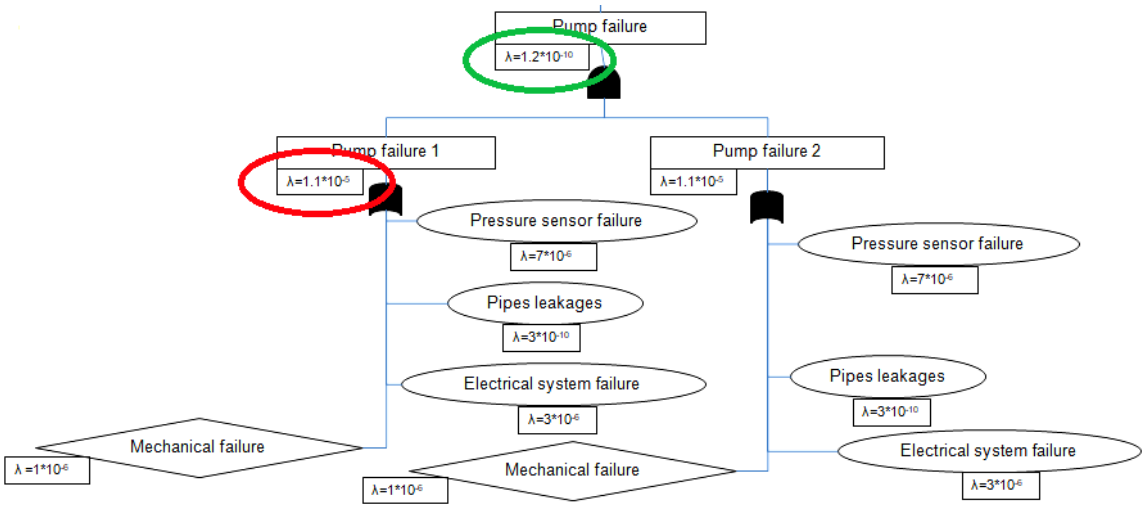


Figure 5.9 In red circle the value of the failure rate of a single channel of pumping system, in green circle the value of the failure rate with double channel.

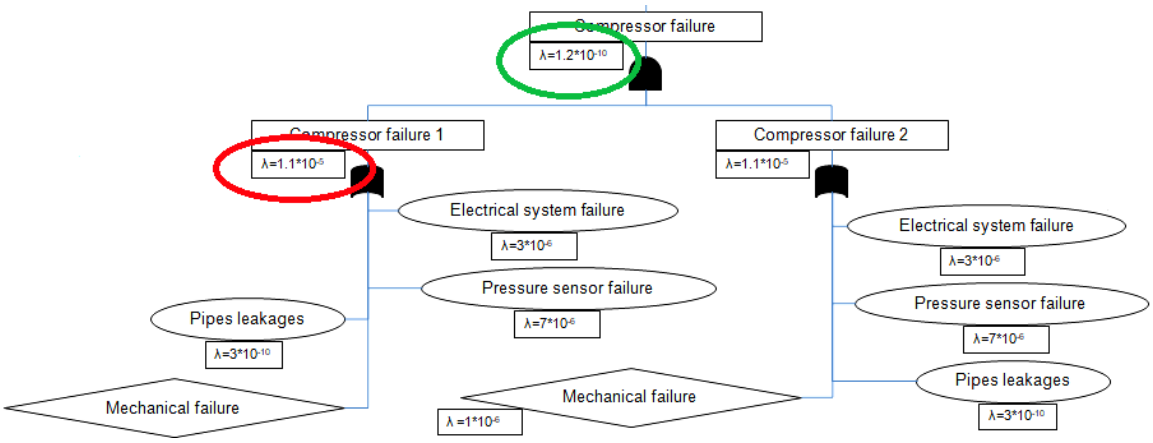


Figure 5.10 In red circle the value of the failure rate of a single channel of compression system, in green circle the value of the failure rate with double channel.

Eventually, in the second one, the research has been focused on the critical components previously highlighted. In this sense, the selection of the failure rates has been stressed in a stricter way because it was evident that some data jeopardize the results. In the evaluation of the critical components, the lowest available failure rates have been linked to the specific equipment, considering that, the vehicle will be in operation in twenty years (for this reason the hypothesis is justified by the foreseen innovative technologies).

5.2 Outcomes

Looking at Attachment D and F, it is possible to link the two kinds of FTA:

- Attachment D contains the failure conditions with the allocation of the failure rates following a top-down approach and it consists of the safety requirements that have to be satisfied;
- Attachment F contains the failure rates allocated with the bottom-up approach starting from the failure rates of the basic components, which have to be managed to fulfil the previous specific requirements.

It is interesting to associate the two diagrams of the corresponding top level functionalities because the FT of the devices have been deduced from the FT related to the respective functions. A detail coming from the failure condition "*Loss of the insulation capability*" is highlighted to display the concept: actually, at each level, the failure rates of the diagram in the right side must be equal or less than the ones in the left side, as Figure 5.11 shows with different colours for each single specification.

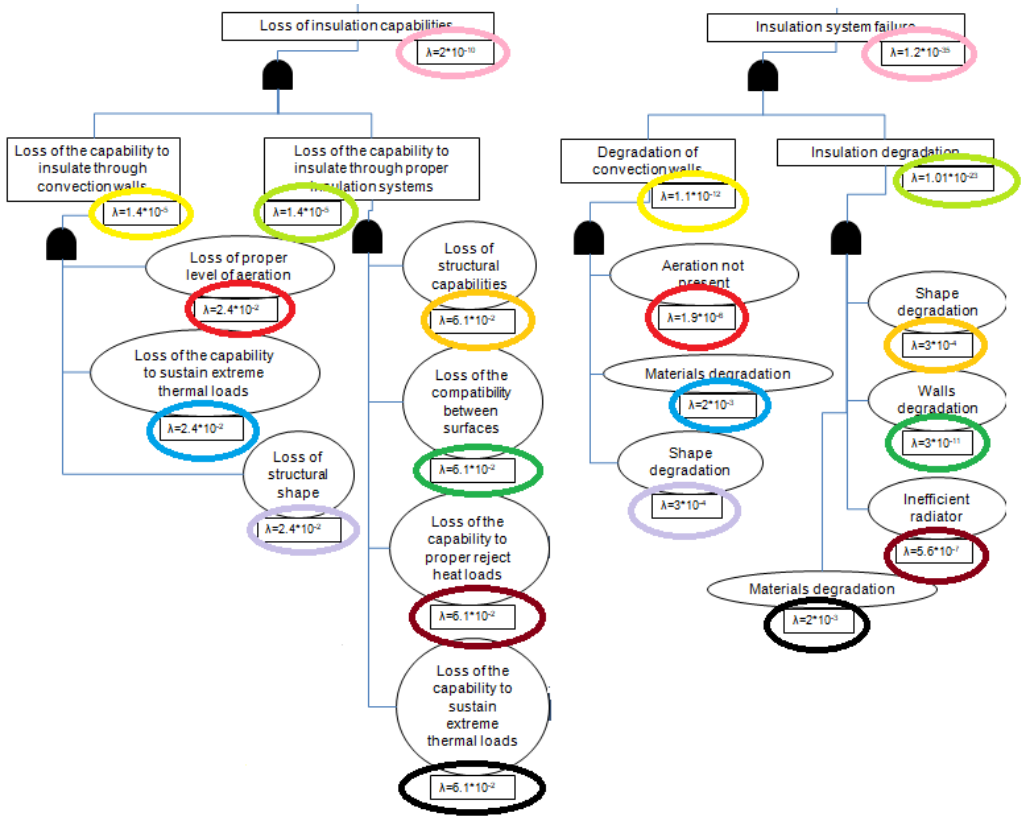


Figure 5.11 Detail of the failure condition "Loss of insulation capability".

Following backwards the "path" up to each main failure event, the significant outcome, that has been obtained, is a successful design, because the likelihood to happen of the top failure conditions is less than the allocated constraint, the Safety Requirements, as Table 5.12 highlights. As a matter of fact, the strict Safety Requirements, due to the innovative kind of mission foreseen for the MR2 vehicle, have been satisfied.

Event	FR (failure/FH)	Requirement (failure/FH)
Loss of the capability to sustain thermal loads	$2,5*10^{-10}$	$1*10^{-9}$
Loss of the capability to cool engines	$2,5*10^{-10}$	$1*10^{-9}$
Loss of the capability to cool systems	$1,1*10^{-11}$	$1*10^{-9}$
Loss of the capability to cool primary structure	$3,3*10^{-10}$	$1*10^{-9}$

Table 5.12 Comparison of outcomes and requirements.

This could have been carried out and fulfilled thanks to the different iterations that have been accomplished, because each of them allows to identify the "weak points" of the proposed architecture.

Event	FR (failure/FH)	Requirement (failure/FH)
Loss of the capability to sustain thermal loads	$2,5*10^{-5}$	$1*10^{-9}$
Loss of the capability to cool engines	$2,2*10^{-5}$	$1*10^{-9}$
Loss of the capability to cool systems	$1,1*10^{-11}$	$1*10^{-9}$
Loss of the capability to cool primary structure	$1,1*10^{-5}$	$1*10^{-9}$

Table 5.13 First results.

The first criticality has been observed indeed when the results of the failure rates were higher than the requirements on account of the lack of redundancies in the system (see Table 5.13). With the addition of the suitable redundancies, the requisites have been almost fulfilled as Table 5.14 shows.

Event	FR (failure/FH)	Requirement (failure/FH)
Loss of the capability to sustain thermal loads	$2,5*10^{-9}$	$1*10^{-9}$
Loss of the capability to cool engines	$2,5*10^{-9}$	$1*10^{-9}$
Loss of the capability to cool systems	$1,1*10^{-11}$	$1*10^{-9}$
Loss of the capability to cool primary structure	$2,9*10^{-9}$	$1*10^{-9}$

Table 5.14 Second results.

The other aspect has been pointed out in the necessity of selecting, for critical mechanical components (pump and compressor), advanced equipment (from the military field, naval sector, nuclear studies, etc, ...) characterized by restrictive failure rates. In this way, the results could have been improved and they are yielded all along in Table 5.12.

The outlined results cannot be compared with statistical data because similar aircrafts do not exist at present.

Pneumatic System, Environmental Control System and Anti-Ice System of a state of art civil transportation aircraft are overall unsophisticated systems, characterized by a failure rate around 1 failures/100FH [17]. This circumstance is understandable because those sorts of systems are marked out by "untroubled" components, meaning the equipment has a higher failure rate (i.e. it is less reliable) but those values are accepted nevertheless. This point is considered coherent in account of the "simpler" operations, these systems have to accomplish.

On the other hand, the TEMS of MR2 has a failure rate of approximately $1*10^{-9}/1*10^{-10}$ failures/FH, in other words, it is reasonable to have obtained these restrictive values because this system has to face more criticalities in case of failures: it is branded indeed by highly-developed operating conditions, therefore if TEMS fails, the consequences could be completely catastrophic. Moreover, the obtained results seem to be realistic as well, in the sense that, the MR2 vehicle is envisaged as a significantly high level of complexity civil transportation vehicle, which will be in operation in 20-30 years, therefore it could be supposed, the acquired low value is, once again, justified. Essentially, thanks to current studies, it is suggested that, to foresee and estimate a failure rate of an innovative product, as it could be the TEMS of the MR2 vehicle, the "technological age" is one of the most influential terms which could diminish the failure rate [17]. New technologies tend to be more performable, in the proper sense that, reliability will be increased and, consequently, the failure rate will be reduced. This leads, necessarily, into a considerable increase in costs and also, considering an extra-perspective, maintenance operations, because a more reliable systems means significant investments in performable sub-systems and in a proper preservation schedule. This object is not further discussed herein but it could be the starting point of additional works.

Conclusion

The purpose of this paper was to present a Safety and Reliability Assessment applied to a high level of complexity system, as a hypersonic transportation vehicle could be, following the main steps of a MBSE approach, and to carry it out during the preliminary design phases of the project. This analysis has been focused on the examination of the MR2 vehicle and, specifically, has been performed on its Thermal Management System because, at this conceptual level of study, is the only system characterized by a coherent architecture and concrete components. Actually, the key advantage of this cited method consists in the capability to overcome the lack of statistical data at system level and exploits them only at equipment level, where documents are available.

The whole methodology has been interfaced by helpful typical systems engineering tools (such as Functional Hazard Analysis, Fault Tree Analysis, Reliability Block Diagram, etc, …) in order to accomplish a first qualitative and deductive estimation of the functionalities, which the aircraft has to guarantee. From the outlined functions it has been possible to derive, firstly, the potential basic failure conditions, the system has to face, plus their associated Safety Requirements, and, subsequently, to identify the components which are related to those hazardous events. This top-down study began with the market analysis within which the hypersonic vehicle will be collocated and an accurate definition of its mission features so as to enable the development a list of Functional Requirements. Considering the Functional Requirements related to the Thermal Management System and with the assistance of the FHA, four main hazardous conditions have been established, regarding the incapability of the TEMS to manage extreme thermal fluxes from the outer environment and from the internal systems (in particular, the propulsion one). All the four conditions have been classified as the most critical level of risk events. At this point, a Fault Tree for each failure situations has been sketched out in order to more deeply characterize the potential dangerous causes. The diagram gathers the potential failure circumstances and their linked Safety Requirements up to the basic ones. After having allocated the functionalities to the proper components, the process has been followed backwards.

Thanks to resolving logical relations, a quantitative evaluation of the failure rates of the specific equipment has led into the numerical likelihood of the top failure event. This procedure has been repeated until a successful design has been achieved.

Actually, the Safety and Reliability Assessment is an iterative and recursive approach, therefore the obtained results have been continuously updated in order to acquire even more precise outcomes: the steps have to be performed as long as the allocated requirements have been fulfilled. Clearly, at each recurring step, a more detailed design has been accessible and the whole study has guided to more accurate conclusions.

In this particular case of study, the iterative approach has been essential and helpful to identify the "weak points" of the physical architecture of the TEMS. Thanks to the iteration indeed, critical components have been detected and the study has been focused on them. The first relevant solution, that has been proposed to face the first unsuccessful result obtained, is to install a redundancy of those components in order to increase consistently the Reliability. Specifically, after having narrowed the potentially hazardous equipment down, it has been possible to identify that, the most dangerous components are the pump and the compressor, therefore a redundancy for both of them must be allocated. Moreover, to completely fulfil totally the requirements, a stricter selection of the most performing and suitable components has been carried out. Hence, the other final significant key point, outlined during the assessment, has been the investigation of the proper equipment into specific sector databases, such as military, naval, nuclear fields so as to adopt the most advanced devices. Following these steps of the analysis, a specific reliability architecture has been proposed in order to satisfy the Safety Requirements as well as they were allocated at the beginning of the study.

The whole analysis has been demanding because of the high level of innovation and complexity of the MR2 and its preliminary design phase. In the course of the study, several reasonable approximations have been included to achieve and convey a potential idea of the reliability of the TEMS (and, in a certain sense, an estimation of the reliability of the entire vehicle) as well as to include a suggestion about how to solve, from a reliability point of view, its criticalities.

Clearly, in the near future the project will gradually improve its systems and sub-systems, therefore, if a similar study is accomplished during a more advanced stage of the design of MR2, the results will be more accurate.

Attachments

Attachment A: Use Case Diagram

Attachment B: Functional Hazard Assessment

Attachment C: Fault Tree Analysis

Attachment D: Functional Tree

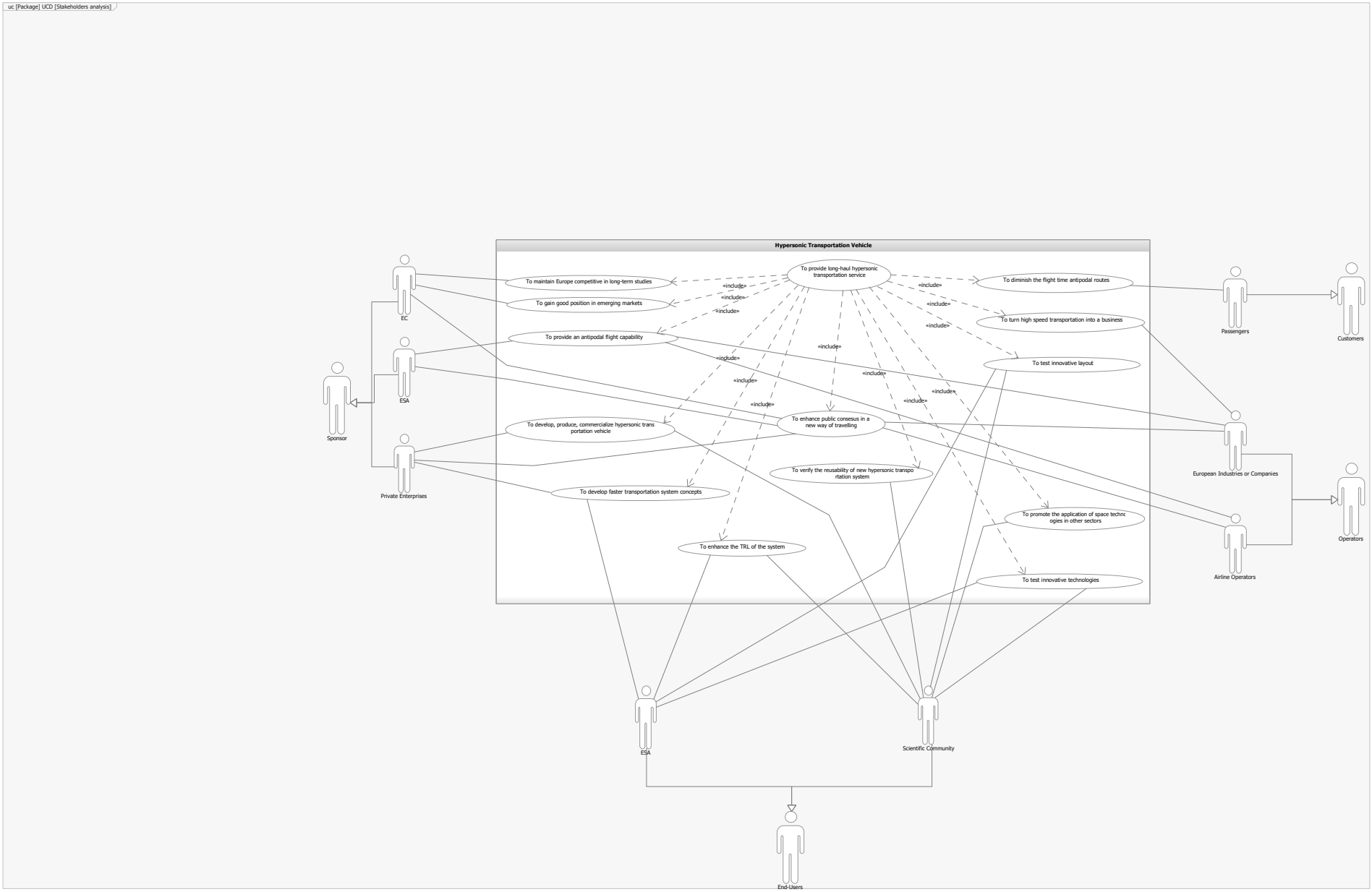
Attachment E: Functional Tree (detail of Failure Conditions)

