POLITECNICO DI TORINO

Corso di Laurea Magistrale in Ingegneria Aerospaziale

Tesi di Laurea Magistrale

Model Based Approach to Safety Assessment of an Environmental Control System for an Unmanned Aerial Vehicle

Relatore:
Prof. Paolo Maggiore
Correlatori:
Prof.ssa Nicole Viola
Ing. Marco Fioriti

Candidato:
Dario Coluzzi

Tutor Leonardo Aircraft Division:
Dott.ssa Elena Valfrè
Ing. Gianni Mancuso
Ing. Marco Borio
Ing. Alessandro d'Errico

Anno Accademico 2018/2019

Ringraziamenti

Desidero innanzitutto ringraziare il Prof. Paolo Maggiore, la Prof.ssa Nicole Viola e l'Ing. Marco Fioriti per avermi permesso di affrontare le interessanti tematiche trattate e per avermi fornito, con gentilezza, l'indispensabile supporto accademico.

Ringrazio inoltre la Dott.sa Elena Valfrè per avermi seguito quotidianamente, con estrema disponibilità e dedizione durante tutto lo svolgimento della tesi. La ringrazio inoltre, assieme a tutto l'ufficio di Engineering System & Configuration Management, per la gentilezza e la cordialità con cui sono stato accolto nei sei mesi passati in azienda. Ringrazio infine l'Ing. Bruno Di Giandomenico, l'Ing. Gianni Mancuso, l'Ing. Marco Borio e l'Ing. Alessandro d'Errico per tutto il tempo che mi hanno dedicato, affiancandomi con continuità nella realizzazione della tesi.

Ringrazio gli amici e tutte le persone che mi vogliono bene e che mi sono state vicino negli ultimi cinque anni per il loro fondamentale supporto.

Un ringraziamento speciale va infine alla mia famiglia, senza la quale non sarei quello che sono.

Abstract

This thesis is dedicated to the application of a model-based approach to the design of the Environmental Control System (ECS) for an Unmanned Air Vehicle (UAV). In particular, the thesis focuses on the safety assessment of the system at issue.

Chapter 1 describes the rationale behind the adopted method and the selected case study. The following chapter is dedicated to the functional analysis: beginning with system requirements, the logical architecture and the functional interconnections are defined according to the methodologies of Model Based System Engineering. Moving to Chapter 3, it is dedicated to the definition of the physical architecture of two different possible solutions: vapour cycle cooling system and air cycle system. A performance analysis tool is used to size all the components making up the system and to verify its correct functioning in different flight conditions.

Chapter 4 is finally aimed to safety assessment. Specifically, Functional Hazard Assessment (FHA), Failure Modes Effect and Criticality Analyses (FMECA) and Fault Tree Analyses (FTA) are carried out relying upon the functional and performance models realized in the previous chapters. The conducted analyses also allowed the allocation of Development Assurance Levels (DAL) and the definition of redundancies.

The last chapter is dedicated to the conduction of a Computational Fluid Dynamics (CFD) analysis aimed the verification of the proper avionic cooling in the event of a failure of the ECS.

Table of Contents

List of Figures

List of Tables

List of Abbreviation and Acronyms

ACM	Air Cycle Machine
ASA	Aircraft Safety Assessment
CAT	Catastrophic (Severity classification)
CAU	Cold Air Unit
CCA	Common Cause Analysis
CFD	Computational Fluid Dynamics
CMA	Common Mode Analysis
CU	Control Unit
DAL	Development Assurance Level
ECS	Environmental Control System
ED	Erroneous Detected
EU	Erroneous Undetected
FDAL	Functional Development Assurance Level
FH	Flight Hours
FHA	Functional Hazard Assessment
FM	Failure Mode
FMEA	Failure Modes Effect Analysis
FMECA	Failure Modes Effect and Criticality Analysis
FMES	Failure Modes and Effect Summary
FR	Failure Rate
FTA	Fault Tree Analysis
HAZ	Hazardous (Severity classification)
HOTOL	Horizontal Take Off and Landing
IAD	Inadvertent Activation Detected
IAU	Inadvertent Activation Undetected
IDAL	Item Development Assurance Level
LD	Loss Detected
LU	Loss Undetected
MAJ	Major (Severity classification)
MBSE	Model-Based System Engineering
MIN	Minor (Severity classification)
MTBF	Mean Time Between Failures

NRV	Non-Return Valve
NSE	No Safety Effect (Severity classification)
OFD	Other Failure Detected
OFU	Other Failure Undetected
PASA	Preliminary Aircraft Safety Assessment
PRA	Particular Risk Analysis
PRSOV	Pressure Reducing – Shut Off Valve
PSSA	Preliminary System Safety Assessment
SE	System Engineering
SOV	Shut Off Valve
SSA	System Safety Assessment
TCV	Thermal Control Valve
UAS	Unmanned Aircraft System
UAV	Unmanned Air Vehicle
UCAV	Unmanned Combat Aerial Vehicle
VCCS	Vapour Cycle Cooling System
ZSA	Zonal Safety Analysis

1 Introduction

1.1 Purpose

The aim of this thesis is to study the application of a model-based approach to the safety assessment process. In particular, the selected case study regards the Environmental Control System (ECS) of an Unmanned Air Vehicle (UAV), which basically consist of the cooling system of the electronics installed onboard the aircraft. More specifically, two different ECS architecture will be studied: air cycle system and vapour cycle system.

The design of an aircraft encloses the definition of its aerodynamic shape, its structure, its propulsive strategy, its flight dynamic performance, its handling qualities and its highly integrated sub-systems. Each of those needs to explicate its own function with an acceptable weight and electrical power requirement. Another series of fundamental requirements derive from the safety assessment, depending on the category of the aircraft.

The purpose of this thesis is indeed to follow some of the processes which concurs to the design of a specific sub-system from functional analysis to safety assessment, supported by performance analysis.

This thesis has been realized in collaboration with Leonardo – Aircraft Division. In particular, the activities have been carried out in the "Engineering System & Configuration Management", "Aircraft Systems" and "System Safety" departments of the engineering organization.

It is fundamental to underline how the technical solutions adopted in this thesis are purely academical and do not derive from any actual project of Leonardo – Aircraft Division. Moreover, all of the data used in the different numerical analyses are fictional and representative of a generic hypothetical and unspecified aircraft. The data have indeed been hypothesized as a mean to test the proposed processes. As has already been mentioned, the main topic of the thesis, rather than the symbolic numerical results, is indeed the model-based process adopted for functional, performance and safety analyses.

1.2 Method

The adopted process relies upon the usage of a series of software aimed to the generation of a functional model and of a performance model, whose outputs shall be linked to the first one.

This peculiar methodology is aimed to the formalization of system development and can be applied to behavioural analysis, system architecture, requirement traceability, performance analysis, simulation and testing. It represents an innovation and an evolution of the document-based approach which does present some difficulties concerning the evaluation and the management of the relationships between requirements. Moreover, Model-Based System Engineering allows a simpler modification of requirements in case that an evolution or a variant of a project is needed. The model represents, indeed, a description of a system and, being realized accordingly to a precise language, it helps to better visualize the system, its complexities and its behaviour. All of these peculiarities, associated with rigor and formalism,

result in productivity improvement and in a lower risk of the project at issue. Moreover, Model-Based System Engineering allows an early detection of design defects.

Dealing with the case study at issue, the safety assessment process interfaces itself with the development process as shown in the following diagram, derived from SAE ARP4754A, "*Guidelines for Development of Civil Aircraft and Systems*":

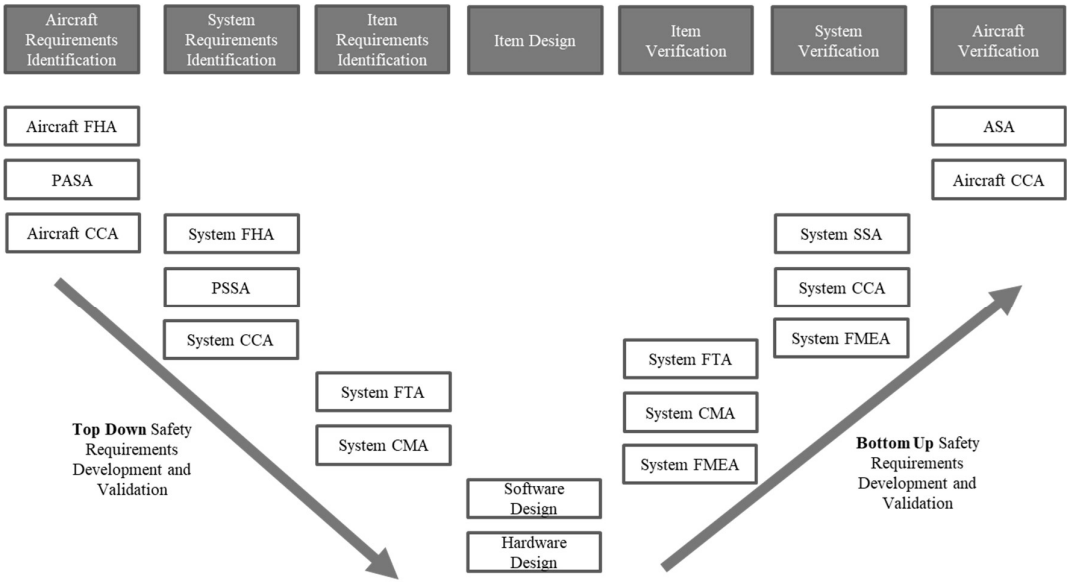

Figure 1.1: Safety Assessment and Development Process (ref. [7])

The diagram perfectly resembles the characteristics of the V-model, typically referred to System Engineering. System Engineering consist of an interdisciplinary logic aimed to the realization of a safe and balanced design which, above all, respects the requirements that have been established. The central core of system engineering is then the management of the conflicting constraints deriving from the different disciplines which concur in an aerospace project, and it is focused on systems integration. This process extends its limits throughout the entire lifecycle of the product and, specifically for the development process, it goes from requirements identification to their verification. This is made beginning from the higher level, i.e. aircraft level, and moving to lower levels, i.e. systems and items, following a top-down approach. The process continues in a bottom-up optic which paves the way to items, systems and aircraft design verification.