Attachment F: Products Tree

Attachment G: Fault Tree Analysis (Devices)

In the following pages, useful documents have been gathered in this order:

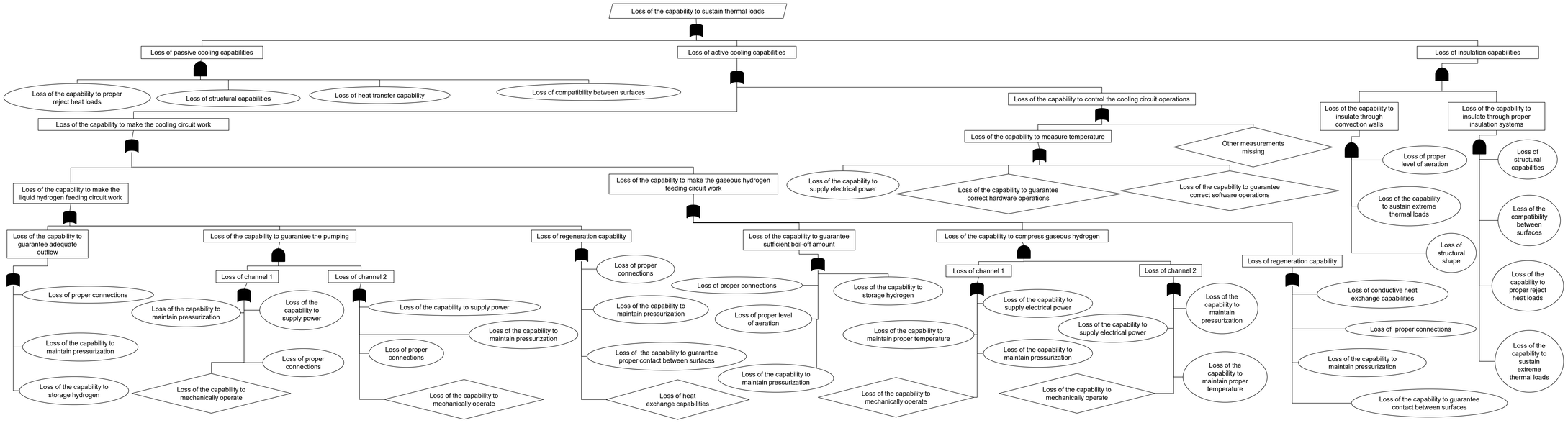
- Attachment A contains the Use Case Diagram (1 page);
- Attachment B contains the Functional Hazard Assessment (1 page);
- Attachment C contains the four "simple" FTA and the four with the top-down allocation of the Safety Requirements (4 pages);
- Attachment D contains the complete Functional Tree (1 page);
- Attachment E contains the Functional Tree of the four Failure Conditions (4 pages);
- Attachment F contains the complete Products Tree (1 page);
- Attachment G contains the four FTA concerning the devices and the four FTA with the bottom-up allocation of the failure rates (4 pages).


uc [Package] UCD [Stakeholders analysis]
Hypersonic Transportation Vehicle
To provide long-haul hypersonic transportation service
To maintain Europe competitive in long-term studies
To gain good position in emerging markets
To provide an antipodal flight capability
To develop, produce, commercialize hypersonic transportation vehicle
To enhance public consesus in a new way of travelling
To verify the reusability of new hypersonic transportation system
To develop faster transportation system concepts
To enhance the TRL of the system
To diminish the flight time antipodal routes
To turn high speed transportation into a business
To test innovative layout
To promote the application of space technologies in other sectors
To test innovative technologies
«include»
EC
ESA
Sponsor
Private Enterprises
ESA
Scientific Community
End-Users
Passengers
Customers
European Industries or Companies
Operators
Airline Operators

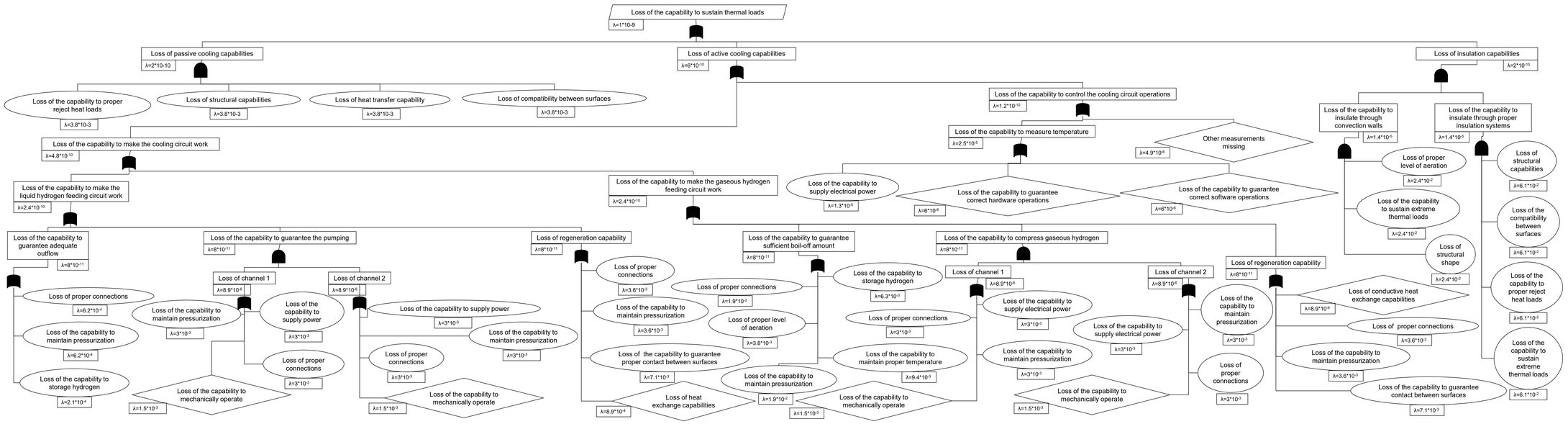
FHA

FUNCTION	FAILURE CONDITION	PHASE	CLASSIFICATION	FAILURE EFFECT
To maintain thermal equilibrium	loss of the capability to sustain thermal loads	climb, cruise	A	the vehicle is exposed to unbalanced thermal loads and overheating
	loss of the capability to cool engines	climb, cruise	A	loss of propulsion system
	loss of the capability to cool the vehicle primary structure	climb, cruise	A	the airframe cannot bear extreme thermal loads
	loss of the capability to cool systems	climb, cruise	A	severe damages to on-board system
To board propellant	loss of the capability to storage the required propellant	taxi	E	the vehicle cannot fulfil the starting check
	loss of the capability to transfer fuel at a proper rate	take off	C	the vehicle cannot perform the running
	loss of the capability to transfer fuel at a proper rate	climb/cruise/descent	A	the engines cannot be fed and lose thrust
	loss of the capability to transfer fuel at a proper rate	landing	C	the vehicle cannot approach and land properly
	unable to maintain the correct relative pressure	all	B	the vehicle cannot provide the sufficient motive flow
	loss of the capability to supply a continuous fuel at proper temperature	all	B	the vehicle cannot work at the desired conditions
	loss of the capability to refuel the tanks	taxi	E	the vehicle cannot operate
	loss of the capability to refuel the tanks	cruise	B	the vehicle cannot operate
	loss of the capability to ensure sufficient fuel in the main tanks to perform an emergency landing	all	B	the vehicle cannot face an emergency condition
To perform HTO	loss of the capability to perform take-off	taxi	E	the vehicle cannot get in position on the runway and cannot start the running
	loss of the capability to generate thrust on ground	take off	C	the vehicle cannot perform the running properly
	loss of the capability to perform taking off acceleration	take off	B	the crew cannot make the aircraft reach the speed V1 necessary for lifting off
To support HTO	unable to reach the proper position on the runway	taxi	D	the crew cannot control the aircraft on ground
	unable to perform straight taking off running on the ground	take off	C	the vehicle cannot maintain runway centerline
	unable to support the taking off manoeuvre	take off	B	the crew cannot perform the rotation manoeuvre
	unable to retract the landing gear	take off	C	Aerodynamic configuration of the vehicle is compromised
To perform HL	loss of the capability to perform the approach for hl	descent	C	the vehicle cannot maintain the descent rate
	loss of the capability to decelerate	landing	B	the vehicle cannot decelerate safely on final
To support HL	unable to perform braking	landing	C	speed cannot be controlled during taxi
	unable to perform steering	taxi	C	loss of aircraft control during taxi
To perform the acceleration phases	loss of the capability to perform the acceleration phases	climb	D	the vehicle cannot meet the acceleration profile
To support the acceleration phases	unable to guarantee the desired fuel mass flow rate	climb	C	severe to moderate degradation of powerplant performance
To perform the initial subsonic cruise	loss of the capability to perform the initial subsonic cruise	cruise	D	the vehicle cannot reach the expected speed and altitude
To support the initial subsonic cruise	loss of all the flight primary surfaces	cruise	B	the vehicle cannot perform any manoeuvres
	loss of any flight primary surfaces	cruise	C	the vehicle encounters a partial degradation of the control
To perform a cruise at 35km	loss of the capability to perform a cruise at 35km	cruise	D	the vehicle cannot get to the expected altitude
To perform a cruise at Mach 8	loss of the capability to perform a cruise at Mach 8	cruise	D	the vehicle cannot reach the expected hypersonic speed
To sustain structural loads	loss of the capability to bear weight and aerodynamic forces	take off/climb/cruise/landing	A	the vehicle encounters a total loss of the primary structure
To safely accommodate passengers and attendants	loss of the capability to accommodate passengers and attendants	taxi	D	passengers and attendants cannot have their own seat and safety equipment
	loss of the capability to accommodate passengers and attendants	take off/climb/cruise/ descent/landing	A	passengers and attendants cannot have their own seat and safety equipment in emergency operational conditions
	loss of the capability to accommodate passengers and attendants	take off/climb/cruise/ descent/landing	C	passengers and attendants cannot have their own seat and safety equipment in nominal operational conditions
To safely accommodate the crew	loss of the capability to accommodate the crew	taxi	E	the crew cannot have its own seat and drive the vehicle
	loss of the capability to accommodate the crew	take off/climb/cruise/landing	A	the crew cannot have its own seat and drive the vehicle in emergency operational conditions
	loss of the capability to accommodate the crew	take off/climb/cruise/landing	B	the crew cannot have its own seat and drive the vehicle in nominal operational conditions
To guarantee communication				
To transmit/receive signals	loss of the capability to transmit/receive signals to/from ground station	taxi	E	the vehicle cannot get in position on the runway
	loss of the capability to communicate the authorization	take off	D	the vehicle cannot start the take off
	loss of the capability to transmit/receive signals to/from ground station	climb, cruise, descent	B	the vehicle cannot exchange any kind of information with the ground
	loss of the capability to communicate the authorization	landing	B	the vehicle cannot land with the assistance of the ground station
	loss of the capability to reach the correct gate	taxi	E	the vehicle cannot take place and passengers cannot get off
To store data	unable to memorize data	all	E	the vehicle cannot collect information
To transmit emergency signal to be localized	loss of the capability to transmit emergency signal	all	B	the vehicle cannot be localized in case of emergency
To inform in case of system failure	unable to warn in case of system failure	all	A	the crew cannot be notified about system failure
To guarantee inner communication	loss of the capability to guarantee inner communications during flight	all	E	the crew cannot communicate with attendants and passengers
To guarantee navigation and guidance				
To acquire navigation data	loss of the capability to acquire navigation data	take off/landing	B	the system cannot calculate distances
	loss of the capability to acquire navigation data	climb/cruise/descent	C	the system cannot calculate distances
To acquire environmental data	loss of the capability to acquire environmental data	climb/cruise/descent	C	the crew cannot know data from the airspace around
To acquire flight data	loss of the capability to acquire flight data	all	C	the system cannot calculate speed and acceleration
To store and process data	loss of the capability to determine the state vector	all	C	the crew cannot know location and speed
	unable to have a database and to upgrade new data	all	D	the crew cannot manage the best route
To manage navigation data	loss of the capability to guarantee automatic guidance	cruise	C	the crew cannot activate autopilot
	loss of the capability to guarantee manual guidance	all	C	the crew cannot control the stick properly and perform manouevres
	loss of the capability to activate a radionavigation	landing	C	the vehicle cannot be supported during landing
To inform the crew	loss of the capability to guarantee guidance and navigation	all	C	the vehicle cannot reach a desired state (specified by a target)
To perform surveillance and identification				
To carry out identification by ground station	loss of the capability to be identified on the runway	taxi	C	the vehicle cannot be tracked
	loss of the capability to be interrogated by radars	take off	D	the ground station cannot authorize the take off
	loss of the capability to be interrogated by radars	climb, cruise, descent	C	the vehicle cannot be recognised by ground station
	loss of the capability to be interrogated by radars	landing	C	the ground station cannot authorize the landing
To carry out identification by other airplanes	loss of the capability to be interrogated by radars	take off	D	the vehicle cannot be recognised by other aircrafts
	loss of the capability to be interrogated by radars	climb, cruise, descent	C	the vehicle cannot be recognised by other aircrafts
	loss of the capability to be interrogated by radars	landing	D	the vehicle cannot be recognised by other aircrafts
To carry out surveillance in the airspace around	loss of the capability to carry out surveillance	climb, cruise, descent	C	the vehicle cannot supervise the flight zone around
To control the system in atmospheric environment	loss of the capability to control the system in atmospheric environment	take off/landing	A	the vehicle cannot perform manoeuvres
	loss of the capability to control the system in atmospheric environment	climb/cruise/descent	A	the vehicle cannot perform manoeuvres
	loss of the capability to guarantee control in case of emergency	take off/climb/cruise/ descent/landing	A	the vehicle cannot perform manoeuvres
To perform unpowered descent	loss of the capability to perform unpowered descent	descent	B	the vehicle cannot switch off the engines
To support unpowered descent	unable to support unpowered descent	descent	B	the vehicle cannot extend the landing gear
To guarantee human habitability	loss of the capability to guarantee human need of temperature pression and oxygen concentration	all	A	passengers, attendants and crew cannot bear unproper environmental conditions
To supply electrical power				
To supply electrical power to vital users	loss of the capability to supply electrical power to vital users	all	A	the vehicle cannot guarantee power distribution
	loss of the capability to supply electrical power to vital users	all	A	the vehicle cannot manage electric loads
	loss of the capability to supply electrical power to vital users	all	A	the vehicle cannot guarantee vital users
	loss of the capability to activate emergency devices	all	A	the vehicle cannot face emergency situations
To supply electrical power to essential users	loss of the capability to supply electrical power to actuators	all	A	the vehicle cannot perform manouevres
	loss of the capability to supply electrical power to on board computers	all	B	the vehicle cannot be controlled and properly drive
	loss of the capability to supply electrical power to essential users	take off/landing	B	the vehicle cannot retract/extract the landing gear
To supply electrical power to non-essential users	loss of the capability to supply electrical power to non-essential users	all	E	the vehicle cannot offer passenger accomodations

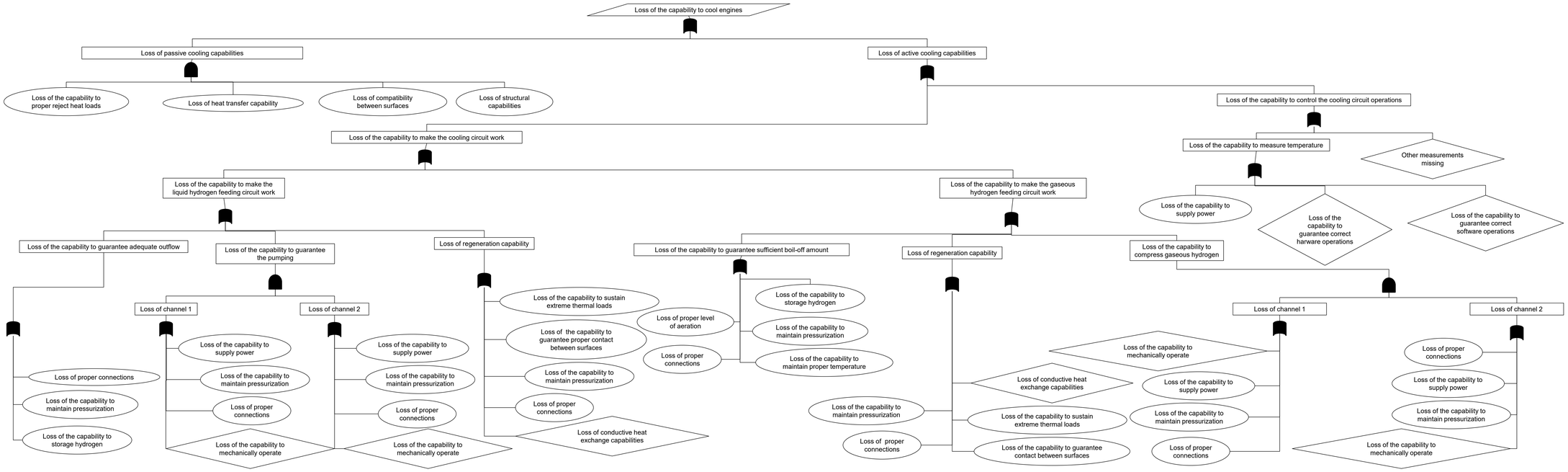
FTA: Loss of the capability to sustain thermal loads



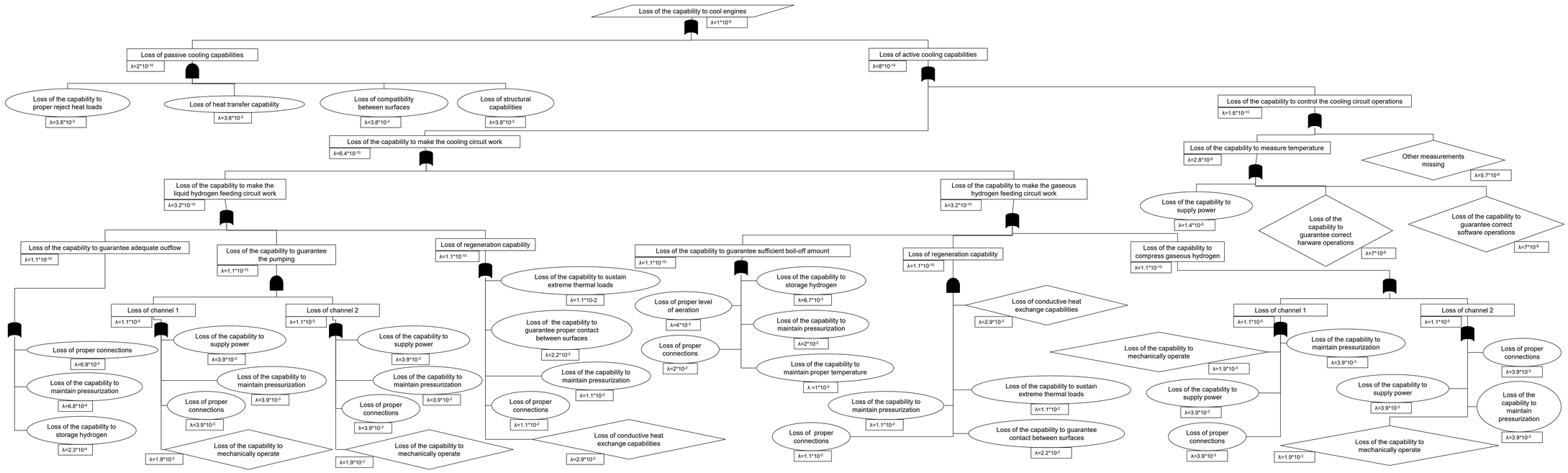
FTA: Loss of the capability to sustain thermal loads (Top-down approach)