The process that has been followed in this thesis is shown in the diagram reported in Figure 1.2 and begins with the system requirements identification. These requirements, deriving from preliminary design, may derive from a requirements management tool and will be deeply described in chapter 2, dedicated to the functional analysis and to requirements analysis.

The first step is then the generation of a functional model via IBM Rational Rhapsody ® beginning with the logical architecture definition of the system at issue. It consists of determining those logical blocks which explicate a specific function, and it is supported by the system functional analysis which concurs to their definition. Subsequently, coherently with the model-based approach, the Functional Hazard Assessment has been carried out exploiting the

generated functional model, fact that provides several advantages regarding completeness and objectivity, as will be explained in Chapter 4. The FHA has also been carried out following the "traditional" document-based approach in order to determine, by direct comparison, those abovementioned advantages. The functional model has then been used to the assignment of FDAL thanks to a semi-automated procedure.

In parallel with this process, a performance analysis has been carried out. The functional analysis of the system, indeed, paved the way to the physical architecture definition of the ECS for both Air Cycle and Vapour Cycle cooling system. Subsequently, the sizing of the components has been carried out in Siemens Simcenter Amesim ®. Moreover, a Computational Fluid Dynamics analysis has been conducted in Siemens STAR CCM+ ® with the aim of validating the safety requirements regarding the back-up cooling system as will be deeply described in the chapters 4 and 5.

Besides from the performance analysis, the physical architectures have been linked to the functional model in order to allow IDAL assignment. Furthermore, those represent the basis for the FMECA/FMES and for the Fault Tree Analysis.

Once that the FTAs have demonstrated the actual satisfaction of the safety requirements, determined thanks to the FHA, the failure rates of each component, and the low-level physical architecture, can be linked to the original functional model (see section 4.4).

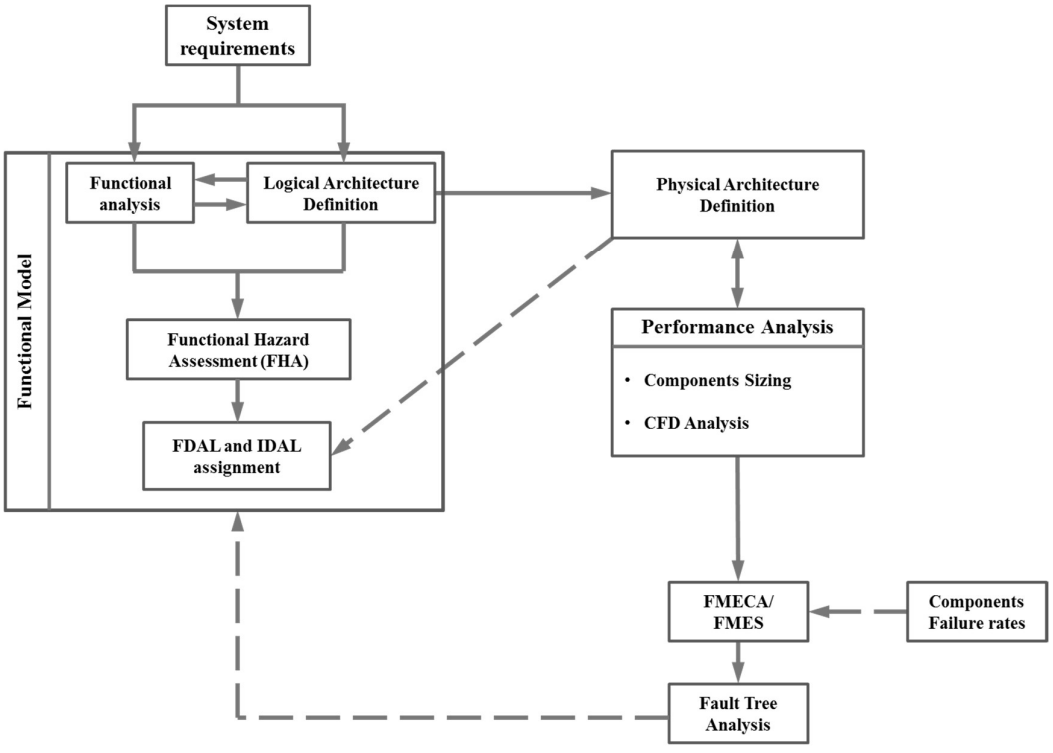

Figure 1.2: Adopted Process

The process here described truly reflects the multidisciplinarity of System Engineering. The followed method underlines indeed the continuous interactions between all the disciplines which concurs to the design of a complex product, such as an aircraft sub-system. Among all of those disciplines, this thesis is focused on functional analysis, performance analysis and safety assessment. As an example, another important process of System Engineering regards the cost estimate of the system at issue. This thesis has indeed been realized in parallel with a specular one[1] that, beginning with the functional analysis of the same case study (i.e. the ECS of an UAV) is aimed to the conduction of a cost estimate of the subsystem.

To conclude, it is possible to notice in Figure 1.3, courtesy of Leonardo Aircraft Division, how the design disciplines described in the thesis regard conceptual and preliminary design. The logical and the physical architecture that will be determined are indeed preliminary architectures.

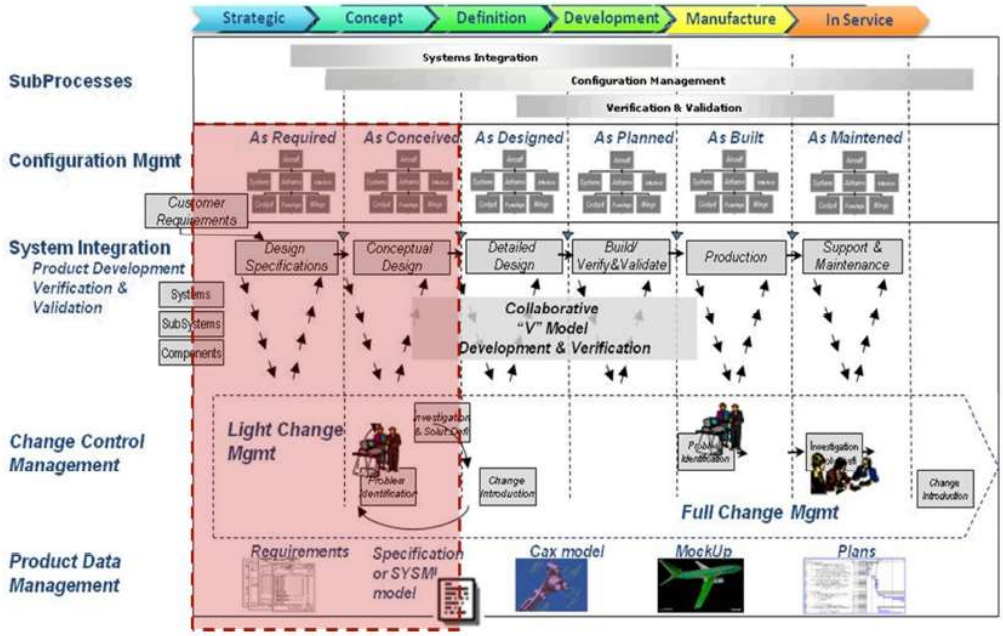

Figure 1.3: Design Process. Courtesy of Leonardo Aircraft Division

1.3 Case study: Environmental Control System for an Unmanned Air Vehicle

1.3.1 Unmanned Air Vehicles (UAV)

An unmanned air vehicle, commonly referred to as UAV, is a component of an Unmanned Aircraft System (UAS). It includes, besides the aircraft itself, a series of other components necessary to allow to the UAV to fully complete its mission. Among these subsystems there are

[1] A. Chierchia, "*Application of System Engineering Processes, Methods and Tools to the ECS System (Environmental Control System for an UAV) and Integration with Parametric Cost Estimates*", Politecnico di Torino, 2019

its payload (typically reconnaissance/surveillance or weapon payloads), one or more control stations, aircraft support and communication subsystems. Based on the autonomy level of the UAV, many functionalities may be performed by the system intelligent computers.

An unmanned aerial vehicle shall be able to communicate with its controller transferring data on its payload acquisition, state information about the aircraft (e.g. state, three-dimensional position, airspeed, attitude and angular velocities) and housekeeping data such as fuel quantity and temperatures of different components. As will be described in the chapter dedicated to the functional analysis of the vehicle at issue, it will be able to perform its built-in tests, whenever asked to, and send the results to the ground control station(s). It will also send alert messages in the event of failure(s) or hazardous conditions. The UAV shall be designed to automatically take corrective actions in case of faults, and, in particularly advanced systems, it may even have onboard decision making and autonomous capabilities exploiting artificial intelligence implementations.

UAS are typically categorized by their performances in term of kilometric range, flight endurance, payload weight capacity and operative cruise altitude. The choice of designing a vehicle belonging to a category rather than to another shall be taken on the basis of the mission that must be completed by the system. In other words, mission profile and payload characteristic, not only in terms of weight but even in terms of other required conditions such as vibration tolerance and operative temperature range, generate the requirements that will lead the overall project of the vehicle. Anyway, the main mentioned categories are:

- HALE: high altitude long endurance. More than 15000 meters of altitude and more than 24 hours of endurance
- MALE: high altitude long endurance. Between 5000 and 15000 meters of altitude and more than 24 hours of endurance.
- TUAV: tactical UAV. Smaller and simpler vehicles with ranges between 100 and 300 kilometres, usually operated by naval forces
- Close-Range UAV. With a maximum range of 100 kilometres, they are typically used by mobile army battle groups.

Although these kinds of aircraft were initially developed for reconnaissance, the actual tendency is to endow them with weapons in order to reduce the reaction time that lies between the discover, through reconnaissance functions, of a target, and an air-strike. The aircraft characterized by those capabilities are known as unmanned combat air vehicle.

The reason why unmanned aircraft do offer a great advantage when compared with manned vehicles lies behind the particular role it is designed to accomplish. These are commonly known as dull, dirty and dangerous (DDD):

- Dull roles: long-endurance surveillance, in both civilian and military application, can be considerably dull for the crew. This is particularly negative since it may lead to a loss of concentration of the crew, fact that may result in a catastrophic event. On the other hand, in case of an unmanned vehicle, the ground operators can alternate in shifting patterns.
- Dirty roles: these tasks usually refer to the monitoring of dangerous environment due to nuclear or chemical contamination. Nevertheless, the aircraft needs to undergo detoxification.