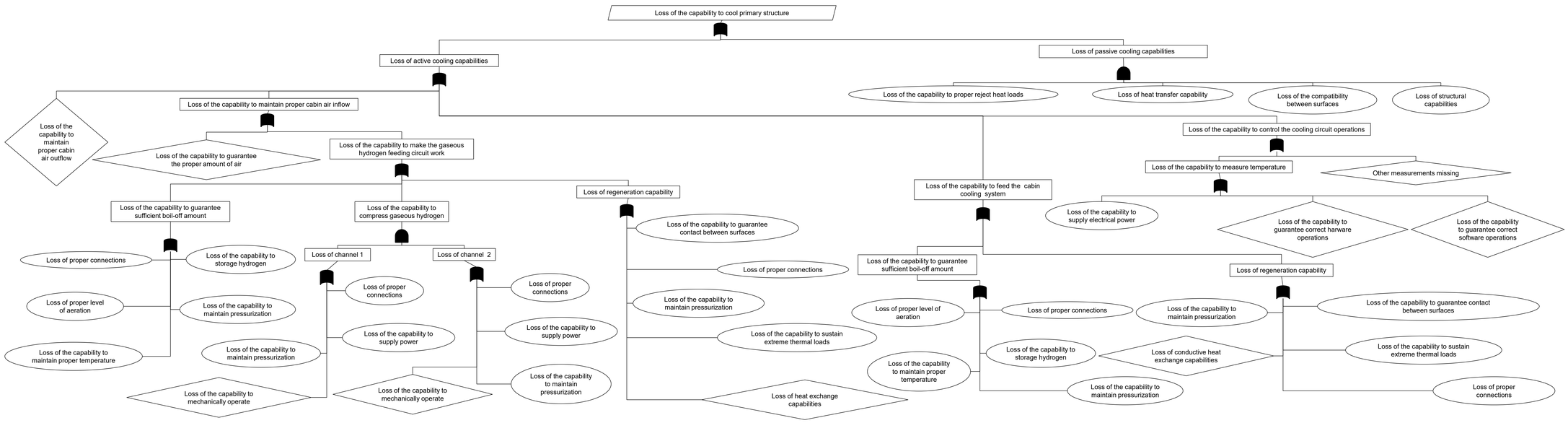
FTA: Loss of the capability to cool the engines



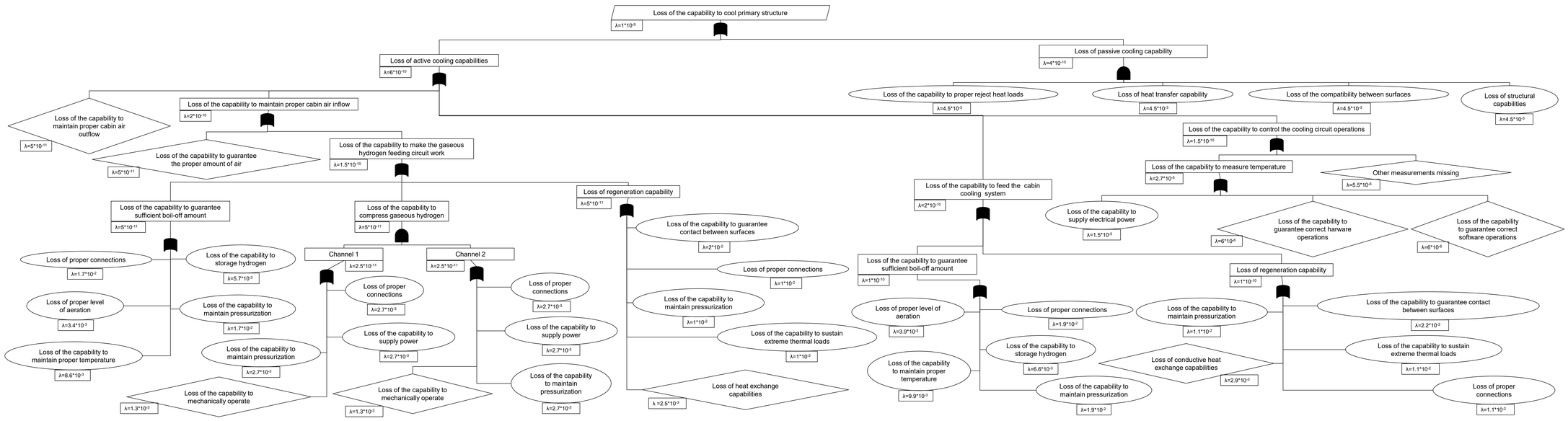
FTA: Loss of the capability to cool the engines (Top-down approach)



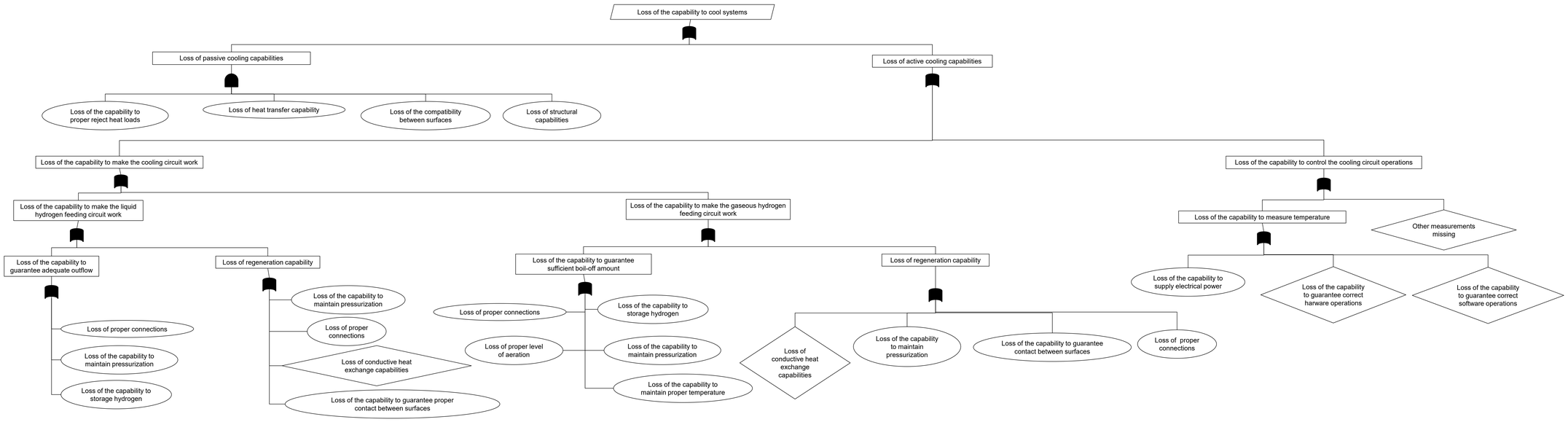
FTA: Loss of the capability to cool the primary structure



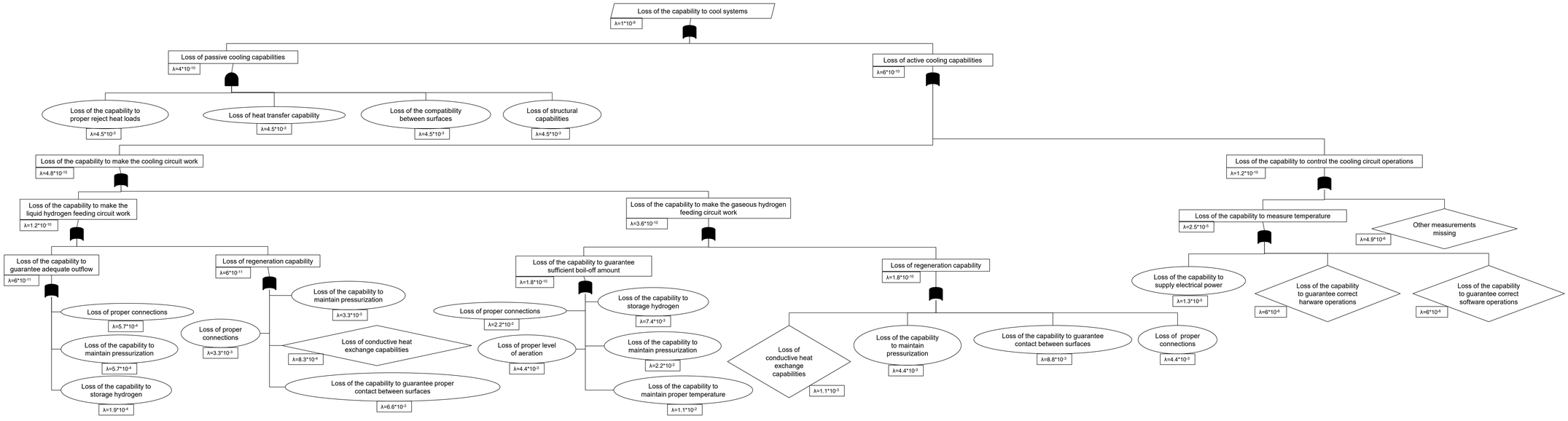
FTA: Loss of the capability to cool the primary structure (Top-down approach)

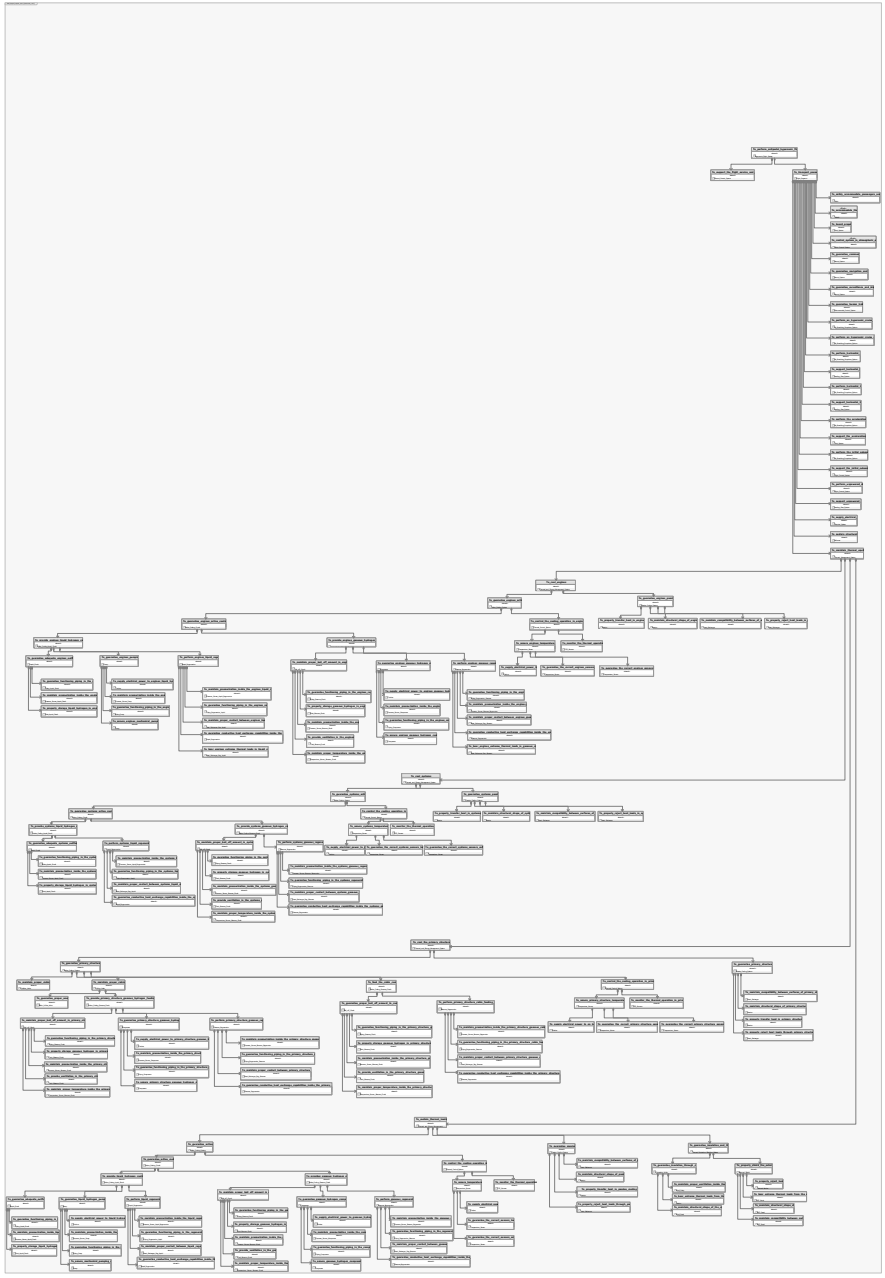


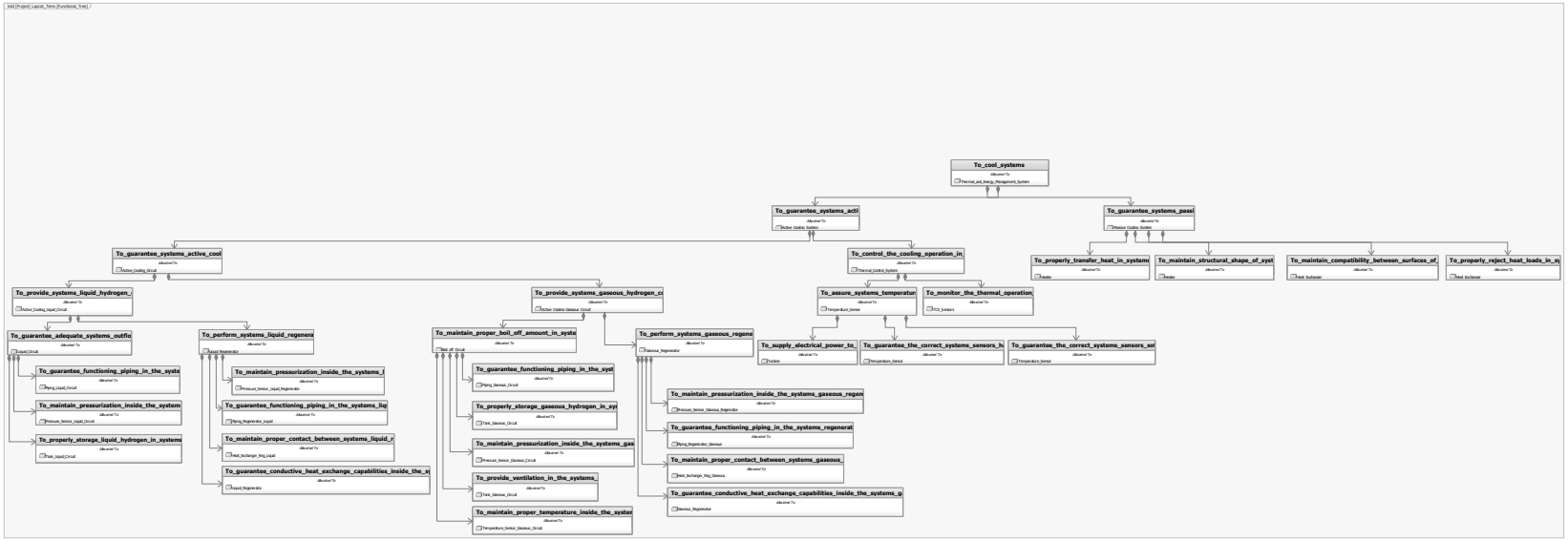
FTA: Loss of the capability to cool the systems

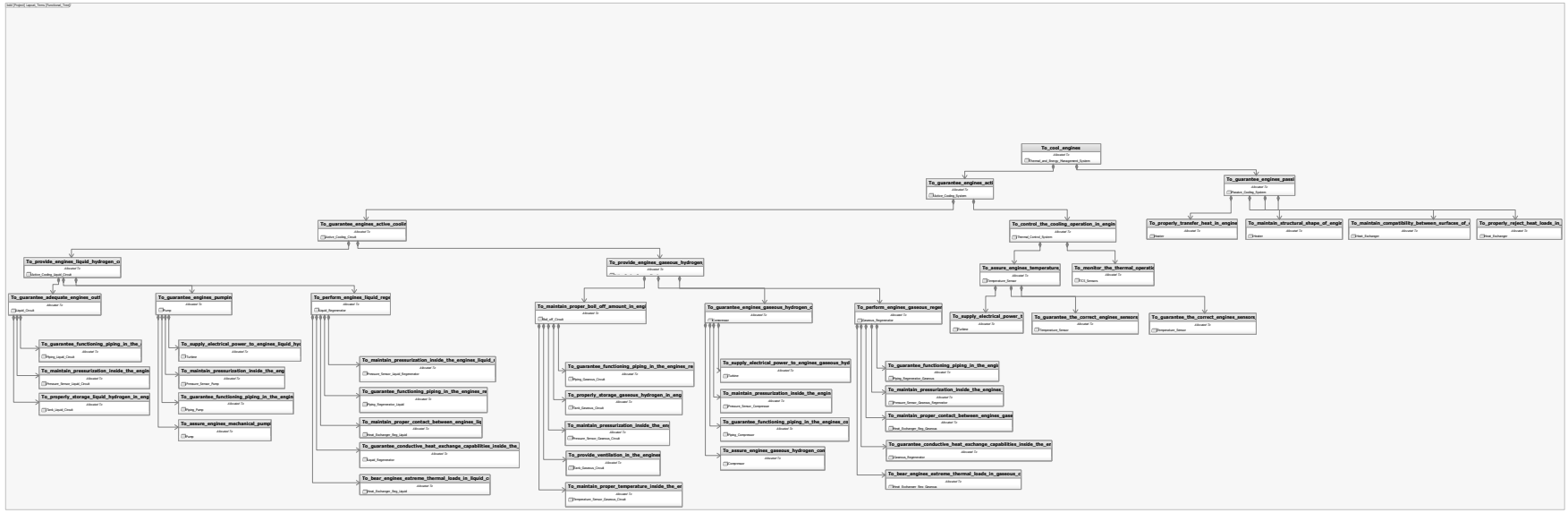


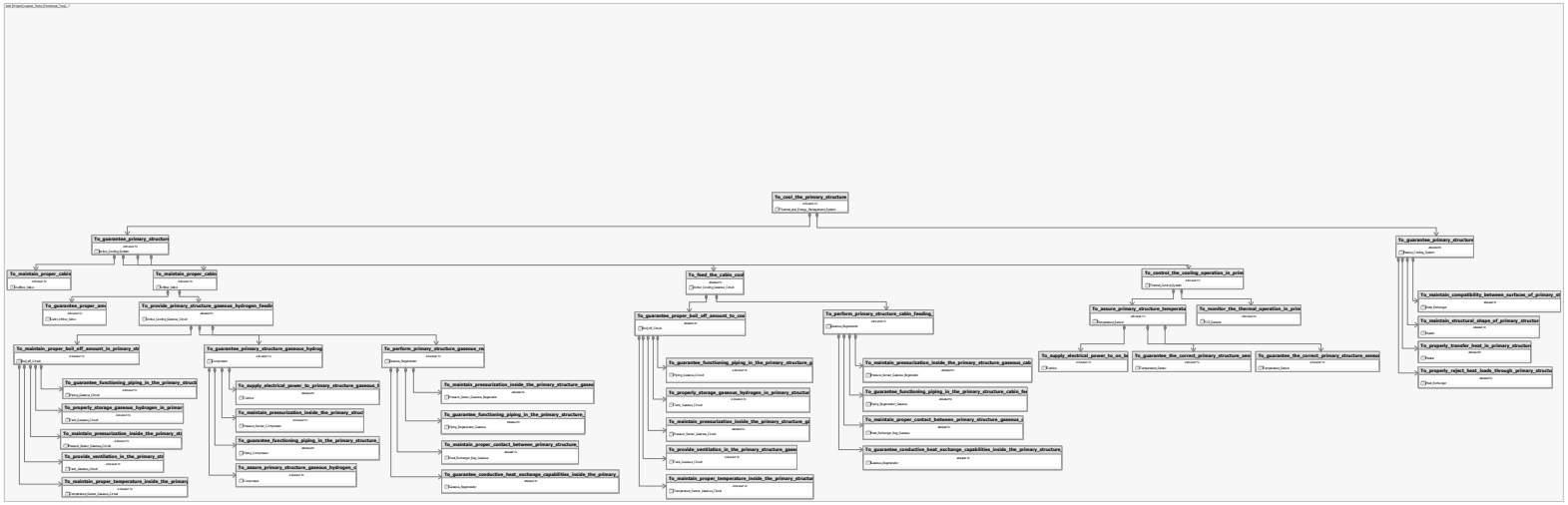
FTA: Loss of the capability to cool the systems (Top-down approach)

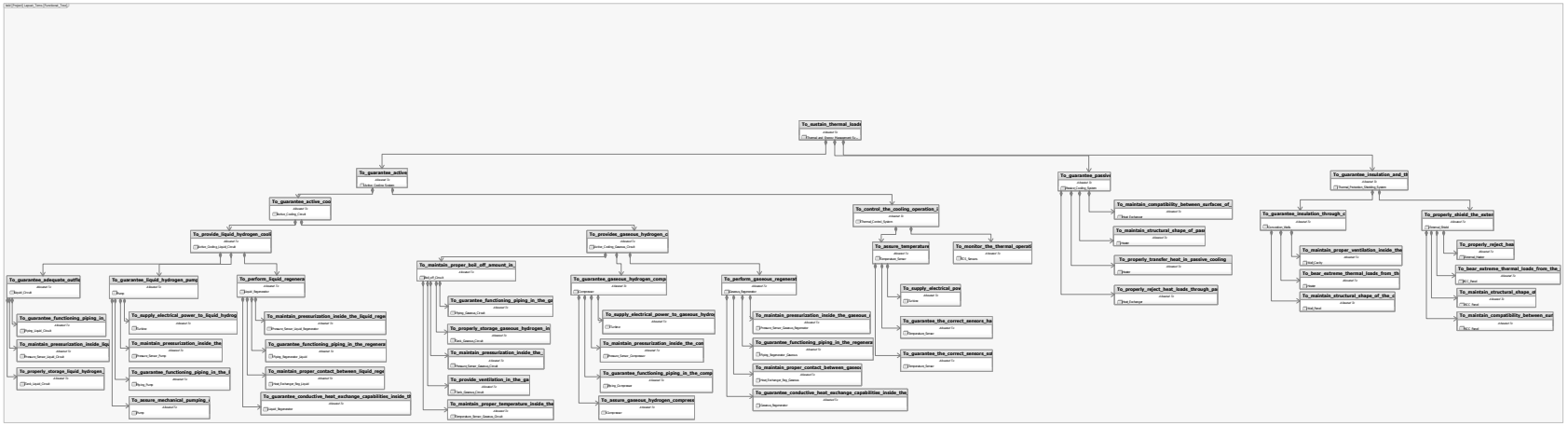


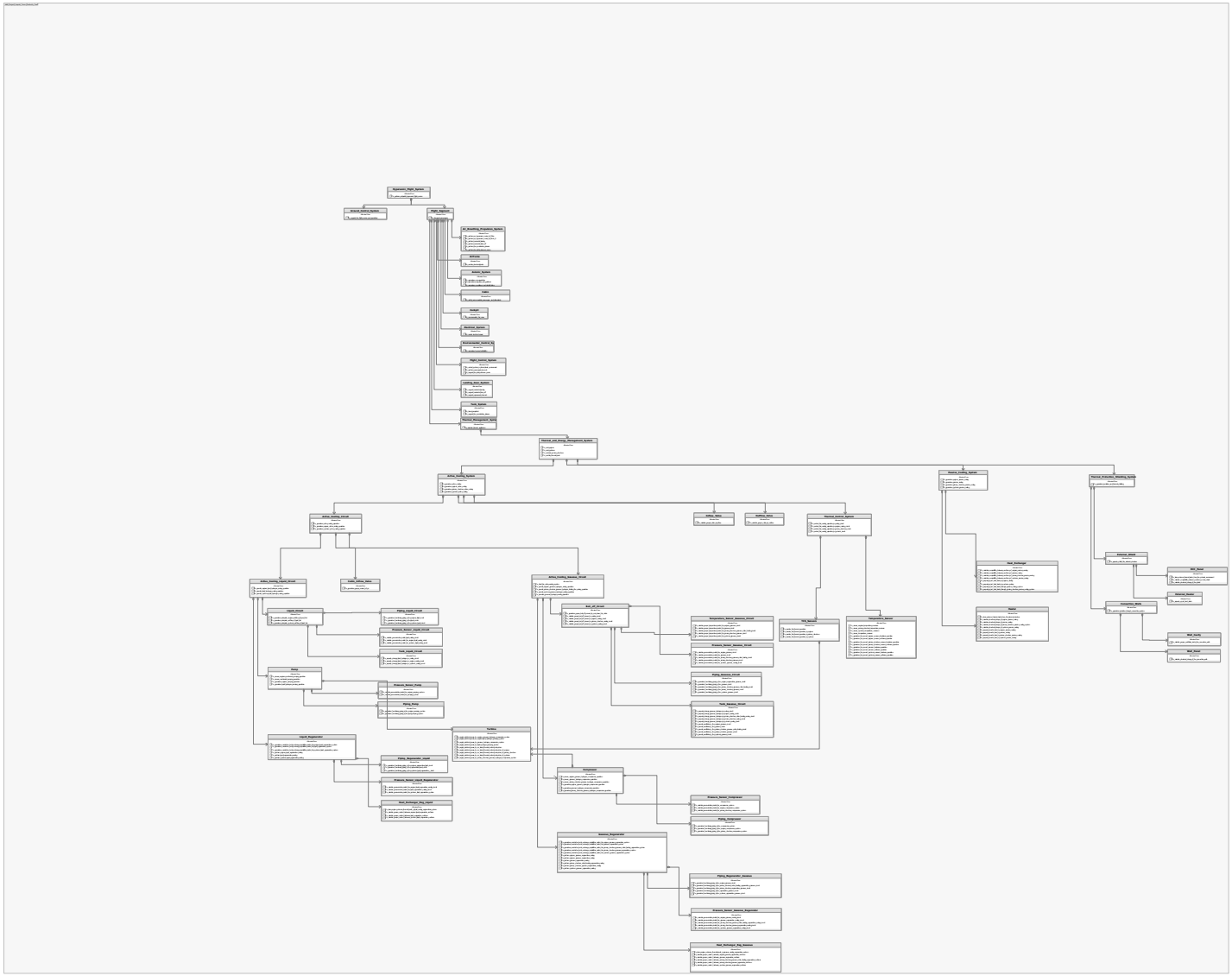



bdd [Project] Logical_Tree [Functional_Tree] /
To_cool_systems
Allocated To
Thermal_and_Energy_Management_System
To_guarantee_systems_acti
To_guarantee_systems_passi
To_guarantee_systems_active_cool
To_control_the_cooling_operation_in
To_properly_transfer_heat_in_systems
To_maintain_structural_shape_of_syst
To_maintain_compatibility_between_surfaces_of_
To_properly_reject_heat_loads_in_sy
To_provide_systems_liquid_hydrogen_
To_provide_systems_gaseous_hydrogen_co
To_assure_systems_temperatur
To_monitor_the_thermal_operation
To_guarantee_adequate_systems_outflo
To_perform_systems_liquid_regenera
To_maintain_proper_boil_off_amount_in_syste
To_perform_systems_gaseous_regene
To_supply_electrical_power_to_
To_guarantee_the_correct_systems_sensors_h
To_guarantee_the_correct_systems_sensors_sol
To_guarantee_functioning_piping_in_the_syste
To_maintain_pressurization_inside_the_systems_
To_guarantee_functioning_piping_in_the_syst
To_maintain_pressurization_inside_the_systems_gaseous_regen
To_maintain_pressurization_inside_the_system
To_guarantee_functioning_piping_in_the_systems_liq
To_properly_storage_gaseous_hydrogen_in_sy
To_guarantee_functioning_piping_in_the_systems_regenerat
To_properly_storage_liquid_hydrogen_in_systems
To_maintain_proper_contact_between_systems_liquid_r
To_maintain_pressurization_inside_the_systems_gas
To_maintain_proper_contact_between_systems_gaseous_
To_guarantee_conductive_heat_exchange_capabilities_inside_the_s
To_provide_ventilation_in_the_systems_
To_guarantee_conductive_heat_exchange_capabilities_inside_the_systems_g
To_maintain_proper_temperature_inside_the_systen

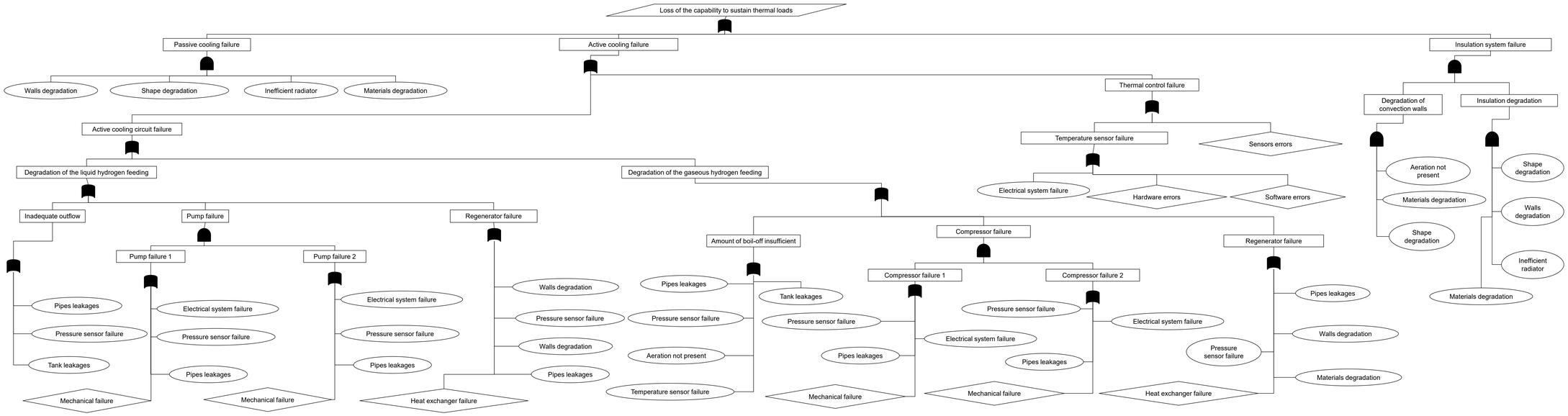

To_cool_engines
To_guarantee_engines_active_cooli
To_guarantee_engines_passi
To_control_the_cooling_operation_in_engin
To_provide_engines_liquid_hydrogen_c
To_provide_engines_gaseous_hydrogen
To_assure_engines_temperature_
To_monitor_the_thermal_operatio
To_guarantee_adequate_engines_cooli
To_guarantee_engines_pumpin
To_perform_engines_liquid_regu
To_maintain_proper_boil_off_amount_in_engi
To_guarantee_engines_gaseous_hydrogen_c
To_perform_engines_gaseous_regen
To_supply_electrical_power_t
To_guarantee_the_correct_engines_sensors
To_guarantee_the_correct_engines_sensors


To_cool_the_primary_structure
To_guarantee_primary_structure
To_maintain_proper_cabin
To_maintain_proper_cabin
To_guarantee_proper_aac
To_provide_primary_structure_gaseous_hydrogen_feedin
To_maintain_proper_boil_off_amount_in_primary_str
To_guarantee_primary_structure_gaseous_hydrog
To_perform_primary_structure_gaseous_re
To_guarantee_functioning_piping_in_the_primary_struct
To_properly_storage_gaseous_hydrogen_in_primar
To_maintain_pressurization_inside_the_primary_st
To_provide_ventilation_in_the_primary_str
To_maintain_proper_temperature_inside_the_primar
To_supply_electrical_power_to_primary_structure_gaseous_h
To_maintain_pressurization_inside_the_primary_struc
To_guarantee_functioning_piping_in_the_primary_structure_
To_ensure_primary_structure_gaseous_hydrogen_d
To_maintain_pressurization_inside_the_primary_structure_gaseo
To_guarantee_functioning_piping_in_the_primary_structure_
To_maintain_proper_contact_between_primary_structure_
To_guarantee_conductive_heat_exchange_capabilities_inside_the_primary_
To_feed_the_cabin_cool
To_guarantee_proper_boil_off_amount_to_coo
To_guarantee_functioning_piping_in_the_primary_structure_g
To_properly_storage_gaseous_hydrogen_in_primary_structur
To_maintain_pressurization_inside_the_primary_structure_ga
To_provide_ventilation_in_the_primary_structure_gase
To_maintain_proper_temperature_inside_the_primary_structur
To_perform_primary_structure_cabin_feeding_
To_maintain_pressurization_inside_the_primary_structure_gaseous_cab
To_guarantee_functioning_piping_in_the_primary_structure_cabin_fe
To_maintain_proper_contact_between_primary_structure_gaseous_c
To_guarantee_conductive_heat_exchange_capabilities_inside_the_primary_structure_
To_control_the_cooling_operation_in_prim
To_ensure_primary_structure_temperatu
To_monitor_the_thermal_operation_in_prim
To_supply_electrical_power_to_co_bo
To_guarantee_the_correct_primary_structure_sen
To_guarantee_the_correct_primary_structure_senso
To_guarantee_primary_structure
To_maintain_compatibility_between_surfaces_of_primary_st
To_maintain_structural_shape_of_primary_structur
To_properly_transfer_heat_in_primary_structur
To_properly_reject_heat_loads_through_primary_structu



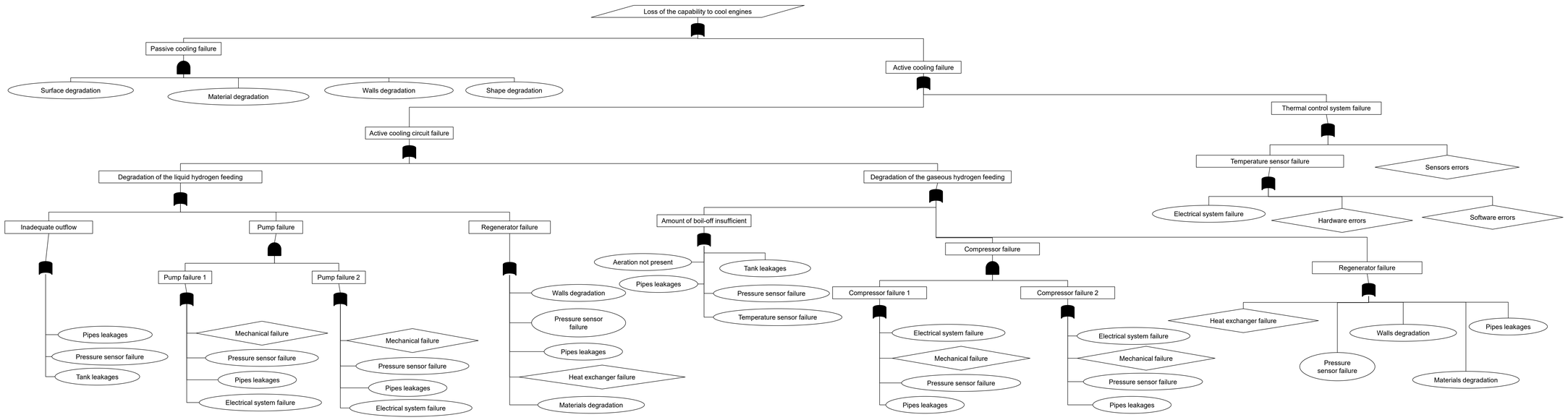


FTA (devices): Loss of the capability to sustain thermal loads

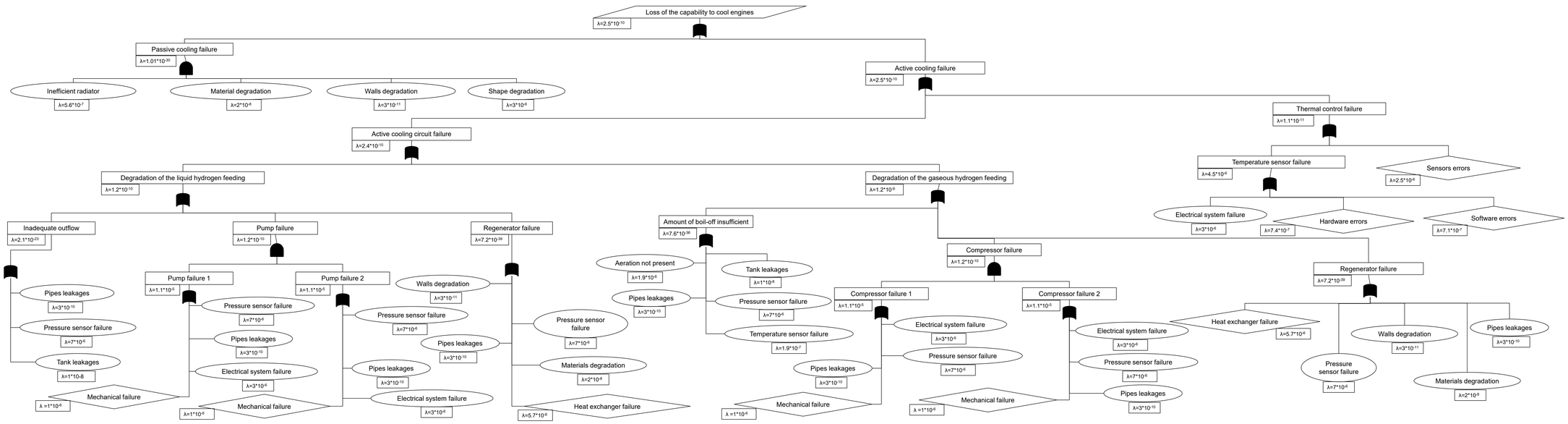


FTA (devices): Loss of the capability to sustain thermal loads (Bottom-up approach)