- Dangerous roles: military operation in heavily defended areas. Apart from the fact that the crew will not be in danger, UCAVs are generally smaller than manned fighters or bombers, hence their radar traceability is consistently lower. This result in a safer and more effective military mission. Moreover, in combat scenarios, flight crews in manned aircrafts are subject to a considerable level of stress, due to the threat of attack, fact that may cause lack concentration. Another example of dangerous roles regards power-line inspections and forest fire control.

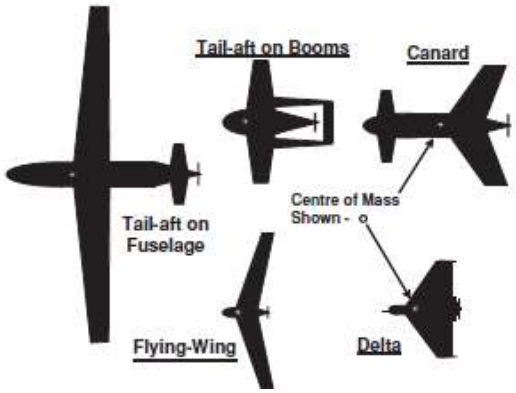

Figure 1.4: HOTOL Aircraft Configurations (ref. [2])

The UAVs are also used for cheaper and safer airborne testing for research and development work in the aeronautical field. Moreover, unmanned vehicles, are smaller, cheaper and cause less environmental distance and pollution with respect of a manned aircraft used for the same roles. In addition to that, UAVs are characterized by lower operating, maintenance, fuel and hangarage cost. Taking all of that into account, the acquisition cost shall be 40-80% of the equivalent manned aircraft cost. The operating cost shall be 60% cheaper.

Focusing on horizontal take-off and landing configurations, the possible solutions are reported in Figure 1.4. They are mainly determined by their means of aerodynamic characteristic, stability and control and payload installation.

1.3.2 Environmental Control System (ECS)

In an unmanned air vehicle, the Environmental Control System (ECS) is dedicated to the provision of those conditions that guarantee the nominal functioning of the avionics of the vehicle. The ECS shall fulfil this task coping with widely different external temperature ranges, varying with altitude, day/night flight and weather conditions. It shall indeed provide air with optimum humidity, a sufficiently low concentration of dust and the suitable temperature to ensure that the electronic equipment remains in the allowable range. All the requirements of the system will be dealt with in the following section. Note that ECS normally provide de-misting, anti-icing and rain dispersal services. However, the case study that will be considered will be mainly focused on the avionic bay air conditioning function.

As will be treated in the section dedicated to the performance analysis, the ECS shall basically be able to function in the two following condition:

- Heating condition: although typically being less demanding than the cooling condition, heating is required in a cold day when the aircraft is flying at subsonic speed and at high altitude due to the progressive decreasing of external temperature with the distance from the ground
- Cooling condition: dealing with subsonic aircrafts, the worst cooling condition happens to be on the ground in a hot day. The principal heat sources are:
    - Kinetic heating: occurs due to the friction present between the skin of the aircraft and the molecules of the air. The temperature of the skin may therefore reach up to 100°C in low altitude and transonic speed flight.
    - Solar heating. This effect has a growing relevance for aircraft endowed with windscreen and canopy. Note that, albeit UAVs do not usually have a windscreen, they may be endowed with a canopy which contains radar, observation payloads and other electronic equipment, and which may be built with a material characterized by non-negligible solar radiation.
    - Avionics heat loads: being typically continuously active, electronic equipment dissipates considerable quantities of heat so that it becomes mandatory to provide the avionic bay with a primary source of air conditioning. The ECS shall be able to protect the components there located throughout the whole flight envelope and in every possible climatic condition in which the aircraft may be required to operate.
    - System heat loads: they include the heat dissipated by the different components installed on the aircraft, such as hydraulic pumps, electrical generators or the ECS itself.

Dealing with the need for avionics conditioning, it generally poses a less important requirement when compared with a manned cabin. Generally speaking, electronic components are able to operate safely with temperature superior to 100°C. Nevertheless, such high level of temperature drastically reduces the reliability of the components at issue. For this reason, military equipment is usually required to work reliably within about -30°C and 70°C. Moreover, they have to be able to operate undamaged, but not necessarily reliably, between -40°C and 90°C.

Prior to deal with ECS functional analysis, it is convenient to present an overview of the main methods used for environmental control.

The simplest, hence less effective, environmental control system is ram air cooling. It basically makes use of external unconditioned air that, moving through a heat exchanger, is used to reject heat from the aircraft. Besides increasing aircraft drag caused by the presence of the duct that slows down ram air, this method is considerably limited due to the condition of external air. While at low altitude the air can be at a very high temperature, at high altitude the density of the atmosphere is quite low, and the cooling capabilities of fluid are compromised. In addition to that, when the aircraft is on the ground it is necessary to implement a way to make air pass through the heat exchanger. This is made either with the use of an electric motor driven fan or a jet pump. The latter, heating the outlet of the scoop, force air to pass through it.

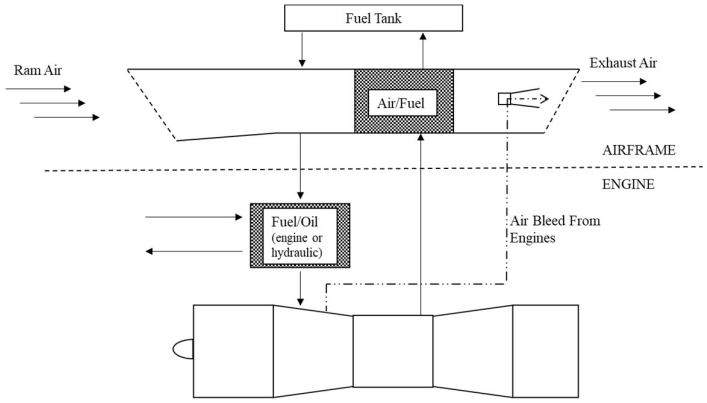

Figure 1.5: Fuel Cooling (ref. [3])

As reported in Figure 1.5, fuel can be cooled in the air/fuel heat exchanger. Moreover, it is usually used to cool hydraulic or engine oil. Note that the fuel/oil heat exchanger has to be designed to avoid, in case of a leak, the fuel insertion in the oil circuit.

The system that paves the way to air conditionig in aircraft is engine bleed. It is indeed possible to use the engine as a source of hot and high pressure air bled from one or more stages of the compressor. Since the required air flow for cooling/heating can considerably affect the thrust and the fuel consumption of the engine, it is possible to implement closed loop systems. In order to reduce the fluid mass flow bled from the engine compressor is indeed possibile to recycle part of the air already present in the cabin. Nevertheless, these kind of systems normally tend to have a higher weight in comparison with open loop systems. A more-electric alternative to engine bleed sees the use of a dedicated compressor moved by an electric motor. This solution, applied in the Boeing 787, allows to completely eliminate engine bleed, hence allowing higher efficiency of the latter. The air bled from the engine has pressure of tens of bars and temperature around 500°C. Those values are too high for the fluid to be direclty workable for air conditioning and the temperautre represents even a threats for the materials of the pipe the air passes through. Moreover, such high levels of pressure increase the complexity, hence the weight, of valves and seals. Nevertheless, bleeding air from lower stages of the compressor would lead to a severe decrease of the already reduced efficiency of the engine. It is therefore necessary to adopt pressure regulating valves and to cool the bleed air via an heat exchanger. As visible from Figure 1.6, and as will be deeply dealt with in the section dedicated to the performance analysis, pressure and temperature regulation need to be subject to a control logic depending on the flight phase and climatic condition.

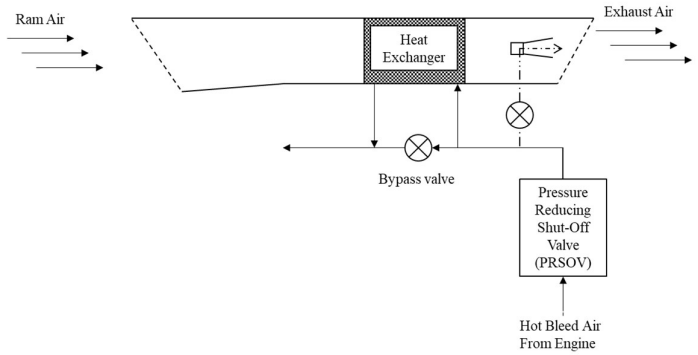

Figure 1.6: Bleed Air Thermal Control (ref. [3])

Moving to air conditioning architectures, those that will be considered and implemented during performance analysis are air cycle and vapor cycle refrigeration systems.

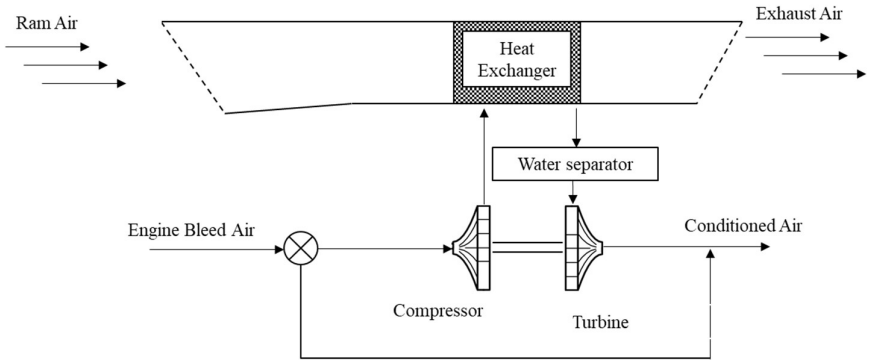

Figure 1.7: Air Cycle System (ref. [3])

To begin with the Air cycle refrigeration system, schematized in Figure 1.7, it is possible to notice how bleed air undergoes a compression, a cooling heat exchange and a turbine expansion. This thermodynamic cycle, which will be dealt with in chapter 3, dedicated to the performance analysis, leads to the provision of conditioned air.

The vapour cycle, reported in Figure 1.8, represents instead a closed loop that exploits a liquid refrigerant that, through its phase changes, exchanges heat loads with the air that will be sent into the cabin or, in the UAV case, to the avionic bay.