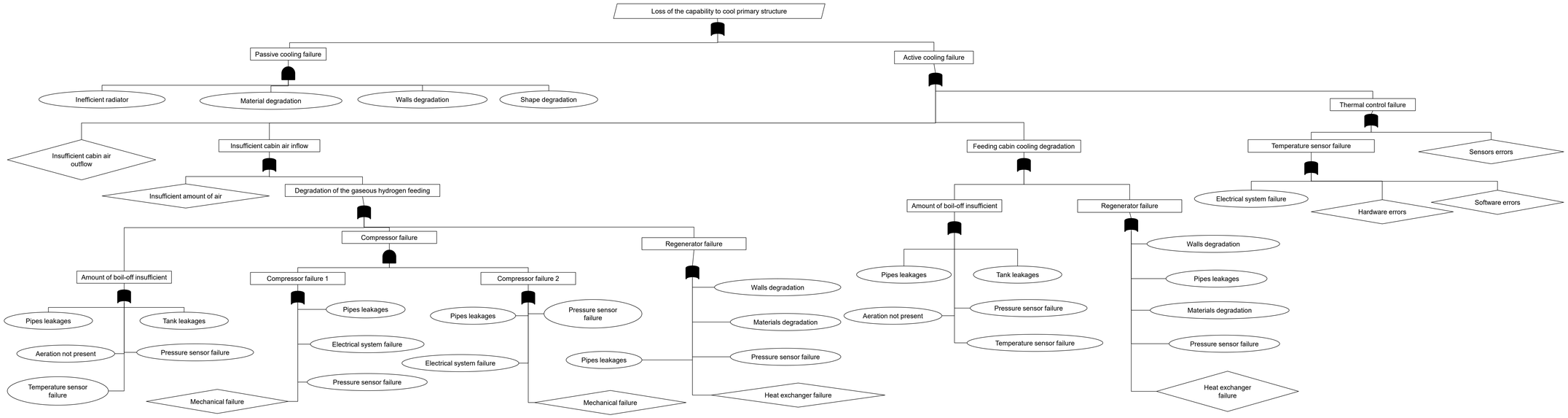
FTA (devices): Loss of the capability to cool the engines



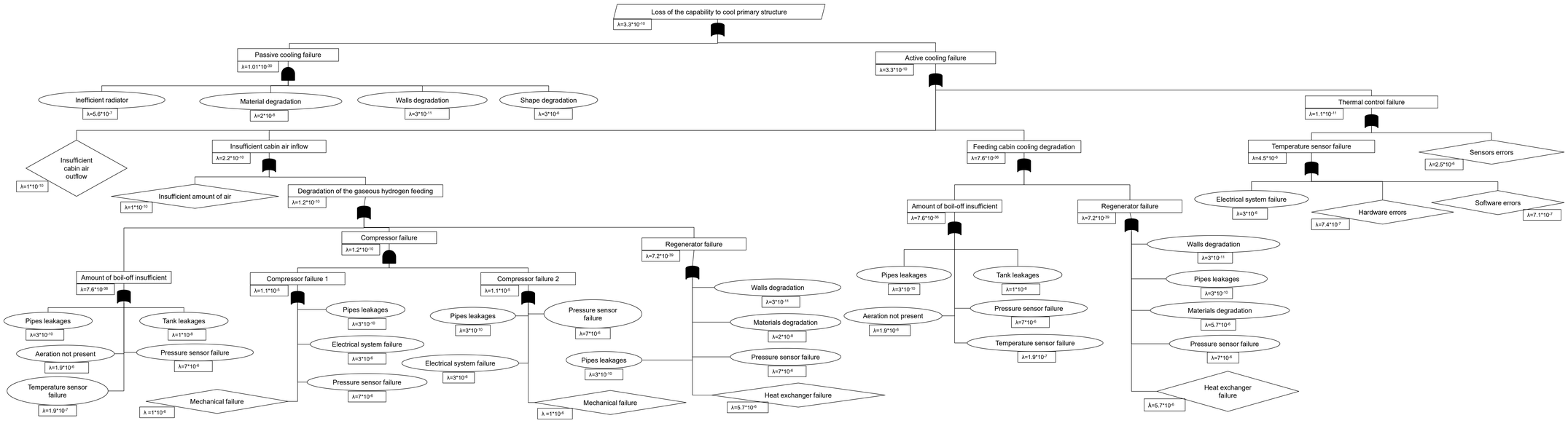
FTA (devices): Loss of the capability to cool the engines (Bottom-up approach)



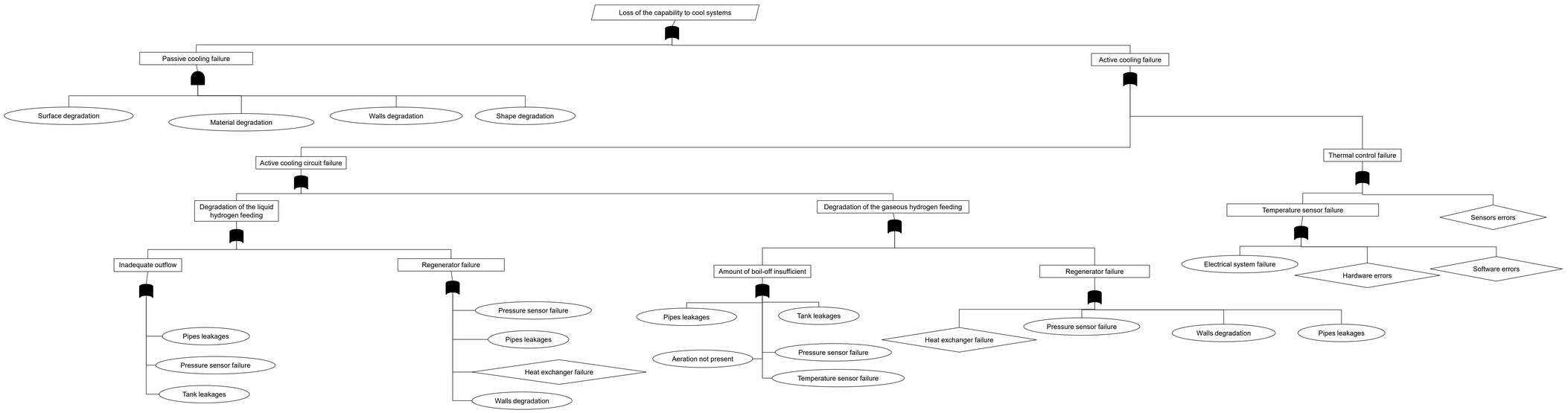
FTA (devices): Loss of the capability to cool the primary structure



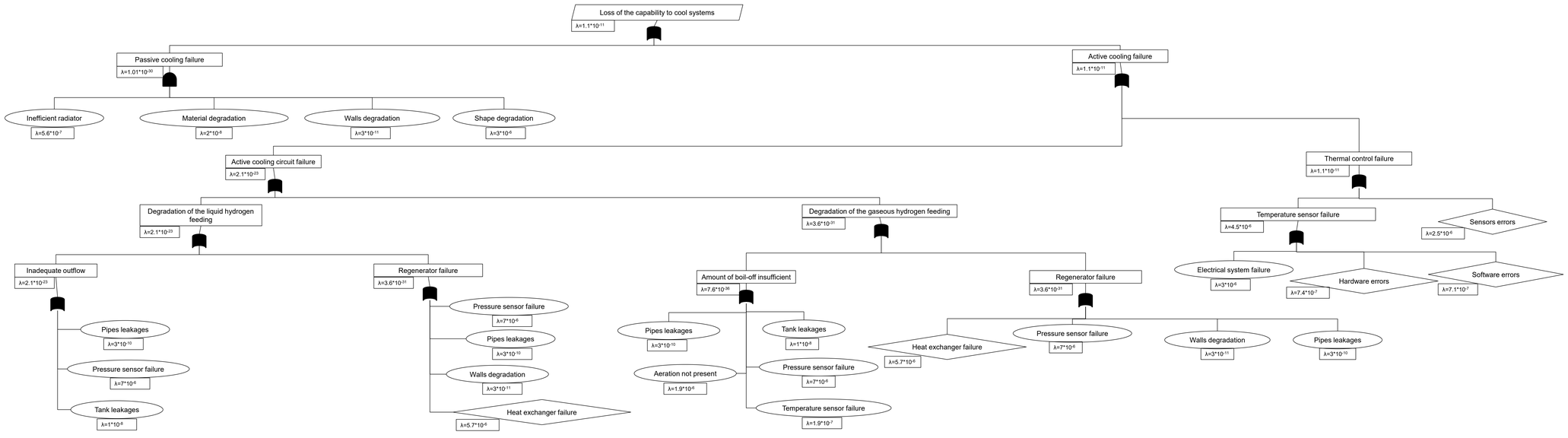
FTA (devices): Loss of the capability to cool the primary structure (Bottom-up approach)



FTA (devices): Loss of the capability to cool the systems



FTA (devices): Loss of the capability to cool the systems (Bottom-up approach)



Attachment H: Sub-systems functional Requirements and Safety Requirements

In this Attachment the Functional Requirements and their associated Safety Requirements are itemized and organized in different sector according to the devices they have been allocated to.

Tems

- The TEMS shall be able to cool down engines.
- *The probability of losing the capability to cool down engines shall be less than $1*10^{-9}$ failure/FH.*
- The TEMS shall be able to cool down the primary structure.
- *The probability of losing the capability to cool down primary structure shall be less than $1*10^{-9}$ failure/FH.*
- The TEMS shall be able to cool down systems.
- *The probability of losing the capability to cool down systems shall be less than $1*10^{-9}$ failure/FH.*
- The TEMS shall be able to sustain thermal loads.
- *The probability of losing the capability to sustain thermal loads shall be less than $1*10^{-9}$ failure/FH.*

Active system

- The Active system shall be able to guarantee active cooling.
- *The probability of losing active cooling capability shall be less than $6*10^{-10}$ failure/FH.*
- The Active system shall be able to guarantee engines active cooling.
- *The probability of losing engines active cooling capability shall be less than $8*10^{-10}$ failure/FH.*
- The Active system shall be able to guarantee primary structure active cooling.
- *The probability of losing primary structure active cooling capability shall be less than $6*10^{-10}$ failure/FH.*
- The Active system shall be able to guarantee systems active cooling.
- *The probability of losing systems active cooling capability shall be less than $6*10^{-10}$ failure/FH.*

Thermal protection and shielding system

- The Thermal protection and shielding system shall be able to guarantee insulation and thermal shielding.
- *The probability of losing insulation capability shall be less than $2*10^{-10}$ failure/FH.*

Passive system

- The Passive system shall be able to guarantee engines passive cooling.
- *The probability of losing engines passive cooling capability shall be less than $2*10^{-10}$ failure/FH.*
- The Passive system shall be able to guarantee systems passive cooling.
- *The probability of losing systems passive cooling capability shall be less than $4*10^{-10}$ failure/FH.*
- The Passive system shall be able to guarantee primary structure passive cooling.
- *The probability of losing primary structure passive cooling capability shall be less than $4*10^{-10}$ failure/FH.*
- The Passive system shall be able to guarantee passive cooling.
- *The probability of losing passive cooling capability shall be less than $2*10^{-10}$ failure/FH.*

Active cooling circuit

- The Active cooling circuit shall be able to guarantee active cooling operation.
- *The probability of losing active cooling circuit operation shall be less than $4.8*10^{-10}$ failure/FH.*

- The Active cooling circuit shall be able to guarantee engines active cooling operation.
- *The probability of losing engines active cooling circuit operation shall be less than $6.4*10^{-10}$ failure/FH.*
- The Active cooling circuit shall be able to guarantee systems active cooling operation.
- *The probability of losing systems active cooling circuit operation shall be less than $4.8*10^{-10}$ failure/FH.*

Thermal Control System

- The Thermal Control System shall be able to control cooling operation in cooling circuit.
- *The probability of losing the control of cooling operations shall be less than $1.2*10^{-10}$ failure/FH.*
- The Thermal Control System shall be able to control the cooling operation in engines cooling circuit.
- *The probability of losing the control of engines cooling operations shall be less than $1.2*10^{-10}$ failure/FH.*
- The Thermal Control System shall be able to control cooling operation in primary structure circuit.
- *The probability of losing the control of primary structure cooling operations shall be less than $1.5*10^{-10}$ failure/FH.*
- The Thermal Control System shall be able to control cooling operation in systems circuit.
- *The probability of losing the control of systems cooling operations shall be less than $1.2*10^{-10}$ failure/FH.*

Active cooling liquid circuit

- The Active cooling liquid circuit shall be able to provide engines liquid hydrogen cooling operation.
- *The probability of losing engines liquid hydrogen cooling operation shall be less than $3.2*10^{-10}$ failure/FH.*
- The Active cooling liquid shall be able to provide systems liquid hydrogen cooling operation.
- *The probability of losing systems liquid hydrogen cooling operation shall be less than $1.2*10^{-10}$ failure/FH.*
- The Active cooling liquid shall be able to provide liquid hydrogen cooling operation.
- *The probability of losing liquid hydrogen cooling operation shall be less than $2.4*10^{-10}$ failure/FH.*

Inflow valve

- The Inflow valve shall be able to maintain proper cabin air inflow.
- *The probability of losing the capability to maintain proper cabin air inflow shall be less than $2*10^{-10}$ failure/FH.*

Outflow valve

- The outflow valve shall be able to maintain proper cabin air outflow.
- *The probability of losing the capability to maintain proper cabin air outflow shall be less than $5*10^{-11}$ failure/FH.*

Cabin inflow valve

- The cabin inflow valve shall be able to guarantee proper amount of air inside the cabin.
- *The probability of losing the capability to guarantee the proper amount of air inside the cabin shall be less than $5*10^{-11}$ failure/FH.*

Liquid circuit

- The Liquid circuit shall be able to guarantee adequate engines outflow of liquid fuel.
- *The probability of losing the adequate engines outflow shall be less than $8*10^{-11}$ failure/FH.*
- The Liquid circuit shall be able to guarantee adequate systems outflow of liquid fuel.
- *The probability of losing the adequate systems outflow shall be less than $6*10^{-11}$ failure/FH.*
- The Liquid circuit shall be able to guarantee adequate outflow of liquid fuel.

- *The probability of losing the adequate outflow shall be less than $8*10^{-11}$ failure/FH.*

Piping liquid circuit

- The Piping of the liquid circuit shall be able to guarantee functioning piping in the engines liquid circuit.
- *The probability of losing proper connections in the engines liquid circuit shall be less than $6.8*10^{-4}$ failure/FH.*
- The Piping of the liquid circuit shall be able to guarantee functioning piping in the liquid circuit.
- *The probability of losing proper connections in the liquid circuit shall be less than $6.2*10^{-4}$ failure/FH.*
- The Piping of the liquid circuit shall be able to guarantee functioning piping in the systems liquid circuit.
- *The probability of losing proper connections in the systems liquid circuit shall be less than $5.7*10^{-4}$ failure/FH.*

Pressure sensor liquid circuit

- The Pressure sensor of the liquid circuit shall be able to maintain pressurization inside engines liquid cooling circuit.
- *The probability of losing the capability to maintain pressurization inside the engines liquid cooling circuit shall be less than $6.8*10^{-4}$ failure/FH.*
- The Pressure sensor of the liquid circuit shall be able to maintain pressurization inside liquid cooling circuit.
- *The probability of losing the capability to maintain pressurization inside the engines liquid cooling circuit shall be less than $6.2*10^{-4}$ failure/FH.*
- The Pressure sensor of the liquid circuit shall be able to maintain pressurization inside systems liquid cooling circuit.
- *The probability of losing the capability to maintain pressurization inside the systems liquid cooling circuit shall be less than $5.7*10^{-4}$ failure/FH.*

Tank liquid circuit

- The Tank of the liquid circuit shall be able to properly storage liquid hydrogen in cooling circuit.
- *The probability of losing the capability to storage liquid hydrogen in cooling circuit shall be less than $2.1*10^{-4}$ failure/FH.*
- The Tank of the liquid circuit shall be able to properly storage liquid hydrogen in engines cooling circuit.
- *The probability of losing the capability to storage liquid hydrogen in engines cooling circuit shall be less than $2.3*10^{-4}$ failure/FH.*
- The Tank of the liquid circuit shall be able to properly storage liquid hydrogen in systems cooling circuit.
- *The probability of losing the capability to storage liquid hydrogen in systems cooling circuit shall be less than $1.9*10^{-4}$ failure/FH.*

Pump

- The pump shall be able to guarantee liquid hydrogen pumping operation inside the engines cooling circuit.
- *The probability of losing the pumping operation in engines cooling circuit shall be less than $1.1*10^{-10}$ failure/FH.*
- The pump shall be able to assure engines mechanical pumping operation.

- *The probability of losing mechanical pumping operation in engines cooling circuit shall be less than $1.9*10^{-3}$ failure/FH.*
- The pump shall be able to guarantee liquid hydrogen pumping operation.
- *The probability of losing the pumping operation in cooling circuit shall be less than $8*10^{-11}$ failure/FH.*
- The pump shall be able to assure mechanical pumping operation.
- *The probability of losing mechanical pumping operation in cooling circuit shall be less than $1.5*10^{-3}$ failure/FH.*

Pressure sensor pump

- The Pressure sensor of the pump shall be able to maintain pressurization inside the engines pumping system.
- *The probability of losing pressurization inside the engines pumping system shall be less than $3.9*10^{-3}$ failure/FH.*
- The Pressure sensor of the pump shall be able to maintain pressurization inside the pumping system.
- *The probability of losing pressurization inside the pumping system shall be less than $3*10^{-3}$ failure/FH.*

Piping pump

- The Piping of the pump shall be able to guarantee functioning piping in the engines pumping system.
- *The probability of losing proper connections inside the engines pumping system shall be less than $3.9*10^{-3}$ failure/FH.*
- The Piping of the pump shall be able to guarantee functioning piping in the pumping system.
- *The probability of losing proper connections inside the pumping system shall be less than $3*10^{-3}$ failure/FH.*

Liquid regenerator

- The Regenerator of the liquid circuit shall be able to perform engines liquid regeneration cooling.
- *The probability of losing the capability to perform engines liquid regeneration cooling shall be less than $1.1*10^{-10}$ failure/FH.*
- The Regenerator of the liquid circuit shall be able to perform liquid regeneration cooling.
- *The probability of losing the capability to perform liquid regeneration cooling shall be less than $8*10^{-11}$ failure/FH.*
- The Regenerator of the liquid circuit shall be able to perform systems liquid regeneration cooling.
- *The probability of losing the capability to perform systems liquid regeneration cooling shall be less than $6*10^{-11}$ failure/FH.*
- The Regenerator of the liquid circuit shall be able to guarantee conductive heat exchange capabilities inside the liquid regeneration system.
- *The probability of losing conductive heat exchange capabilities inside the liquid regeneration system shall be less than $8.9*10^{-4}$ failure/FH.*
- The Regenerator of the liquid circuit shall be able to guarantee heat exchange capabilities inside the engines liquid regeneration system.
- *The probability of losing conductive heat exchange capabilities inside the engines liquid regeneration system shall be less than $2.9*10^{-3}$ failure/FH.*
- The Regenerator of the liquid circuit shall be able to guarantee heat exchange capabilities inside the systems liquid regeneration system.

- *The probability of losing conductive heat exchange capabilities inside the systems liquid regeneration system shall be less than $8.3*10^{-4}$ failure/FH.*

Piping regenerator liquid

- The Piping of the regenerator in the liquid circuit shall be able to guarantee functioning piping in the engines liquid regeneration circuit.
- *The probability of losing proper connection in the engines liquid regeneration cooling circuit shall be less than $1.1*10^{-2}$ failure/FH.*
- The Piping of the regenerator in the liquid circuit shall be able to guarantee functioning piping in the liquid regeneration circuit.
- *The probability of losing proper connection in liquid regeneration cooling circuit shall be less than $3.6*10^{-3}$ failure/FH.*
- The Piping of the regenerator in the liquid circuit shall be able to guarantee functioning piping in the systems liquid regeneration circuit.
- *The probability of losing proper connection in the systems liquid regeneration cooling circuit shall be less than $3.3*10^{-3}$ failure/FH.*

Pressure sensor liquid regenerator

- The Pressure sensor of the regenerator in the liquid circuit shall be able to maintain pressurization inside the engines liquid regeneration cooling circuit.
- *The probability of losing pressurization inside the engines liquid regeneration cooling circuit shall be less than $1.1*10^{-2}$ failure/FH.*
- The Pressure sensor of the regenerator in the liquid circuit shall be able to maintain pressurization inside the systems liquid regeneration cooling circuit.
- *The probability of losing pressurization inside the engines liquid regeneration cooling circuit shall be less than $3.3*10^{-3}$ failure/FH.*
- The Pressure sensor of the regenerator in the liquid circuit shall be able to maintain pressurization inside the liquid regeneration cooling circuit.
- *The probability of losing pressurization inside the liquid regeneration cooling circuit shall be less than $3.6*10^{-3}$ failure/FH.*

Heat exchanger regenerator liquid

- The Heat exchanger of the regenerator in the liquid circuit shall be able to bear extreme thermal loads in engines liquid regeneration system.
- *The probability of losing the capability to bear extreme thermal loads in engines liquid regeneration system shall be less than $1.1*10^{-2}$ failure/FH.*
- The Heat exchanger of the regenerator in the liquid circuit shall be able to maintain proper contact between engines liquid regenerator surfaces.
- *The probability of losing proper contact between engines liquid regenerator surfaces shall be less than $2.2*10^{-2}$ failure/FH.*
- The Heat exchanger of the regenerator in the liquid circuit shall be able to maintain proper contact between systems liquid regenerator surfaces.
- *The probability of losing proper contact between systems liquid regenerator surfaces shall be less than $6.6*10^{-3}$ failure/FH.*
- The Heat exchanger of the regenerator in the liquid circuit shall be able to maintain proper contact between liquid regenerator surfaces.
- *The probability of losing proper contact between liquid regenerator surfaces shall be less than $7.1*10^{-3}$ failure/FH.*

Active cooling gaseous circuit

- The Active gaseous cooling circuit shall be able to feed the cabin cooling system.
- *The probability of losing the capability to feed the cabin cooling system shall be less than $2*10^{-10}$ failure/FH.*
- The Active gaseous cooling circuit shall be able to provide engines gaseous hydrogen cooling operation.
- *The probability of losing the capability to provide engines gaseous hydrogen cooling operation shall be less than $3.2*10^{-10}$ failure/FH.*
- The Active gaseous cooling circuit shall be able to provide systems gaseous hydrogen cooling operation.
- *The probability of losing the capability to provide systems gaseous hydrogen cooling operation shall be less than $3.6*10^{-10}$ failure/FH.*
- The Active gaseous cooling circuit shall be able to provide primary structure gaseous hydrogen cooling operation.
- *The probability of losing the capability to provide primary structure gaseous hydrogen cooling operation shall be less than $1.5*10^{-10}$ failure/FH.*
- The Active gaseous cooling circuit shall be able to provide gaseous hydrogen cooling operation.
- *The probability of losing the capability to provide gaseous hydrogen cooling operation shall be less than $2.4*10^{-10}$ failure/FH.*

Boil-off circuit

- The Boil-off circuit shall be able to guarantee proper boil-off amount to cool down the cabin.
- *The probability of losing the capability to guarantee proper boil-off amount to cool down the cabin shall be less than $1*10^{-10}$ failure/FH.*
- The Boil-off circuit shall be able to maintain proper boil-off amount in cooling circuit.
- *The probability of losing the capability to maintain proper boil-off amount in cooling circuit shall be less than $8*10^{-11}$ failure/FH.*
- The Boil-off circuit shall be able to maintain proper boil-off amount in engines cooling circuit.
- *The probability of losing the capability to maintain proper boil-off amount in engines cooling circuit shall be less than $1.1*10^{-10}$ failure/FH.*
- The Boil-off circuit shall be able to maintain proper boil-off amount in systems cooling circuit.
- *The probability of losing the capability to maintain proper boil-off amount in systems cooling circuit shall be less than $1.8*10^{-10}$ failure/FH.*
- The Boil-off circuit shall be able to maintain proper boil-off amount in primary structure cooling circuit.
- *The probability of losing the capability to maintain proper boil-off amount in primary structure cooling circuit shall be less than $5*10^{-11}$ failure/FH.*

Temperature sensor gaseous circuit

- The Temperature sensor in the gaseous circuit shall be able to maintain proper temperature inside the gaseous circuit.
- *The probability of losing the proper temperature inside the gaseous cooling circuit shall be less than $9.4*10^{-3}$ failure/FH.*
- The Temperature sensor in the gaseous circuit shall be able to maintain proper temperature inside the engines gaseous circuit.

- *The probability of losing the proper temperature inside the engines gaseous cooling circuit shall be less than $1*10^{-2}$ failure/FH.*
- The Temperature sensor in the gaseous circuit shall be able to maintain proper temperature inside the systems gaseous circuit.
- *The probability of losing the proper temperature inside the systems gaseous cooling circuit shall be less than $1.8*10^{-10}$ failure/FH.*
- The Temperature sensor in the gaseous circuit shall be able to maintain proper temperature inside the primary structure gaseous circuit.
- *The probability of losing the proper temperature inside the primary structure gaseous cooling circuit shall be less than $8.6*10^{-3}$ failure/FH.*
- The Temperature sensor in the gaseous circuit shall be able to maintain proper temperature inside the primary structure gaseous cabin feeding circuit.
- *The probability of losing the proper temperature inside the primary structure gaseous cabin feeding circuit shall be less than $9.9*10^{-3}$ failure/FH.*

Pressure sensor gaseous circuit

- The Pressure sensor in the gaseous circuit shall be able to maintain pressurization inside gaseous circuit.
- *The probability of losing pressurization inside the gaseous cooling circuit shall be less than $1.9*10^{-2}$ failure/FH.*
- The Pressure sensor in the gaseous circuit shall be able to maintain pressurization inside engines gaseous circuit.
- *The probability of losing pressurization inside the engines gaseous cooling circuit shall be less than $2*10^{-2}$ failure/FH*
- The Pressure sensor in the gaseous circuit shall be able to maintain pressurization inside systems gaseous circuit.
- *The probability of losing pressurization inside the systems gaseous cooling circuit shall be less than $2.2*10^{-2}$ failure/FH.*
- The Pressure sensor in the gaseous circuit shall be able to maintain pressurization inside the primary structure gaseous circuit.
- *The probability of losing pressurization inside the primary structure gaseous cooling circuit shall be less than $1.7*10^{-2}$ failure/FH.*
- The Pressure sensor in the gaseous circuit shall be able to maintain pressurization inside the primary structure gaseous cabin feeding circuit.
- *The probability of losing pressurization inside the primary structure gaseous cabin feeding cooling circuit shall be less than $1.9*10^{-2}$ failure/FH.*

Piping gaseous circuit

- The Piping of the gaseous circuit shall be able to guarantee functioning piping in the gaseous circuit.
- *The probability of losing proper connection in the gaseous cooling circuit shall be less than $1.9*10^{-2}$ failure/FH.*
- The Piping of the gaseous circuit shall be able to guarantee functioning piping in the engines gaseous circuit.
- *The probability of losing proper connection in the engines gaseous cooling circuit shall be less than $2*10^{-2}$ failure/FH.*
- The Piping of the gaseous circuit shall be able to guarantee functioning piping in the systems gaseous circuit.

- *The probability of losing proper connection in the systems gaseous cooling circuit shall be less than $2.2*10^{-2}$ failure/FH.*
- The Piping of the gaseous circuit shall be able to guarantee functioning piping in the primary structure gaseous circuit.
- *The probability of losing proper connection in the primary structure gaseous cooling circuit shall be less than $1.7*10^{-2}$ failure/FH.*
- The Piping of the gaseous circuit shall be able to guarantee functioning piping in the primary structure cabin feeding gaseous circuit.
- *The probability of losing proper connection in the engines gaseous cooling circuit shall be less than $1.9*10^{-2}$ failure/FH.*

Tank gaseous circuit

- The Tank of the gaseous circuit shall be able to properly storage gaseous hydrogen in cooling circuit.
- *The probability of losing the capability to storage gaseous hydrogen in cooling circuit shall be less than $6.3*10^{-3}$ failure/FH.*
- The Tank of the gaseous circuit shall be able to properly storage gaseous hydrogen in engines cooling circuit.
- *The probability of losing the capability to storage gaseous hydrogen in engines cooling circuit shall be less than $6.7*10^{-3}$ failure/FH.*
- The Tank of the gaseous circuit shall be able to properly storage gaseous hydrogen in systems cooling circuit.
- *The probability of losing the capability to storage gaseous hydrogen in systems cooling circuit shall be less than $7.4*10^{-3}$ failure/FH.*
- The Tank of the gaseous circuit shall be able to properly storage gaseous hydrogen in primary structure cooling circuit.
- *The probability of losing the capability to storage gaseous hydrogen in primary structure cooling circuit shall be less than $5.7*10^{-3}$ failure/FH.*
- The Tank of the gaseous circuit shall be able to properly storage gaseous hydrogen in primary structure feeding cabin cooling circuit.
- *The probability of losing the capability to storage gaseous hydrogen in primary structure cabin feeding cooling circuit shall be less than $6.6*10^{-3}$ failure/FH.*
- The Tank of the gaseous circuit shall be able to provide ventilation in the engines gaseous circuit.
- *The probability of losing the capability to provide ventilation in the engines gaseous hydrogen cooling circuit shall be less than $4*10^{-3}$ failure/FH.*
- The Tank of the gaseous circuit shall be able to provide ventilation in the systems gaseous circuit.
- *The probability of losing the capability to provide ventilation in the systems gaseous hydrogen cooling circuit shall be less than $4.4*10^{-3}$ failure/FH.*
- The Tank of the gaseous circuit shall be able to provide ventilation in the gaseous circuit.
- *The probability of losing the capability to provide ventilation in the gaseous hydrogen cooling circuit shall be less than $3.8*10^{-3}$ failure/FH.*
- The Tank of the gaseous circuit shall be able to provide ventilation in the primary structure gaseous circuit.
- *The probability of losing the capability to provide ventilation in the primary structure gaseous hydrogen cooling circuit shall be less than $3.4*10^{-3}$ failure/FH.*

- The Tank of the gaseous circuit shall be able to provide ventilation in the primary structure gaseous cabin feeding circuit.
- *The probability of losing the capability to provide ventilation in the primary structure gaseous hydrogen cooling circuit shall be less than $3.9*10^{-3}$ failure/FH.*

Compressor

- The compressor shall be able to guarantee engines gaseous hydrogen compression operation.
- *The probability of losing gaseous hydrogen compression operation in engines cooling circuit shall be less than $1.1*10^{-10}$ failure/FH.*
- The compressor shall be able to guarantee primary structure gaseous hydrogen compression operation.
- *The probability of losing gaseous hydrogen compression operation in primary structure cooling circuit shall be less than $5*10^{-11}$ failure/FH.*
- The compressor shall be able to guarantee gaseous hydrogen compression operation.
- *The probability of losing gaseous hydrogen compression operation in cooling circuit shall be less than $8*10^{-11}$ failure/FH.*
- The compressor shall be able to assure engines gaseous hydrogen compression operation.
- *The probability of losing mechanical compression operation in engines cooling circuit shall be less than $1.9*10^{-3}$ failure/FH.*
- The compressor shall be able to assure gaseous hydrogen compression operation.
- *The probability of losing mechanical compression operation in cooling circuit shall be less than $1.5*10^{-3}$ failure/FH.*
- The compressor shall be able to assure primary structure gaseous hydrogen compression operation.
- *The probability of losing mechanical compression operation in primary structure cooling circuit shall be less than $1.3*10^{-3}$ failure/FH.*

Pressure sensor compressor

- The Pressure sensor of the compressor shall be able to maintain pressurization inside the compression system.
- *The probability of losing pressurization inside the compression system shall be less than $3*10^{-3}$ failure/FH.*
- The Pressure sensor of the compressor shall be able to maintain pressurization inside the engines compression system.
- *The probability of losing pressurization inside the engines compression system shall be less than $3.9*10^{-3}$ failure/FH.*
- The Pressure sensor of the compressor shall be able to maintain pressurization inside the primary structure compression system.
- *The probability of losing pressurization inside the primary structure compression system shall be less than $2.7*10^{-3}$ failure/FH.*

Piping compressor

- The Piping in the compressor shall be able to guarantee functioning piping in the engines compression system.
- *The probability of losing proper connection in the engines compression system shall be less than $3.9*10^{-3}$ failure/FH.*
- The Piping in the compressor shall be able to guarantee functioning piping in the compression system.

- *The probability of losing proper connection in the compression system shall be less than $3*10^{-3}$ failure/FH.*
- The Piping in the compressor shall be able to guarantee functioning piping in the primary structure compression system.
- *The probability of losing proper connection in the primary structure compression system shall be less than $2.7*10^{-3}$ failure/FH.*

Turbine

- The Turbine shall be able to supply electrical power to the gaseous hydrogen compression system.
- *The probability of losing the capability to supply electrical power to the gaseous hydrogen compression system shall be less than $3*10^{-3}$ failure/FH.*
- The Turbine shall be able to supply electrical power to the liquid hydrogen pumping system.
- *The probability of losing the capability to supply electrical power to the liquid hydrogen pumping system shall be less than $3*10^{-3}$ failure/FH.*
- The Turbine shall be able to supply electrical power to primary structure gaseous hydrogen compression system.
- *The probability of losing the capability to supply electrical power to primary structure gaseous hydrogen compression system shall be less than $2.7*10^{-3}$ failure/FH.*
- The Turbine shall be able to supply electrical power to engines liquid hydrogen pumping system.
- *The probability of losing the capability to supply electrical power to engines liquid hydrogen pumping system shall be less than $3.9*10^{-3}$ failure/FH.*
- The Turbine shall be able to supply electrical power to engines gaseous hydrogen compression system.
- *The probability of losing the capability to supply electrical power to engines gaseous hydrogen compression system shall be less than $3.9*10^{-3}$ failure/FH.*
- The Turbine shall be able to supply electrical power to primary structure TCS.
- *The probability of losing electrical power to primary structure TCS shall be less than $1.5*10^{-5}$ failure/FH.*
- The Turbine shall be able to supply electrical power to engines TCS.
- *The probability of losing electrical power to engines TCS shall be less than $1.4*10^{-5}$ failure/FH.*
- The Turbine shall be able to supply electrical power to systems TCS.
- *The probability of losing electrical power to systems TCS shall be less than $1.3*10^{-5}$ failure/FH.*
- The Turbine shall be able to supply electrical power to TCS.
- *The probability of losing electrical power to TCS shall be less than $1.3*10^{-5}$ failure/FH.*

Gaseous regenerator

- The Gaseous regenerator shall be able to perform engines gaseous regeneration cooling.
- *The probability of losing the capability to perform engines gaseous regeneration cooling shall be less than $1.1*10^{-10}$ failure/FH.*
- The Gaseous regenerator shall be able to perform gaseous regeneration cooling.
- *The probability of losing the capability to perform gaseous regeneration cooling shall be less than $8*10^{-11}$ failure/FH.*
- The Gaseous regenerator shall be able to perform primary structure gaseous regeneration cooling.