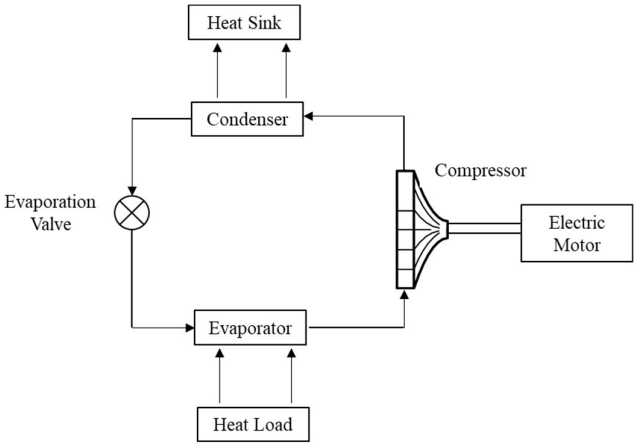

Figure 1.8: Vapour Cycle System (ref. [3])

Albeit vapour cycle solutions are up to five times more efficient, they are also heavier and, depending on the refrigerant used, they have more restrictive operating temperature ranges.

2 ECS Functional Analysis

2.1 Model Based System Engineering

The functional analysis of the environmental control system at issue has been performed, rather than referring to the traditional document-based systems engineering approach, referring to a Model Based System Engineering (MBSE) approach. As has already been explained, this approach relies upon a precise language which provides the associated rigor, formalism, productivity improvement and risk reduction.

The abovementioned language is System Modelling Language (SysML), a graphical modelling language that allows to model the requirements, the behaviour of the system and its logical and physical architecture. Specifically, as reported in L. E. Hart, "Introduction to Model-Based System Engineering (MBSE) and SysML", Lockheed Martin, Delaware Valley INCOSE Chapter Meeting July 30, 2015, a system model focuses on:

- Requirements:
  - What are the stakeholder goals, purposes, and success conditions for the system
  - Specification of black box behaviour and characteristics
- Behaviour:
  - What the system has to do to meet the requirements
  - Transformations of inputs to outputs (functional/activity models)
  - State/Mode-based behavioural differences (state models)
  - Responses to incoming requests for services (message models)
- Structure:
  - The parts that exhibit the behaviour
  - The component hierarchy, elements, and stores
- Properties:
  - The performance, physical characteristics and governing rules that constrain the structure and behaviour
- Interconnections:
  - The way the structural elements arrange and communicate to achieve the required behaviour under the given constraints

Moreover, SysML is made up of several diagrams, reported in the scheme in Figure 2.1.

Dealing with the ECS functional analysis, the SysML has been applied adopting the IBM Harmony ® methodology and the software IBM Rational Rhapsody ®. The main phases of the analysis were:

1. Requirement Analysis
2. System Functional Analysis
3. Design Synthesis

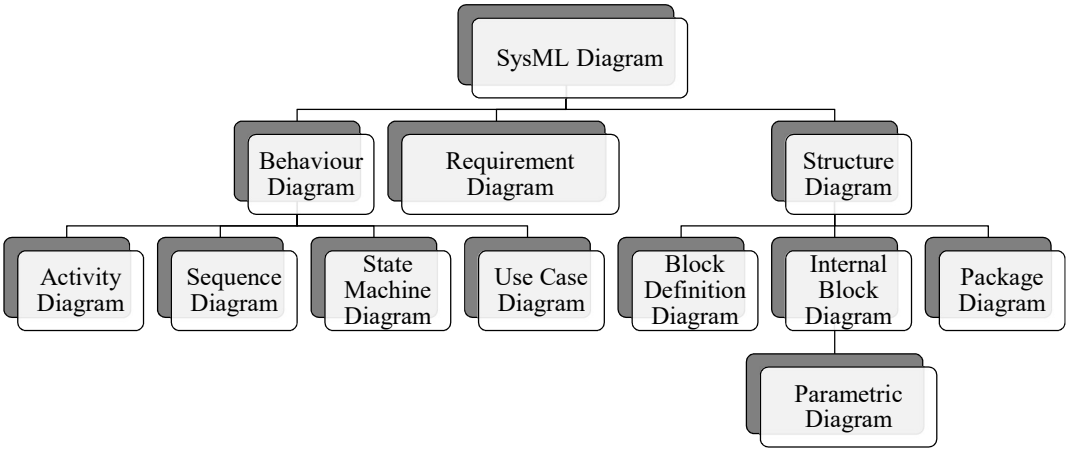

Figure 2.1: SysML Diagrams (ref. [4])

2.2 Requirement Analysis

In this phase the system requirements are analysed with the aim of determining system macro-functionalities. Those entities will be the basis for the following to steps.

To begin with the requirements of the environmental control system at issue, they have been determined by the ECS specialist and by the preliminary design expert. They are both functional and performance requirements and are reported in Table 2.1.

ID	Name	Specification
SR001	SR001 – Air Conditioning	The ECS shall autonomously assure air conditioning to the avionics/electronics equipment, allocated in the avionic bay, from start up to shut down
SR001.1	SR001.1 – Air Conditioning (Ground Operations)	The ECS shall autonomously assure air conditioning to the avionics/electronics equipment, allocated in the avionic bay, during ground operations
SR002	SR002 – Air Filtering	The ECS shall assure air filtered to avionics equipment, allocated in the avionic bay, in order to protect the avionic from fine dust and water
SR002.1	SR002.1 – Filter Pressure Difference Comparison	The ECS shall measure information about pressure difference and compare it with a threshold value
SR002.2	SR002.2 - Filter Clogged Alert	When the measured pressure difference is higher than the threshold value, the ECS shall send the value of pressure difference (filter clogged) to Central Maintenance system
SR003	SR003 - Bay Monitoring	The ECS shall monitor the avionic bay temperatures
SR004	SR004 - Over Temperature or Under Temperature Alert	The ECS shall provide an alert to Utility Management System when avionic bay temperature is out of range
SR004.1	SR004.3 - Over Temperature or Under Temperature Condition -	In case an over temperature or under temperature is detected in the avionic bay, the ECS shall be powered off

	Power Off	by Utility Management System
SR004.2	SR004.1 - Over Temperature or Under Temperature Condition – Air inlet area control	In case an over temperature or under temperature is detected in the avionic bay, the ECS shall autonomously increase or decrease air inlet area
SR005	SR005 - ECS Health Status Monitoring	The ECS shall monitor its health status, from start up to shut down
SR005.1	SR005.1 - ECS Health Status Information	The ECS shall send information about its health status to the Utility management system and Central Maintenance System
SR005.2	SR005.2 - ECS working fluid Over or Under Temperature Information	The ECS shall send information about working fluid over temperature or under temperature to the Utility Management System and Central Maintenance System.
SR006	SR006 - ECS Start Up Condition	The ECS shall start up when powered by electrical system
SR006.1	SR006.1 - IBIT	At start up the ECS shall provide IBIT to Central Maintenance System
SR007	SR007 - MBIT Performing	The ECS shall perform MBIT when requested by Central Maintenance System
SR007.1	SR007.1 - MBIT Results	The ECS shall send MBIT result to Central Maintenance System
SR008	SR008 - Shut Down	The ECS shall shut down when electrical system stops providing electrical power
SR009	SR009 - Bay Temperature	The ECS shall protect avionics/electronics equipment, allocated in the avionic bay, within the following avionic bays temperature range: from -20°C to 50°C

Table 2.1: System Requirements

The analysis of these requirements leads to the definition of six “use cases”, identifiable as macro-functionalities of the system. The determined macro-functionalities are:

1. **Start up**. The ECS shall start up and execute an initial built in test (IBIT). This test comprehends a preliminary check-up of the correct behaviour of the sub-systems that make up the ECS (it includes, for instance, a complete opening and closing of the air intake with the aim of verifying the correct functioning of the dedicated actuator). The results shall be sent to the Central Maintenance System (CMS) which represents, as will be explained later, one of the actors interacting with the system and with its functions.

2. **Provide air conditioning**. When the ECS is operating, its primary function is to provide the avionic bay with enough conditioned air so its temperature does not exceed the allowed ranges. A precise description of this process will be deeply faced in the chapter dedicated to the performance analysis of the environmental control system. In the event of an over temperature or under temperature condition, the ECS shall be able to perform two

recovery, or back up, actions. These includes powering off the system and autonomously controlling the air inlet area in order to increase or decrease, when needed, the quantity of external air, warm or cold depending on climatic and flight condition, that is sent to the avionic bay. This process have to be completely autonomous since it has to be correctly executed even in case of loss of communication between the vehicle and the ground station. Moreover, in case of avionic bay temperature outside the ranges, the system shall send an alert to the Utility Management System.

3. **Monitor its health status**. The system shall continuously monitor the health status of its components computing the measurements of different sensor (e.g. temperatures, pressures, rates per minute, mass flow).

4. **Monitor status of air filer**. The air filter is necessary since it does not allow dust to reach the electronic equipment installed in the avionic bay. When the pressure difference between the entrance and the exit of the air filter exceeds a certain range, the filter is considered clogged and a message is sent to the Central Maintenance System.

5. **Provide maintenance**. When required, the system shall perform a built-in test (MBIT) and send its results to the CMS.

6. **Shut down**. In nominal functioning, the system has to be powered off once the flight is ended. Moreover, it may be convenient to shut down the ECS in the event of a malfunction of that leads to the provision of overheated/overcooled air to the avionic bay.

The description of each macro-functionality has been executed in the system functional analysis and, as will be explained later, it is represented in several diagrams that will be used again in the safety analysis.

Anyway, the actors interacting with the mentioned functionalities are:

- **Central Maintenance System:** it represents the interface between the on-board systems and the ground maintenance systems. Receiving information about the health status of the various equipment installed on the aircraft is indeed useful to undertake an optimization of maintenance processes and the increase of the reliability of the system.
- **Electrical System:** it represents the source of electrical power used to feed the components of the onboard system at issue.
- **Utility Management System:** it represents the system intended to manage the performance information regarding the functioning of the on-board systems.
- **Avionic Bay:** it represents the target of the air that is conditioned by environmental control system.
- **Environment**

The use-case diagram realized in the adopted functional analysis tool is reported in Figure 2.2.