- *The probability of losing the capability to perform primary structure gaseous regeneration cooling shall be less than $5*10^{-11}$ failure/FH.*
- The Gaseous regenerator shall be able to perform primary structure gaseous cabin feeding regeneration cooling.
- *The probability of losing the capability to perform primary structure gaseous cabin feeding regeneration cooling shall be less than $1*10^{-10}$ failure/FH.*
- The Gaseous regenerator shall be able to perform systems gaseous regeneration cooling.
- *The probability of losing the capability to perform systems gaseous regeneration cooling shall be less than $1.8*10^{-10}$ failure/FH.*
- The Gaseous regenerator shall be able to guarantee conductive heat exchange capabilities inside the gaseous regeneration system.
- *The probability of losing conductive heat exchange capabilities inside the gaseous regeneration system shall be less than $8.9*10^{-4}$ failure/FH.*
- The Gaseous regenerator shall be able to guarantee conductive heat exchange capabilities inside the engines gaseous regeneration system.
- *The probability of losing conductive heat exchange capabilities inside the engines gaseous regeneration system shall be less than $2.9*10^{-3}$ failure/FH.*
- The Gaseous regenerator shall be able to guarantee heat exchange capabilities inside the primary structure gaseous regeneration system.
- *The probability of losing conductive heat exchange capabilities inside the primary structure gaseous regeneration system shall be less than $2.5*10^{-3}$.*
- The Gaseous regenerator shall be able to guarantee heat exchange capabilities inside the primary structure gaseous cabin feeding regeneration system.
- *The probability of losing conductive heat exchange capabilities inside the primary structure gaseous cabin feeding regeneration system shall be less than $2.9*10^{-3}$ failure/FH.*
- The Gaseous regenerator shall be able to guarantee heat exchange capabilities inside the systems gaseous regeneration system.
- *The probability of losing conductive heat exchange capabilities inside the systems gaseous regeneration system shall be less than $1.1*10^{-3}$ failure/FH.*

Piping regenerator gaseous

- The Piping of the regenerator in the gaseous circuit shall be able to guarantee functioning piping in the engines gaseous regeneration circuit.
- *The probability of losing proper connection in the engines gaseous regeneration circuit shall be less than $1.1*10^{-2}$ failure/FH.*
- The Piping of the regenerator in the gaseous circuit shall be able to guarantee functioning piping in the gaseous regeneration circuit.
- *The probability of losing proper connection in the gaseous regeneration circuit shall be less than $3.6*10^{-3}$ failure/FH.*
- The Piping of the regenerator in the gaseous circuit shall be able to guarantee functioning piping in the systems gaseous regeneration circuit.
- *The probability of losing proper connection in the systems gaseous regeneration circuit shall be less than $4.4*10^{-3}$ failure/FH.*
- The Piping of the regenerator in the gaseous circuit shall be able to guarantee functioning piping in the primary structure gaseous regeneration circuit.
- *The probability of losing proper connection in the primary structure gaseous regeneration circuit shall be less than $1*10^{-2}$ failure/FH.*

- The Piping of the regenerator in the gaseous circuit shall be able to guarantee functioning piping in the primary structure gaseous cabin feeding regeneration circuit.
- *The probability of losing proper connection in the primary structure gaseous cabin feeding regeneration circuit shall be less than $1.1*10^{-2}$ failure/FH.*

Pressure sensor gaseous regenerator

- The Pressure sensor of the regenerator in the gaseous circuit shall be able to maintain pressurization inside the engines gaseous regeneration cooling circuit.
- *The probability of losing pressurization inside the engines gaseous regeneration cooling circuit shall be less than $1.1*10^{-2}$ failure/FH.*
- The Pressure sensor of the regenerator in the gaseous circuit shall be able to maintain pressurization inside the gaseous regeneration cooling circuit.
- *The probability of losing pressurization inside the gaseous regeneration cooling circuit shall be less than $3.6*10^{-3}$ failure/FH.*
- The Pressure sensor of the regenerator in the gaseous circuit shall be able to maintain pressurization inside the primary structure gaseous cabin feeding regeneration cooling circuit.
- *The probability of losing pressurization inside the primary structure gaseous cabin feeding regeneration cooling circuit shall be less than $1.1*10^{-2}$ failure/FH.*
- The Pressure sensor of the regenerator in the gaseous circuit shall be able to maintain pressurization inside the primary structure gaseous regeneration cooling circuit.
- *The probability of losing pressurization inside the engines gaseous regeneration cooling circuit shall be less than $1*10^{-2}$ failure/FH.*
- The Pressure sensor of the regenerator in the gaseous circuit shall be able to maintain pressurization inside the systems gaseous regeneration cooling circuit.
- *The probability of losing pressurization inside the systems gaseous regeneration cooling circuit shall be less than $4.4*10^{-3}$ failure/FH.*

Heat exchanger regeneration gaseous

- The Heat exchanger of the regenerator in the gaseous circuit shall be able to bear extreme thermal loads in engines gaseous cooling regeneration system.
- *The probability of losing the capability to bear engines extreme thermal loads in gaseous regeneration system shall be less than $1.1*10^{-2}$ failure/FH.*
- The Heat exchanger of the regenerator in the gaseous circuit shall be able to maintain proper contact between engines gaseous regenerator surfaces.
- *The probability of losing proper contact between engines gaseous regenerator surfaces shall be less than $2.2*10^{-2}$ failure/FH.*
- The Heat exchanger of the regenerator in the gaseous circuit shall be able to maintain proper contact between gaseous regenerator surfaces.
- *The probability of losing proper contact between gaseous regenerator surfaces shall be less than $7.1*10^{-3}$ failure/FH.*
- The Heat exchanger of the regenerator in the gaseous circuit shall be able to maintain proper contact between primary structure cabin feeding gaseous regenerator surfaces.
- *The probability of losing proper contact between primary structure cabin feeding gaseous regenerator surfaces shall be less than $2.2*10^{-2}$ failure/FH.*
- The Heat exchanger of the regenerator in the gaseous circuit shall be able to maintain proper contact between primary structure gaseous regenerator surfaces.
- *The probability of losing proper contact between primary structure gaseous regenerator surfaces shall be less than $2*10^{-2}$ failure/FH.*

- The Heat exchanger of the regenerator in the gaseous circuit shall be able to maintain proper contact between systems gaseous regenerator surfaces.
- *The probability of losing proper contact between systems gaseous regenerator surfaces shall be less than $8.5*10^{-3}$ failure/FH.*

TCS sensors

- The TCS sensor shall be able to monitor the thermal operation.
- *The probability of losing the capability to monitor the thermal operation shall be less than $1.2*10^{-10}$ failure/FH.*
- The TCS sensor shall be able to monitor the thermal operation in engines.
- *The probability of losing the capability to monitor the thermal operation in engines shall be less than $1.6*10^{-10}$ failure/FH.*
- The TCS sensor shall be able to monitor the thermal operation in systems.
- *The probability of losing the capability to monitor the thermal operation in systems shall be less than $1.2*10^{-10}$ failure/FH.*
- The TCS sensor shall be able to monitor the thermal operation in primary structure.
- *The probability of losing the capability to monitor the thermal operation shall be less than $1.5*10^{-10}$ failure/FH.*

Temperature sensor

- The Temperature sensor shall be able to assure engines temperature measure.
- *The probability of losing the capability to assure engines temperature measure shall be less than $2.8*10^{-5}$ failure/FH.*
- The Temperature sensor shall be able to assure systems temperature measure.
- *The probability of losing the capability to assure systems temperature measure shall be less than $2.5*10^{-5}$ failure/FH.*
- The Temperature sensor shall be able to assure primary structure temperature measure.
- *The probability of losing the capability to assure primary structure temperature measure shall be less than $2.7*10^{-5}$ failure/FH.*
- The Temperature sensor shall be able to assure temperature measure.
- *The probability of losing the capability to assure temperature measure shall be less than $2.5*10^{-5}$ failure/FH.*
- The Temperature sensor shall be able to guarantee the correct engines sensors hardware operation.
- *The probability of losing correct engines sensors hardware operation shall be less than $7*10^{-8}$ failure/FH.*
- The Temperature sensor shall be able to guarantee the correct engines sensors software operation.
- *The probability of losing correct engines sensors software operation shall be less than $7*10^{-8}$ failure/FH.*
- The Temperature sensor shall be able to guarantee the correct systems sensors hardware operation.
- *The probability of losing correct systems sensors hardware operation shall be less than $6*10^{-8}$ failure/FH.*
- The Temperature sensor shall be able to guarantee the correct systems sensors software operation.
- *The probability of losing correct systems sensors software operation shall be less than $6*10^{-8}$ failure/FH.*
- The Temperature sensor shall be able to guarantee the correct sensors hardware operation.
- *The probability of losing correct sensors hardware operation shall be less than $6*10^{-8}$ failure/FH.*

- The Temperature sensor shall be able to guarantee the correct sensors software operation.
- *The probability of losing correct sensors software operation shall be less than $6*10^{-8}$ failure/FH.*
- The Temperature sensor shall be able to guarantee the correct primary structure sensors hardware operation.
- *The probability of losing correct primary structure sensors hardware operation shall be less than $6*10^{-8}$ failure/FH.*
- The Temperature sensor shall be able to guarantee the correct primary structure sensors software operation.
- *The probability of losing correct primary structure sensors software operation shall be less than $6*10^{-8}$ failure/FH.*

External shield

- The External shield shall be able to properly shield the external structure.
- *The probability of losing the capability to properly shield the external structure shall be less than $1.4*10^{-5}$ failure/FH.*

Convection walls

- The Convection wall shall be able to guarantee insulation through convection system.
- *The probability of losing the capability to insulate through convection system shall be less than $1.4*10^{-5}$ failure/FH.*

RCC panel

- The RCC panel shall be able to bear extreme thermal loads from the external environment.
- *The probability of losing the capability to extreme thermal loads from the external environment shall be less than $6.1*10^{-2}$ failure/FH.*
- The RCC panel shall be able to maintain compatibility between surfaces of the shield.
- *The probability of losing the capability to compatibility between surfaces of the shield shall be less than $6.1*10^{-2}$ failure/FH.*
- The RCC panel shall be able to maintain structural shape of the shield.
- *The probability of losing the capability to structural shape of the shield shall be less than $6.1*10^{-2}$ failure/FH.*

External heater

- The External heater shall be able to properly reject heat loads.
- *The probability of losing the capability to reject heat loads shall be less than $6.1*10^{-2}$ failure/FH.*

Wall cavity

- The wall cavity shall be able to maintain proper ventilation inside the walls.
- *The probability of losing the capability to maintain proper ventilation inside the convection walls shall be less than $2.4*10^{-2}$ failure/FH.*

Wall panel

- The wall panel shall be able to maintain structural shape of the convection walls.
- *The probability of losing the capability to maintain structural shape of the convection walls shall be less than $2.4*10^{-2}$ failure/FH.*

Heater

- The Heater shall be able to maintain structural shape in engines passive cooling.
- *The probability of losing the capability to maintain structural shape in engines passive cooling shall be less than $3.8*10^{-3}$ failure/FH.*
- The Heater shall be able to maintain structural shape in systems passive cooling.

- *The probability of losing the capability to maintain structural shape in systems passive cooling shall be less than $4.5*10^{-3}$ failure/FH.*
- The Heater shall be able to maintain structural shape in primary structure passive cooling.
- *The probability of losing the capability to maintain structural shape in primary structure passive cooling shall be less than $4.5*10^{-3}$ failure/FH.*
- The Heater shall be able to maintain structural shape passive cooling.
- *The probability of losing the capability to maintain structural shape in passive cooling shall be less than $3.8*10^{-3}$ failure/FH.*
- The Heater shall be able to bear extreme thermal loads from the internal structure.
- *The probability of losing the capability to bear extreme thermal loads from the internal structure shall be less than $2.4*10^{-2}$ failure/FH.*
- The Heater shall be able to properly transfer heat in systems passive cooling.
- *The probability of losing the capability to transfer heat in systems passive cooling shall be less than $4.5*10^{-3}$ failure/FH.*
- The Heater shall be able to properly transfer heat in engines passive cooling.
- *The probability of losing the capability to transfer heat in engines passive cooling shall be less than $3.8*10^{-3}$ failure/FH.*
- The Heater shall be able to properly transfer heat in primary structure passive cooling.
- *The probability of losing the capability to transfer heat in primary structure passive cooling shall be less than $4.5*10^{-3}$ failure/FH.*
- The Heater shall be able to properly transfer heat in passive cooling.
- *The probability of losing the capability to transfer heat in passive cooling shall be less than $3.8*10^{-3}$ failure/FH.*

Heat exchanger

- The Heat exchanger of the passive cooling system shall be able to maintain compatibility between surfaces of engines passive cooling.
- *The probability of losing the capability to maintain compatibility between surfaces of engines passive cooling shall be less than $3.8*10^{-3}$ failure/FH.*
- The Heat exchanger of the passive cooling system shall be able to maintain compatibility between surfaces of systems passive cooling.
- *The probability of losing the capability to maintain compatibility between surfaces of systems passive cooling shall be less than $3.8*10^{-3}$ failure/FH.*
- The Heat exchanger of the passive cooling system shall be able to maintain compatibility between surfaces of primary structure passive cooling.
- *The probability of losing the capability to maintain compatibility between surfaces of primary structure passive cooling shall be less than $4.5*10^{-3}$ failure/FH.*
- The Heat exchanger of the passive cooling system shall be able to maintain compatibility between surfaces of passive cooling.
- *The probability of losing the capability to maintain compatibility between surfaces of passive cooling shall be less than $3.8*10^{-3}$ failure/FH.*
- The Heat exchanger of the passive cooling system shall be able to reject heat loads in engines passive cooling.
- *The probability of losing the capability to reject heat loads in engines passive cooling shall be less than $3.8*10^{-3}$ failure/FH.*
- The Heat exchanger of the passive cooling system shall be able to reject heat loads in systems passive cooling.

- *The probability of losing the capability to reject heat loads in systems passive cooling shall be less than $4.5*10^{-3}$ failure/FH.*
- The Heat exchanger of the passive cooling system shall be able to reject heat loads in primary structure passive cooling.
- *The probability of losing the capability to reject heat loads in primary structure passive cooling shall be less than $4.5*10^{-3}$ failure/FH*
- The Heat exchanger of the passive cooling system shall be able to reject heat loads in passive cooling.
- *The probability of losing the capability to reject heat loads in passive cooling shall be less than $3.8*10^{-3}$ failure/FH.*

Appendix A

This Appendix contains the relevant steps regarding the tools useful to perform the Reliability and Safety Assessment included in this report.

The Reliability Engineering supports the design of a project which has potential failure modes that can affect the safety of the final product itself. It comprises different tool-sets, which are presented in detail in the following paragraphs:

- FHA (Fault/Functional Hazard Analysis/Assessment);
- FTA (Fault Tree Analysis);
- FMEA/FMECA (Failure Mode, Effects and – Criticality - Analysis).

The previously cited tools are applied and carried out one after the other in a iterative and recursive methodology in order to ensure that safety and operational requirements can be fully realized and verified.

Each iteration starts with the Functional Analysis at the proper level of study and then, an hazards list, formalized in the FHA, could be derived. At the end of the FHA is the turn to perform the FTA and finally the FMECA.

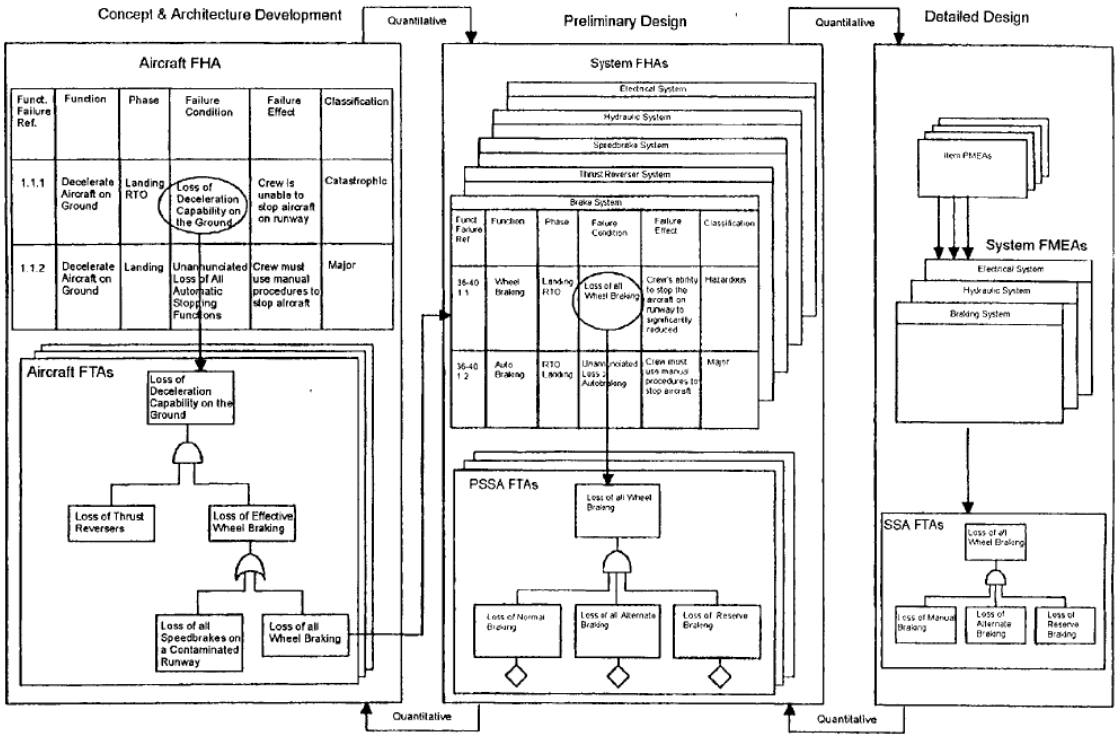


Figure A.1 Relationship among tools [30].

The Functional Hazard Assessment/Analysis

The Fault Hazard Analysis (FHA), also referred as the Functional Hazard Analysis/Assessment, follows an inductive reasoning approach to problem solving, in which the analysis concentrates firstly on the specific and then moves toward the general. The FHA is a qualitative analysis similar to an expansion of Failure Mode and Effect Analysis (FMEA, see the following pages) and it takes in consideration only the failure conditions that cause safety-related events. The tool is useful to derive lower Safety Requirements as well and subsequently, constraints or maintenance actions to ensure that the effects and the risk of the failures are limited [30].

The FHA is the first step in a Safety Assessment process and is carried out during the whole product design, starting from a description of product functionalities for each mission phase. Then, following allocation of functions to the systems and subsystems, which have to perform them, FHA is carried out again for each lower level of study, such as subsystem level, until components level, in other words, up to the design is satisfied. The primary aim of conducting a FHA is to investigate and to identify hazardous function failure conditions. The method to apply FHA is relatively similar to an initial brainstorming generating high level requirements. From a suitable knowledge of the system or subsystem (drawings, schematics and block diagrams to understand integration and interaction among them), it is necessary to select a list of top-level functions and their behaviour, in relation with requirements and initial design decisions, and then, to consider potential failures during operational. Next, the effects of the hazards to the system (or subsystems) and its operation must be determined and categorized (catastrophic, severe, major, minor, no safety effect).

Top-Level Failure Condition Severity Classification	Associated Top-Level Function FDAL Assignment
Catastrophic	A
Hazardous/Severe Major	B
Major	C
Minor	D
No Safety Effect	E

Figure A.2 Failure Classification [31].

The classification can be accomplished by using previous design experience or flight test and simulations, consulting with flight crew or reviewing regulatory guidance material and data. It is important to list all conditions that can influence and increase the probability of failures, such as periods of operation, emergency/abnormal conditions, mission phases, stress, personnel actions and interactions.

Function	Phase	Failure Condition	Failure Effect	Risk

Table A.1 Example of basic FHA tabulation [1].

The result is a table of functions, their potential failures and effects to the operation of the systems in relation with the assigned qualitative design requirements: as seen above, it is also important to specify particular conditions, that can influence the occurrence of failures, and the phase as well, in which the analysis is focused. When the list of failure conditions and their classifications has been produced, it may be worth comparing the list with lists from other similar projects as an extra aid to guard against overlooking some of the minor hazardous conditions. Furthermore, it may also be useful creating and maintaining a generic list, as a checklist, to be used during the review process of the FHA.

The final step provides a list of corrective actions that can mitigate the risk: in this context, the FHA is an excellent system safety engineering method, which can be used to ensure system operational safety and integrity. The results of the FHA process should be tracked, so there are traceable steps taken into account to develop the FHA document.