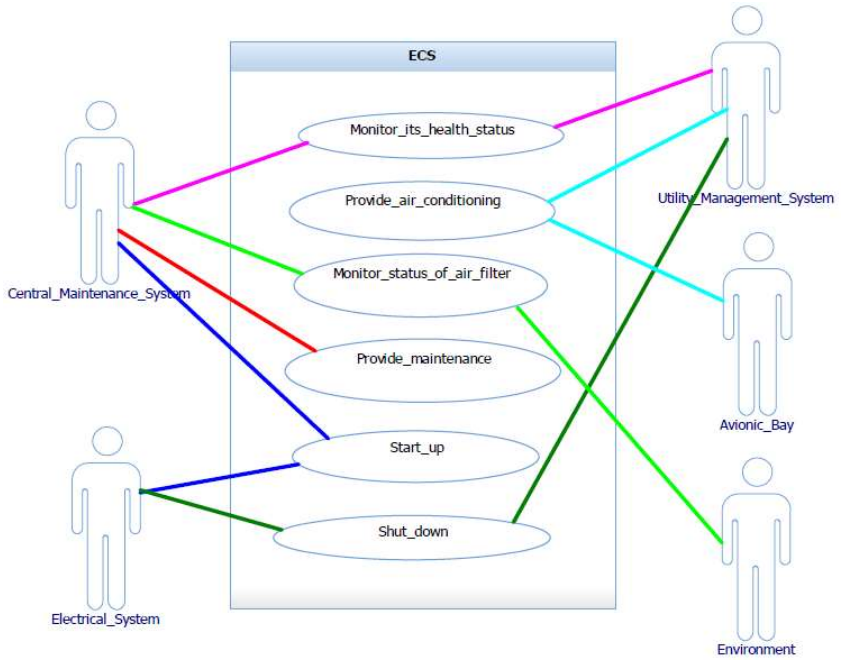

Figure 2.2: Use Case Diagram

Once that the use cases have been identified it is possible to build the requirements table, reported in Table 2.2. It consists of a matrix intended to point out the allocation of the requirements to the relative use case: the coloured boxes indicate indeed the links between every requirement and the macro-function of the system that concur at the execution of the function at issue. Note that while every requirement is associated to a single use case, the latter includes several requirements.

	Shut down	Start up	Provide maintenance	Monitor status of air filter	Monitor its health status	Provide air conditioning
SR5 - ECS Health Status Monitoring						
SR4.2 - Over Temperature Or Under Temperature Condition - Power Off						
SR5.2 – ECS working fluid Over Or Under Temperature Information						
SR5.1 - ECS Health Status Information						
SR6 - ECS Start Up Condition						
SR6.1 - IBIT						
SR7 - MBIT Performing						
SR1 - Air Conditioning						

SR1.1 - Air Conditioning During Ground Operation						
SR2 - Air Filtering						
SR2.1 - Filter Pressure Difference Comparison						
SR2.2 - Filter Clogged Alert						
SR3 - Bay Monitoring						
SR4 - Over Temperature Or Under Temperature Alert						
SR4.1 - Autonomous Air Inlet Area Control						
SR7.1 - MBIT Results						
SR8 - Shut Down						
SR9 - Bay Temperature						

Table 2.2: Requirements Table

2.3 System Functional Analysis

In this phase the abovementioned macro-functionalities are analysed with the aim of defining the single activities, or single functions/actions, that the system has to execute in order to completely fulfil the macro-functionality at issue. This process also comprehends the definition of the interactions between the system itself and external actors. The single functions that will be determined in this phase will be exploited during the execution of the Functional Hazard Assessment according to the MBSE approach.

All the diagrams that will be reported in this section, for sake of brevity, are referred to the use-case “Providing Air Conditioning”. This is indeed the main functionality of the ECS at issue, hence its diagrams, when compared with the others, are the most meaningful.

The first step of the analysis at issue is the definition of the Activity Diagram, reported in Figure 2.3, which illustrates the actions undertaken by the system with the aim of performing the macro-functionality (or use-case) to whom the diagram is aimed.

The first action necessary to complete the functionality at issue is the measurement of the avionic bay temperature, hence the action see an interaction with the avionic bay itself which is, as a matter of fact, one of the actors whose links are reported in the use-case diagram described in the section above. Subsequently, the system sees the comparison of the measured temperature with the established threshold values and, coherently with what has already been described, varies its functionality depending on the truthfulness of the “threshold exceeded” condition.

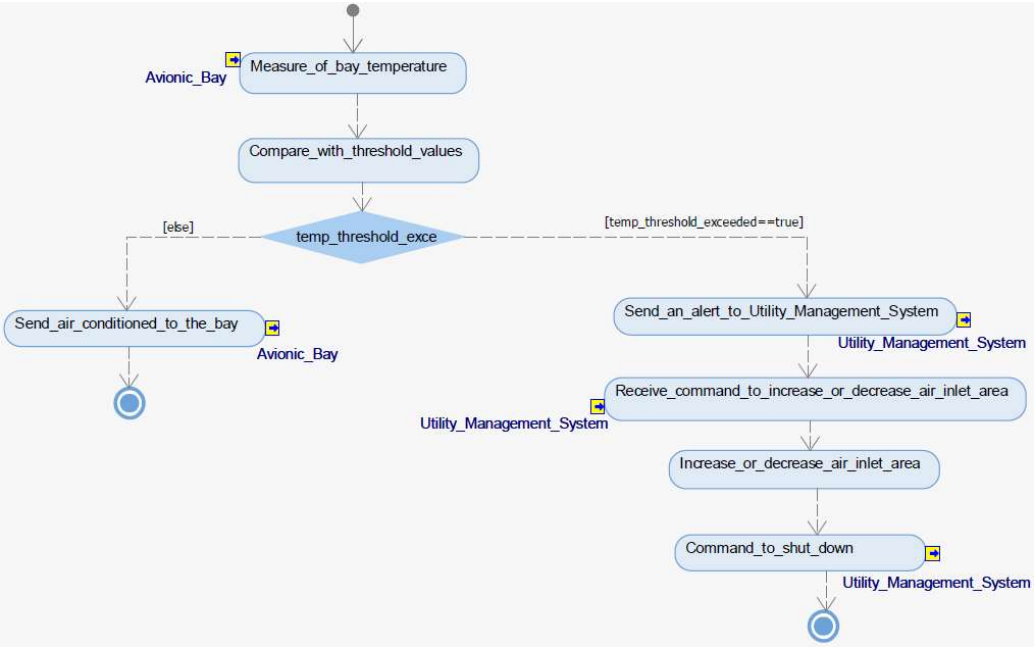

Figure 2.3: Provide Air Conditioning – Activity Diagram

The diagram here generated is moreover used to the generation of one, or more, Sequence Diagrams. This particular diagram, although containing the same actions already reported in the previous diagram, appears particularly useful to the comprehension of the system since it highlights the interactions between the actors and the use cases. The following two figures (Figure 2.4 and Figure 2.5) report the Sequence Diagram for the use-case at issue for both the conditions of temperature. While the activity diagram contains indeed both possibilities, a different Sequence Diagram may be required for every possible condition.

Figure 2.4: Provide Air Conditioning - Sequence Diagram 1

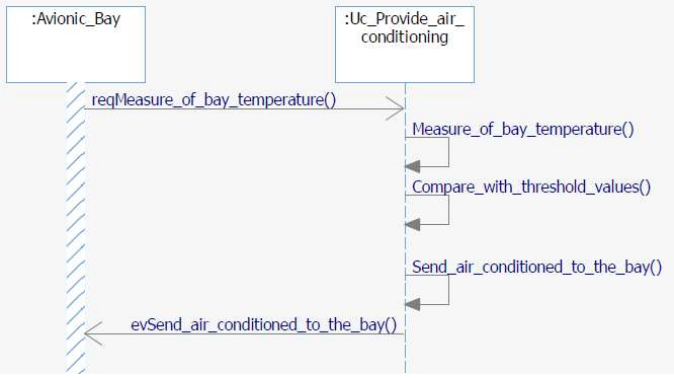

Figure 2.5: Provide Air Conditioning - Sequence Diagram 2

The following phase of the analysis lays its base on the diagrams generated until now and sees the creation of the Internal Block Diagram. It consists of different blocks representing the use case at issue and the different actors which interact with the latter. The diagram, reported in Figure 2.6, is completed with all the operations executed by each block and shows the interconnections between the various elements.

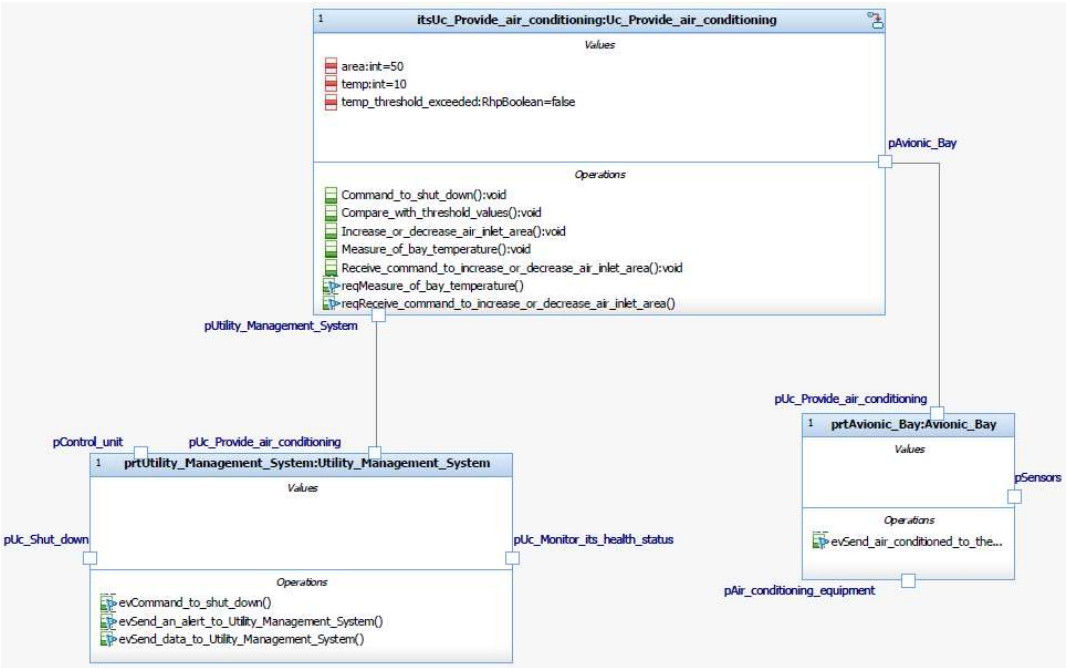

Figure 2.6: Provide Air Conditioning - Internal Block Diagram

Subsequently, it is possible to build the State Machine. It has the aim of describing the different states in which the system can function and the events whose happening causes the transition between a state and another. The diagram is reported in Figure 2.7 where it is possible to notice how the first state of the system is a standby one: the ECS is waiting to receive the measurement of the temperature. It will maintain itself in this state until the mentioned measurement is available: the measure represents indeed the event which makes the system move to the

following state. As soon as it enters into a new state, one or more actions, previously assigned to the state at issue, are executed.

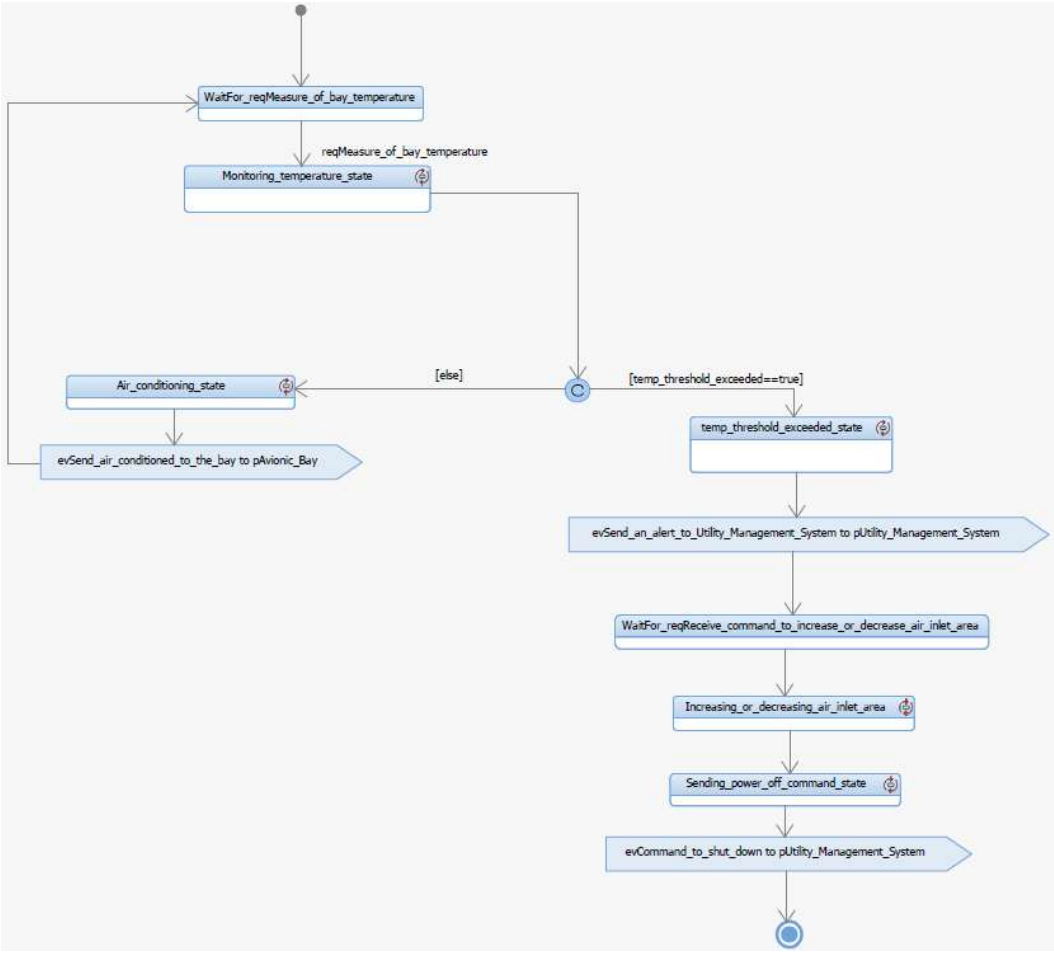

Figure 2.7: Provide Air Conditioning - State Machine Diagram

The State Machine Diagram appears to be particularly useful since it allows to build a panel whose important function is to validate the analyses conducted so far. It is indeed possible to use the mentioned panel in order to verify every functional requirement that paved the way to the construction of the already mentioned diagrams.

The panel that has been built is reported in Figure 2.8 and it is divided into two zones:

(1) Pilot Control Panel: it reports the commands available to the pilot (ECS start up, shut down, MBIT request); two dials reporting the temperature of the avionic bay as measured by sensors and the air inlet area; a series of displays and led aimed to the signalling of the various alerts (over/under temperature, filter clogged) and of the state of the system (ON/OFF, IBIT and MBIT results).

(2) External Events: similarly to what happens in a flight simulation, this panel allows to manipulate the avionic bay temperature and the state of the air filter (filter working – filter clogged). Those commands are useful since they allow to force the system to leave the nominal state hence verify the correct execution of the emergency procedures which

comprehend, as already described, the powering off of the system and the increasing (or decreasing depending on the over/under temperature) of the air inlet area.

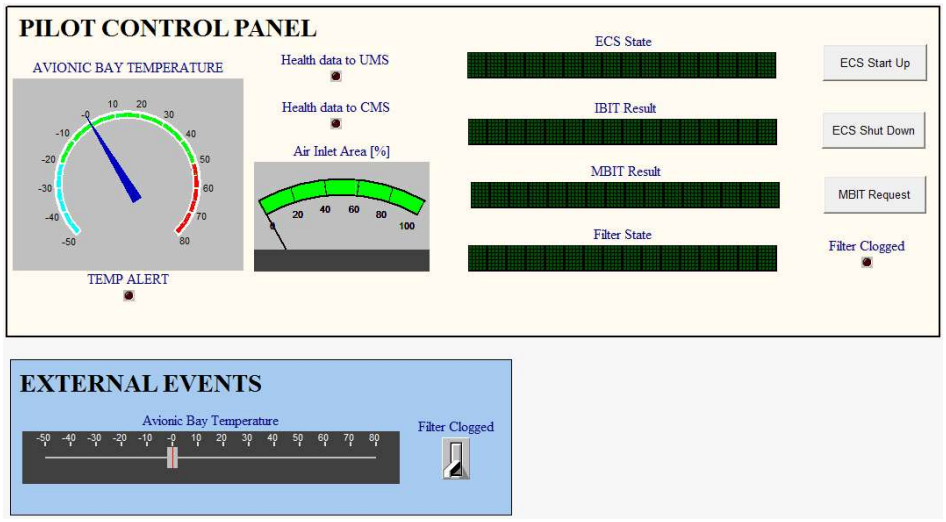

Figure 2.8: ECS Panel (Functional Model)

2.4 Design Synthesis

This phase is aimed to the linkage of the abovementioned single functions/actions to the component that will execute the action at issue. Since the components make up a logical or a physical architecture of the system, this phase is particularly useful in order to locate function and sub-function to a specific equipment. This process paves indeed the way to the safety analysis inasmuch it allows to comprehend which are the components linked to more severe safety requirements and that, as a consequence, need to be characterized by certain level of reliability.

Design Synthesis is made up of two phases: Architectural Design and Architectural Analysis. While the first is aimed to the modelling of a logical or physical architecture of the system, the second one sees the allocation of the actions making up the Activity Diagram to the respective equipment. The physical description of the system is then reported in the figure below which represents the Block Definition Diagram. It is possible to divide the ECS in the following group components:

- Control Unit
- Air conditioning equipment
- Filter
- Sensors

As already mentioned, each operation introduced in the previous analysis is here assigned to a specific equipment.

Moreover, it is of fundamental importance to notice that, up to this point, and to the end of the functional analysis at issue, the real physical architecture of the ECS has been chosen yet. Whether we are dealing with a vapour cycle system or an air cycle one, the elements that characterize those architectures are part of the “air conditioning equipment” and, since they

cover the same functions, they do not influence the functional analysis conducted at this stage of the design.

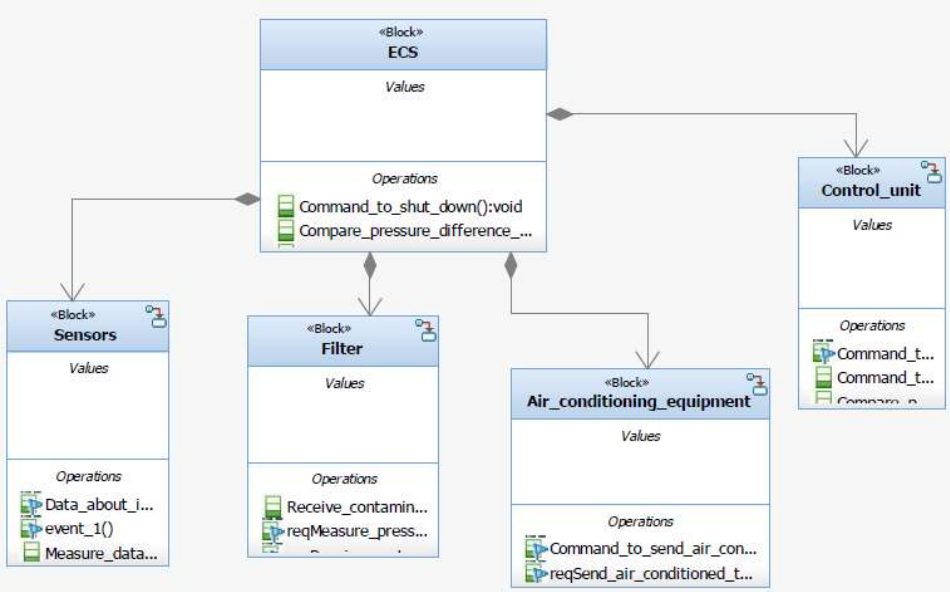

Figure 2.9: Block Definition Diagram

Subsequently, it is possible to generate the White Box Diagram. They are basically made up of Activity Diagrams whose actions have been assigned to the blocks making up the Block Definition Diagram. For a better understating, the following figure reports the White Box Diagram referred to the same use-case used before.