Hazard ID #	Life-Cycle Phase	Activity	State/ Mode	Function	Functional Failure	Hazard Description	System Item(s)	Causal Factor Description	Mishap	Effect(s)
Identifier used to reference specific hazard	*The life-cycle phase for which the risk and risk assessment apply*	*The actions performed within a life-cycle phase*	*The state and/or mode of the system for the hazard of concern*	*One of the system functions (implicit, implied, or derived)*	*The detailed description for the specific failure mode of the function analyzed*	*The detailed description of the conditions under which the hazardous energy may be release in an uncontrolled or inadvertent way*	*A functional or physical portion of a system designed, used, or integrated to accomplish one aspect of the system task or mission*	*The detailed description of the failures, conditions, or events that contribute either directly or indirectly to the existence of a hazard*	*The event or series of events where hazardous energy release could negatively effect equipment, personnel, or environment; accident*	*The results of the mishap to include injury or death, damage to equipment and property, or damage to the environment*

Existing Mitigations	Software Control Category	Initial MRI	Software Criticality Index	Target MRI	Causal Factor Risk Level	Recommended Mitigations	Comments	Follow-On Actions
Controls that are already planned or existing to mitigate the risk	*The degree of autonomy, command and control authority, and redundant fault tolerance of a software function in context with its system behavior*	*The first assessment of the potential risk of an identified hazard to establish a fixed baseline for the hazard. This may have come from the PHA*	*The level of analysis rigor required for risk assessment defined by the software control category and the mishap severity of the MRI*	*The projected risk the PM plans to achieve by implementing one or more of the designated recommended mitigations. This field should remain blank if no recommended mitigations are identified*	*The projected mishap risk level associated with the existence of the specific causal factor and its potential to realize the hazard and mishap*	*Controls that would reduce the mishap risk potential. The goal should always be to eliminate the hazard if possible. When a hazard cannot be eliminated, the associated risk should be reduced to the lowest acceptable level by applying the system safety design order of precedence*	*Any important information and relevant information not captured elsewhere*	*Assigned or designated actions necessary to identify or better understand or characterize risk (e.g. perform FTA, perform software code analysis)*

Table A.2 Typical Worksheet of FHA [32].

Fault Tree Analysis

The Fault Tree Analysis is the most effective method for safety analysis and it consists of a detailed logic diagram, known as Fault Tree, illustrating the basic combinations of intermediate failures, that can cause a system risky event, so-called Top Event. Resolving the Fault Tree model with a deductive backward method, it can be clear which are the causes of the undesired top event.

The Fault Tree is the logical model of the relationship through the failure events of different levels, and it consists of top event, intermediate events and basic events logically linked by logical gates.

Each event is derived by the identification of the hazards of the previous event, following a deductive approach. The result is a graphical model that displays the combinations of possible failures, malfunctions and errors that can occur. Reasoning backwards from the top event through intermediate events (subsystem failures) and basic events (components failures) it is possible to calculate the combination of failures that causes the top one, evaluated in the FHA.

The main steps are:

- To define the undesired top event;
- To define the boundary of the system and the intermediate events;
- To draw the appropriate symbols;
- To define the basic events;
- To treat each intermediate events as a top event;
- To draw the appropriate gates;
- To define the initial state of the system.

It is noticeable to remember that, a correct Fault Tree is developed only if the events are well-known and studied. To evaluate the Fault Tree, it is necessary to derive the equivalent logic equations: each gate event is expressed as a logic input events that, by substitution, it consists in a combination of basic events. The result is a mathematical expression: the smallest combination of basic events causing the top event is called Minimal Cut Set, which links the top event to the basic ones.

The Fault Tree is characterized by a specific "language". The events are shown as symbols like rectangle, triangle, circle and diamond:

- Rectangle represents intermediate events (combination of lower events);
- Circle represents basic events (no further expansions);
- Triangle represents a transfer gate;
- Diamond represents undeveloped events.

The top event is shown as parallelogram.

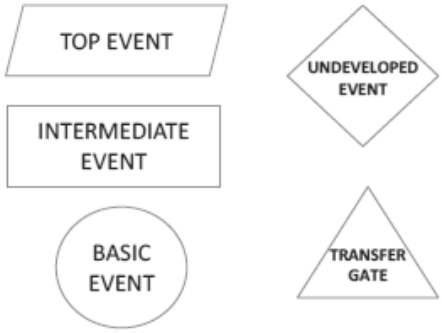


Figure A.3 Logical Gate to develop a Fault Tree [33].

To "solve" a Fault Tree it must be apply the Boolean Relationships:

- $A \cdot (B + C) = A \cdot B + A \cdot C \quad distributive\ law$
- $A + A = A \qquad identity\ union\ law$
- $A + A \cdot B = A \qquad subset\ absorption\ law$
- $A \cdot A = A \qquad identity\ intersection\ law$
- $(A + B)' = A' \cdot B' \quad union\ complementation\ law$
- $(A \cdot B)' = A' + B' \quad intersection\ complementation\ law$

Events are linked together by AND / OR gates, called Boolean operators: the first one is used to identify that an event happens only if both lower events happen, the latter means that the failure happens only if one of the lower events happen. When an AND gate is applied, that means the likelihood of the upper event is the multiplication of the probability of the lower events, on the other side, if there is a OR gate, the upper likelihood is the sum of the probabilities of the lower events.

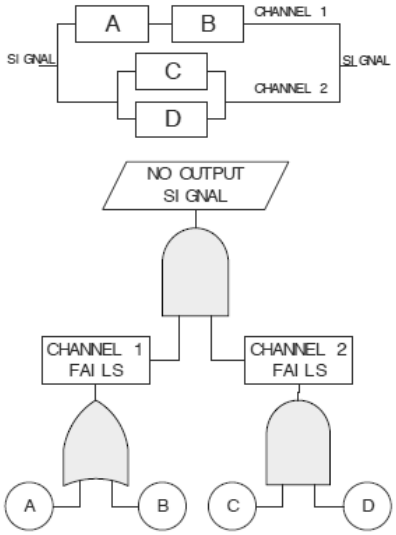


Figure A.4 Example of Fault Tree [33].

To performed a quantitative analysis, probability of occurrence of each event must be assigned. The resulting equation is a basis to calculate and evaluate the probability of the undesired top level event. If the requirements are not met, corrective actions must be implemented [33].

The development of FTA is in compliancy with the regulations, such as ECSS-Q-ST-40-12C.

Failure Mode, Effects and (Criticality) Analysis

The Failure Mode, Effects and (Criticality) Analysis (FMEA/FMECA) is a reliability and safety evaluation tool, which examines the potential failure modes within a process or product, in order to determine the effects on equipments and on system performances on the proper level of design. It is a inductive approach considering each single elementary failure and assessing its effects up to the product or process under examination. A FMEA is used more generally to support the Safety Assessment process by providing failure rates to quantify the basic events of the FTA. It may also be used to support verification of the FTA through a comparison of the FMEA failure modes with the basic events of the Fault Tree.

The FMEA/FMECA is developed throughout the project life as an integral part of the design process in order to define, verify and test the design of the product. It should be useful to integrate this method at the early beginning of the conceptual phases and design stages, in order to reflect, in the final part, the mission criteria, requirements and performance data.

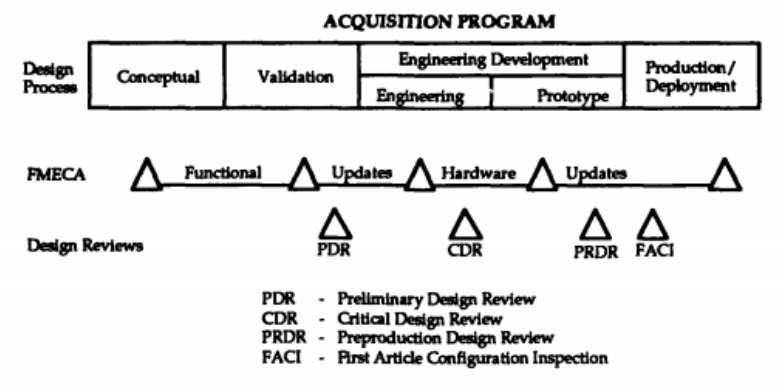


Figure A.5 Design Review Program of FMEA/FMECA [34].

The FMEA/FMECA is an iterative process: gradually, it reflects the additional details of the project, designing and redesigning the specific sectors in order to drive and lead into corrective action implementation and gain a suitable result.

The FMEA/FMECA consists of these following steps:

- To identify each component in the system (the proper level of decomposition depends on the stage of the programme);
- To determine the potential effects of failure modes for the component;
- To determine all causes for each failure mode;
- To determine the worst-case effect of each failure mode on the component and on each level corresponding to each mission phase;
- To determine the severity of each failure mode on each mission phase (only FMECA);
- To determine the criticality of each failure mode on each mission phase (only FMECA).

Its final aspect consists in a tabulation of equipments or components and their associated single failure modes and critical points, consequences and safety modes: looking at each component, it is possible to derive and identify the risk, in order to take corrective actions and to contain the dangerous effects [33].

Analysis technique

Applying FMEA/FMECA, there are two most effective methodologies for reliability analysis:

- The functional approach;
- The hardware approach.

The hardware approach

The hardware approach is a kind of list of individual hardware items at the bottom level, then the analysis continues upwards through the higher level of the system. Before beginning the FMEA analysis, it is necessary to have clear the operation and the features about the system, to have accomplished the Reliability Block Diagram and identify each part under analysis of the scheme. Next level is to lead the potential effects of the failure into the higher levels in order to produce the final outcomes. The final outputs include a list of hazards to be eliminated or reduced, a list of critical failures and a list of undetectable failures.

The functional approach

On the other side, the functional approach consists of analysing the functions, where it is not possible to identify the associated hardware: this justifies the employment of this technique in the early design process. Within the Functional Analysis is also necessary to derive the system definition and functional breakdown and other representations such as the block diagram of the system. To accomplish a functional FMEA is essential to define and identify each system function and its associated failure modes for each functional output. The failure mode and effects analysis is completed by determining the potential failure modes and failure causes of each system function. The failure mode probability is a value (the percentage of time expressed in decimal format) that the function will fail in a specific mode.
The modal failure rate is defined as the functional failure rate (*in failures/1000hours*) multiplied by the probability that the failure event will occur. The effects of each functional failure mode are then determined by propagating the effect of the failure through each higher level of the system [33]. The outputs derived from the functional FMEA must contain a list of hazard risks to be eliminated or diminished, a list of critical single point failures and list of undetectable failures.

FMEA and FMECA have been up to now shown as similar concept but this is not exactly coherent. The difference between FMEA and FMECA is that, the latter is an approach more suited for hazard control and with numerical aspects.

It is used when are available failure rates data to calculate a sort of index/figure of merit as a combination of severity and probability of occurrence and, at the end, identify a criticality classification.

Failure Modes and Effects Analysis (FMEA)											
Product:			**System:**				**Subsystem:**			**Equipment:**	
Ident. number	Item/ block	Function	Failure mode	Failure cause	Mission phase/ Op. mode	Failure effects a. Local effects b. End effects	Severity classification	Failure detection method/ observable symptoms	Compensating provisions	Recommendations	Remarks

Table A.3 Example of FMEA [33].

Failure Modes Effects and Criticality Analysis (FMECA)													
Product:			**System:**				**Subsystem:**			**Equipment:**			
Ident. number	Item/ block	Function	Failure mode	Failure cause	Mission phase/ Op. mode	Failure effects a. Local effects b. End effects	Severity classification	Failure detection method/ observable symptoms	Compensating provisions	Severity Number SN	Probability and PN	Criticality Number CN	Recommendations	Remarks

Table A.4 Example of FMECA [33].

In Table A.3 and Table A.4 the difference between the two methodologies is shown: in the FMECA there are the specific columns to collect the cited numerical data.

The FMEA/FMECA is developed according to regulations, such as ECSS-Q-ST-30-02C and MIL-ST-1629.

References

[1] Fusaro R., Ferretto D., Viola N. "*MBSE approach to support and formalize Mission Alternatives generation and selection processes for hypersonic and suborbital transportation systems*" ISSE 2017 - 2017 International Symposium on Systems Engineering, 2017.

[2] FAA System Safety Handbook: *https://www.faa.gov/regulations_policies/handbooks_manuals/aviation/risk_management/ss_handbook/media/Chap8_1200.pdf*

[3] Fusaro R., "*Preliminary Reliability and Safety Assessment Methodology for Trans--Atmospheric Transportation Systems",* Torino, 2016.

[4] Fusaro R., Ferretto D., Viola N., Fioriti M., Boggero L., Aleina S.C. *"Methodology for the Safety and Reliability assessment of hypersonic transportation systems in conceptual design activities".*

[5] NASA, *"Systems Engineering Handbook"*, NASA Headquarters, Washington, D.C., 2007.

[6] Perry S., Holt J., *"SysML for Systems Engineering"*, ESA-ESTEC, The Institution of Engineering and Technology, London, 2008.

[7] Viola N., Corpino S., Fioriti M., Stesina F., *"Functional Analysis in Systems Engineering: Methodology and Applications,"* Boris Cogan, Torino, 2012.

[8] CORDIS, Community Research and Development Information Service: *http://cordis.europa.eu/result/rcn/46660_en.html*

[9] Steelant J., Langener T., *"The Lapcat-MR2 hypersonic cruiser concept"*, ESA-ESTEC, Noordwijk, 2014.

[10] Steelant J., Erb S., Langener T., *"Trajectory Simulation and Optimization of the LAPCAT-MR2 Hypersonic Cruiser Concept"*, ESA-ESTEC, Noordwijk, 2014.

[11] FAA, System Design and Analysis, "*AC 25.1309-1A",* Northwest Mountain Region - Transport Airplane Directorate, 1988.

[12] Langener T., Steelant J., Karl S., Hannemann K., "*Design and Optimization of a Small Scale M=8 Scramjet Propulsion System*", Göttingen, 2012.

[13] Meerts C., Steelant J., *"Air Intake Design for the Acceleration Propulsion Unit of the LAPCAT-MR2 Hypersonic Aircraft"*, ESA-ESTEC, Noordwijk, 2013.

[14] Fernandez Villace V., Paniagua G., Steelant J., *"Installed performance evaluation of an air turbo-rocket expander engine"*, ESA-ESTEC, Noodwijk, 2014.

[15] Balland S., Fernandez Villace V., Steelant J., *"Thermal and Energy Management for Hypersonic Cruise Vehicles – Cycle Analysis"*, 20th AIAA, Glasgow, 2015.

[16] Fernandez Villace V., Steelant J., *"A Generic Thermodynamic Assessment of Reusable High-Speed Vehicles"*, ESA-ESTEC, Noordwijk, 2016.

[17] Chiesa S., *"Affidabilità, sicurezza e manutenzione nel progetto dei sistemi"*, Torino, 2010.

[18] Vitali R., Lutomski M. G., *"Derivation of Failure Rates and Probability of Failures for the International Space Station Probabilistic Risk Assessment study"*.

[19] Cadwallader L., *"Reliability and Maintainability Data for Liquid Metal Cooling Systems"*, 26th Symposium on Fusion Engineering, 2015.

[20] Technical document issued by the International Atomic Energy Agency (IAEA), "*Component Reliability data for use in probabilistic Safety Assessment"*, Vienna, 1988.

[21] Report of a Technical Committee Meeting organized by the IAEA, *"Evaluation of Reliability Data Sources"*, Vienna, 1988.

[22] Cadwallader L., Reliability Estimates for Selected Sensors in Fusion Applications, Idaho National Engineering Laboratory, 1996:

http://www.iaea.org/inis/collection/NCLCollectionStore/_Public/28/044/28044377.pdf

[23] Department of Defense, Military Handbook MIL-HDBK-217F, "*Reliability Prediction of Electronic Equipment",* Carderock, 1991.

[24] Naval Surface Warfare Center, Systems Department Research and Development Report, "*Handbook of Reliability Prediction Procedures for Mechanical Equipment"*, 1992.

[25] Pilot S., Naikan V. N. A., "*Reliability analysis of temperature sensor system",* International Journal of Reliability, Quality and Safety Engineering, 2013.

[26] Sintef, *"Reliability Data for Safety Instrumented systems"*, Trondheim, 2010.

[27] Marè J. C., *"Aerospace Actuators: Needs, Reliability and Hydraulic Power Solutions",* Chapter 2, Wiley, 2016.

[28] Department of Defense, Military Handbook, MIL-HDBK-251, "*Reliability/Design, Thermal Applications*", Washington D.C., 1978.

[29] Denson W., Chandler G., Crowell W., Wanner R., "*Non-electronic parts Reliability Data"*, Reliability Analysis Center Rome NY, 1991.

[30] SAE Aerospace, ARP4761, "*Guidelines and Methods for conducting the Safety Assessment process on civil airborne systems and equipment",* 1996.

[31] SAE Aerospace, ARP4754, "*Guidelines for Development of Civil Aircraft and Systems",* 2010.

[32] Scharl A., Stottlar K., Kady R., *"Functional Hazard Analysis, Methodology Tutorial"*, International System Safety Training Symposium, Missouri, 2014.

[33] Corpino S., "Sistemi Aerospaziali", Politecnico di Torino, Torino, A.A. 2015/2016.

[34] Reliability Analysis Center, *"Failure Mode, Effects, and Criticality Analysis",* Rome NY, 1993.

Ringraziamenti

Il primo importante ringraziamento va alla Professoressa Nicole Viola per avermi dato la possibilità di concludere il mio percorso approfondendo un tema interessante e stimolante per me.

Un ringraziamento speciale va all'Ing. Roberta Fusaro e all'Ing. Davide Ferretto per l'attenzione, la disponibilità, la pazienza, i suggerimenti, i consigli e il supporto che mi hanno sempre dimostrato lungo tutto il mio lavoro.

Ringrazio infinitamente i miei genitori, Andrea e Oriana, per aver reso possibile questo cammino, per non avermi mai fatto mancare nulla, per aver supportato ogni mia scelta e per avermi sostenuta *sempre*: è grazie a loro se sono questa persona oggi.

Ringrazio Alex per avermi fatto pensare agli aspetti positivi di ogni cosa, soprattutto nelle difficoltà, e per avermi sopportata quando son stata insopportabile, restando *sempre* al mio fianco.

Ringrazio Flavia per avermi tenuta per mano giorno dopo giorno, un po' come una *mamma*, ed essersi dimostrata pronta a reagire *in ogni momento* qualcosa andasse storto.

Ringrazio infinitamente i miei colleghi di avventura Andrea C., Andrea F., Angelo, Eleonora, Filippo, Giulia, Luca, Pietro, Umberto per il supporto morale che ci siamo dati.

Un ringraziamento particolare va a Francesca, Luca e Mattia perché ciascuno di loro è stato *indispensabile* a proprio modo.

Ringrazio Alessandro C., Alessandro M., Andrea e Irene per le risate che non mi hanno *mai* fatto mancare e che son state *sempre* spontanee e sincere.

Un ringraziamento di cuore va i miei amici di sempre, Alice, Cristina, Edoardo, Eugenia, Francesco, Sara, Sara, Silvia, Marta, Sofia per avermi *sempre* appoggiata anche da lontano.

Un ultimo fondamentale ringraziamento, non meno importante, va a tutta la mia famiglia, ai nonni Armando e Edda, alla nonna Maria Rosa, ai miei zii Alessandra, Daniele, Luca e Roberta ed infine alla mia cugi Silvia.