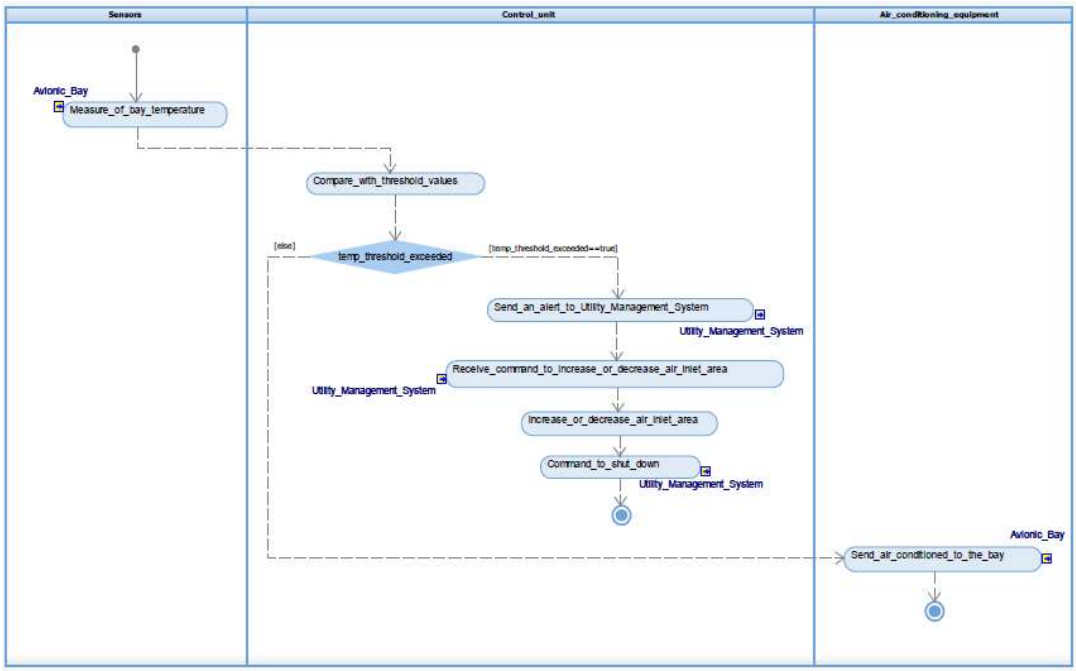

Figure 2.10: White Box Diagram

3 ECS Performance Analysis

The performance analysis of the environmental control system at issue has been executed using the Siemens software Simcenter Amesim ®. This tool allowed indeed to numerically verify that the chosen components were suitable to respect the requirements: the ran simulations were aimed to the determination of the avionic bay temperature along the whole considered mission profile. The next subsection will indeed be focused on the model used to represent the thermofluidodynamic behaviour of the bay and to the definition of the mission profile and of the climatic conditions.

Moreover, the following subsection will be dedicated to the modelling of two different ECS typologies: vapour cycle and air cycle systems. While the subsystem-level architectural, and performance, differences of the two solutions will be deeply described below, it is of fundamental importance to pay attention to the integration of these two systems in the overall vehicle. While the vapour cycle lays basically on the provision, from the electrical system of the vehicle, of electrical power needed to feed the compressor, the air cycle exploits bleed air. Albeit there exists the possibility of using the air cycle in a more-electric aircraft feeding it with air compressed by a dedicated compressor, which is moved by a dedicated electrical motor, the considered solution makes use of air bled from the engines. This means that, in case of the air cycle, the design, or the selection, of the engine will have to keep in consideration the mass flow required by the bleed system. On the other hand, apart from electrical power needed in both cases to move the small fan used to draw air into the inlet when the aircraft is on the ground, vapour cycle has higher level of electrical power required, hence it will have a certain influence on the design and on the sizing of the electrical system of the vehicle.

3.1 Bay model and mission profile

In order to model the avionic bay from a thermodynamic point of view it is necessary to take in consideration the different kind of heat loads that influence the bay. In particular, as visible from the figure below, the considered heat fluxes are:

- Conduction and convective heating. These affect the walls of the vehicle surrounding the avionic bay. In particular, it has been considered a carbon fibre reinforced polymer skin, whose thickness is 2.5 mm, and an internal layer of Aluminium alloy whose thickness is 3 mm. The temperature used to compute the conduction heating between the external environment and the skin of the aircraft is the recovery temperature, calculated as a function of the external temperature T_0 and the flight Mach number M:

$$T_{rec} = T_0 \left(1 + r \frac{\gamma - 1}{2} M^2\right)$$

The model then considers conductive heating between the skin and the avionic equipment.

- Radiative heating. Since in an unmanned air vehicle part of the skin may be "transparent" to solar radiation, so that to favour the functioning of different payloads, it appears also necessary to take in consideration radiative heating. As will be explained later, this will not be considered in the "cold" condition, representing as a matter of fact a cold (ISA-35) night flight, since it is only present in daylight.

- Electronic heating. As will be discovered running the simulation, the major heating contribute to the avionic bay is electronic heating. Although it usually varies along the whole mission, its most meaningful variation takes place between in-flight and on-the-ground phases. For this reason, a first value of 4 kW has been considered until take-off while, as soon as the aircraft is in the air, a value of 9 kW is computed.

All of these contributes converge in the thermal chamber, represented in Figure 3.1 by the blue "C", which represent the thermal model of the avionic bay, characterized by a volume of 2.5 m^3.

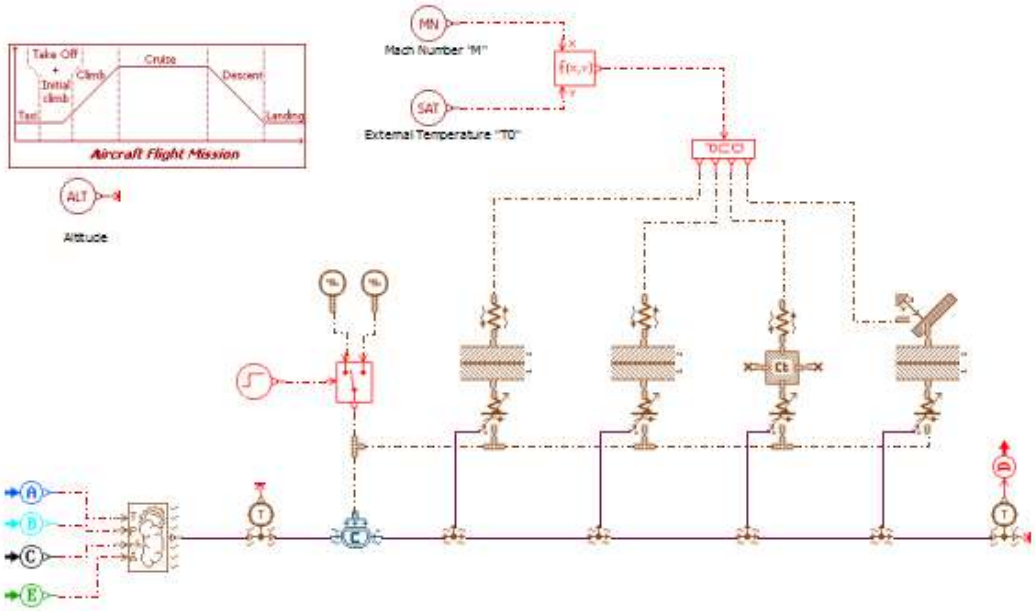

Figure 3.1: Avionic Bay Model

As visible from the model (Figure 3.1), there are two temperature sensors before and immediately after the avionic bay. The measured values are indeed used to compute a weighted medium temperature ($T_M = 0.25\,T_{IN} + 0.75\,T_{OUT}$) which will be used to evaluate the avionic bay temperature and verify that this does not exceeds the threshold for the whole simulation. Note that, in more advanced stages of the design, a Computational Fluid Dynamics (CFD) analysis shall be used in order to evaluate the three-dimensional distribution of temperatures (At

this purpose, see chapter 5). In a real-life scenario, the bay temperature is indeed measured in specific locations of the equipment where sensors are installed.

In the top left corner of the figure representing the avionic bay model it is possible to notice the presence of the block aimed to the definition of the mission profile. In order to validate the correct functioning of the components during the whole flight it is indeed necessary to take in consideration a complete mission profile. This leads to the obliged consideration of those conditions that most stresses the ECS at issue.

The mission profile in terms of altitude and Mach number is reported in the figures below (Figure 3.2 and Figure 3.3).

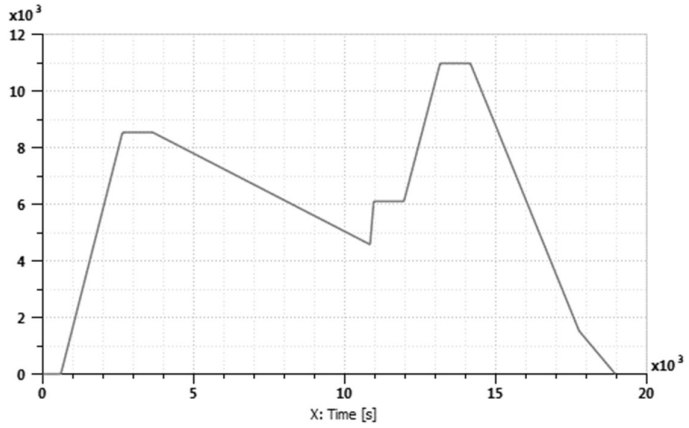

Figure 3.2: Mission Profile - Altitude [m]

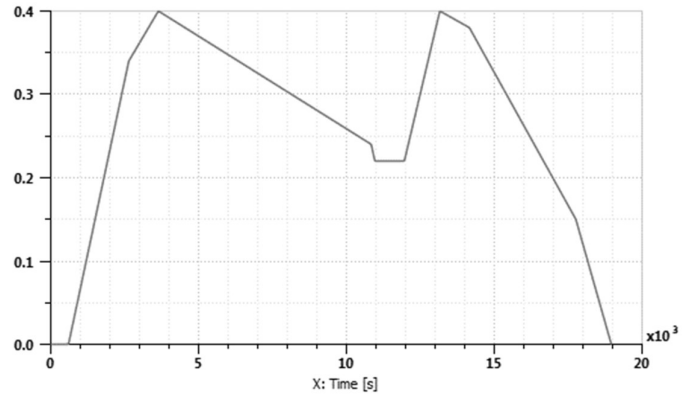

Figure 3.3: Mission Profile - Mach

The particular mission profile reported has been chosen since, reporting different cruises at different altitudes (hence different climbs, descents and relative rates), it is representative of a wide number of flight condition that the aircraft may encounter in its operative life.

Since those conditions do not only depend on the flight phase (Mach – external pressure and temperature) but even on the meteorological conditions in which the aircraft is flying, it is convenient to consider a “hot” day and a “cold” night as worst cases:

(1) Hot condition: the aircraft is on the ground on a hot day, characterized by a sea level temperature of 50°C (323.15 K). The altitude-temperature profile has been computed considering ISA + 35.

(2) Cold condition: the aircraft is at its maximum cruise altitude (i.e. 11000 m or FL360) on a cold night, characterized by a sea level temperature of -20°C (253.15 K). The altitude-temperature profile has been computed considering ISA - 35. Note that, as already mentioned, since this condition happens to take place at night, the radiative solar heating has not been considered.

Taking into account all of what has been said, it is necessary to consider that a certain value of air flow is required for cooling even when the aircraft is on the ground, hence its airspeed is equal to zero. For this reason, a fan driven by an electric motor has been considered. This stops to work, soon after take-off, as soon as the air flow generated by airspeed alone becomes superior to the value guaranteed by the fan. Nevertheless, it is possible to avoid the presence of the fan, hence saving weight and the electrical power required by the dedicated motor, exploiting a small amount of hot air flow. As a matter of fact, this air can be expelled in the exit nozzle of the duct containing the heat exchangers in order to force the environmental calm air to pass through it. Although being simple and usually adopted on air cycle systems, where the hot air at issue derives from the engine bleed system, this solution appears disadvantageous on bleed-less aircrafts endowed with vapour cycle cold air unit. Anyway, the values of the external and recovery temperature are reported in the figure below (Figure 3.4 and Figure 3.5), respectively in blue and in red.

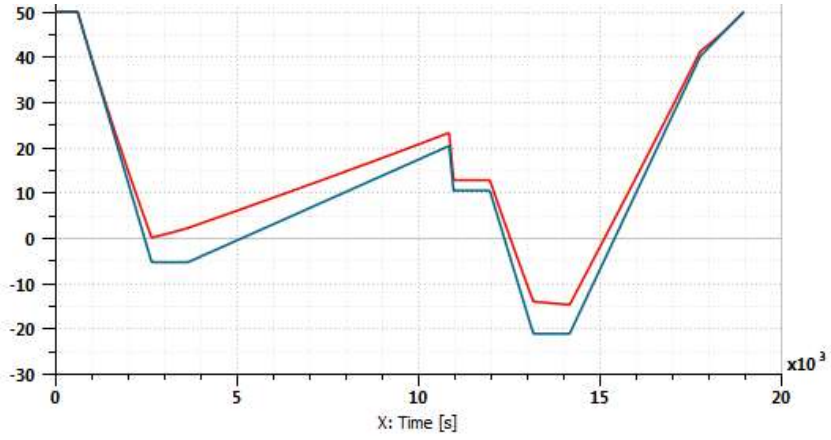

Figure 3.4: External and Recovery Temperatures [°C] – ISA+35

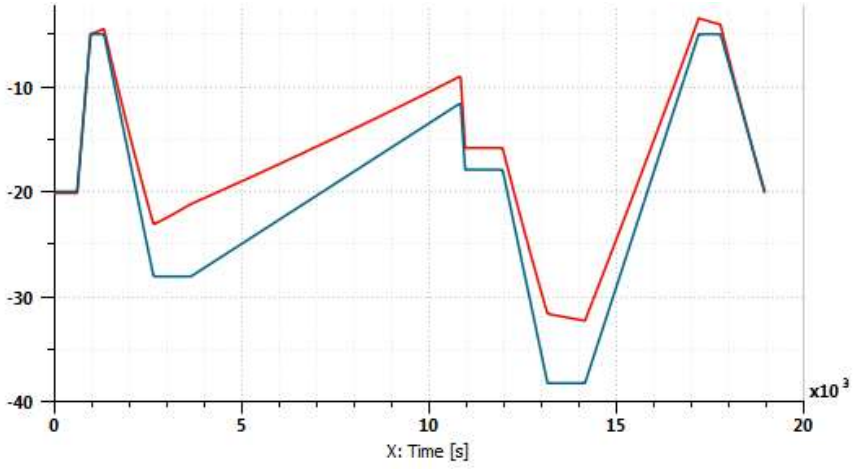

Figure 3.5: External and Recovery Temperatures [°C] – ISA-35

Dealing with the avionic bay CAD model, its peculiarities will be fully described in the chapter dedicated to the CFD analysis. Anyway, Figure 3.6 and Figure 3.7 report the hypothesized vehicle configuration and the estimated bay external dimensions. Specifically, the avionic bay occupies a major section of the fuselage and, as will be deeply discussed in chapter 5, is filled with Line Replaceable Unit avionics in accordance with reference [8]. The considered bay has a trapezoidal shape in order to allow the installation of a SATCOM antenna in the typical position for unmanned aerial vehicles, as visible in the scheme.

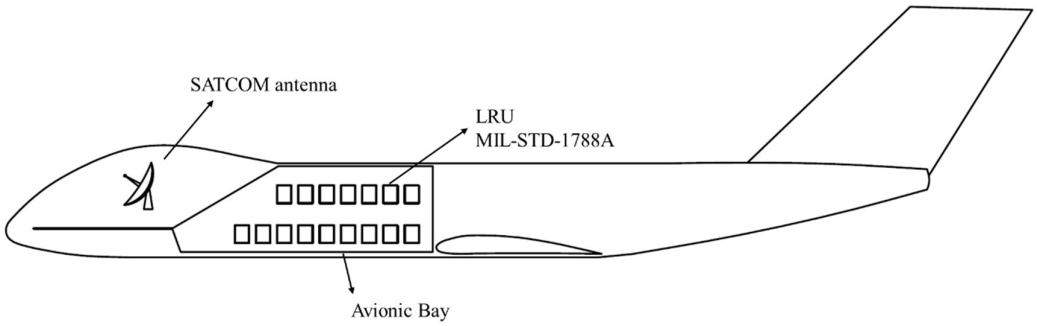

Figure 3.6: Aircraft Configuration

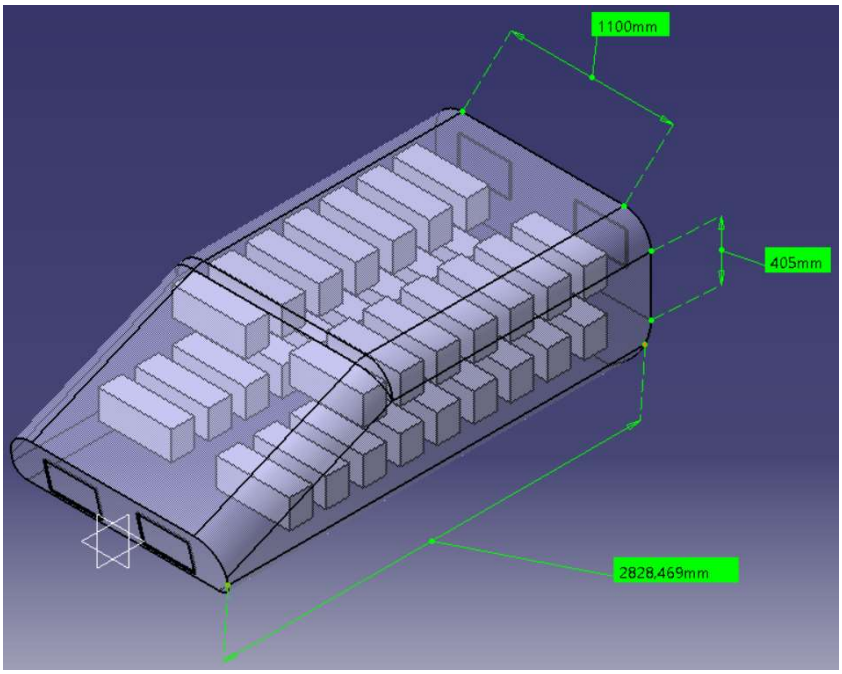

Figure 3.7: Avionic Bay CAD Model

Dealing with the avionic equipment installed in avionic bay, preliminary consideration for the reference vehicle led to the list reported in Table 5.2 in section 5.2.4.2 (page 92).

3.2 Vapour Cycle System

The Vapour Cycle System is based on a refrigerant, which in this thesis is assumed to be R-134a, which undergoes several thermodynamic transformations. The following two figures (Figure 3.8 and Figure 3.9) report, indeed, the architectural scheme of the designed system and the thermodynamic cycle on a H-p diagram. Beginning from the component number 1, it is possible to notice how the refrigerant fluid is subject a compression thanks to the electric motor. Subsequently, the highly compressed vapour passes through a condenser (2) which rejects the avionic heat, warming ram air passing through the duct where the condenser is installed. Inside the condenser, the fluid undergoes a phase change at constant pressure becoming liquid. The expansion valve (5) is then used to reduce the pressure and the temperature is furtherly reduced. Finally, the R-134s passes in the evaporator (6) where it is exploited to extract heat from the avionic bay. Parallelly to the refrigerant cycle, the air which cools the avionics undergoes a closed cycle, exchanging heat with the refrigerant. Note that, in order to guarantee the sufficient air circulation, the ducts are endowed with recirculating fans (7).

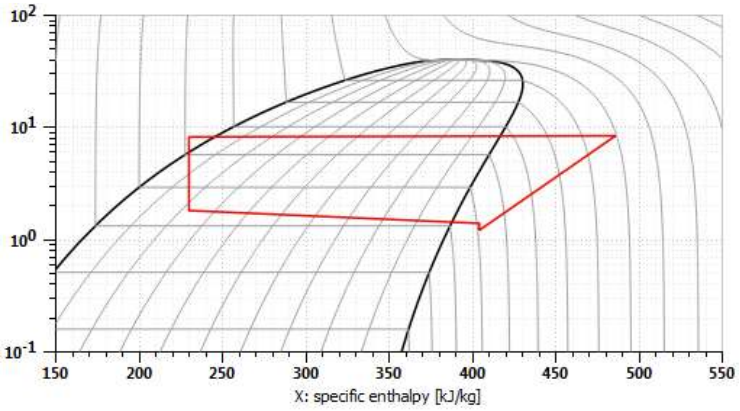

Figure 3.8: Vapour Cycle diagram (Specific Enthalpy [kJ/kg] - Pressure [bar])

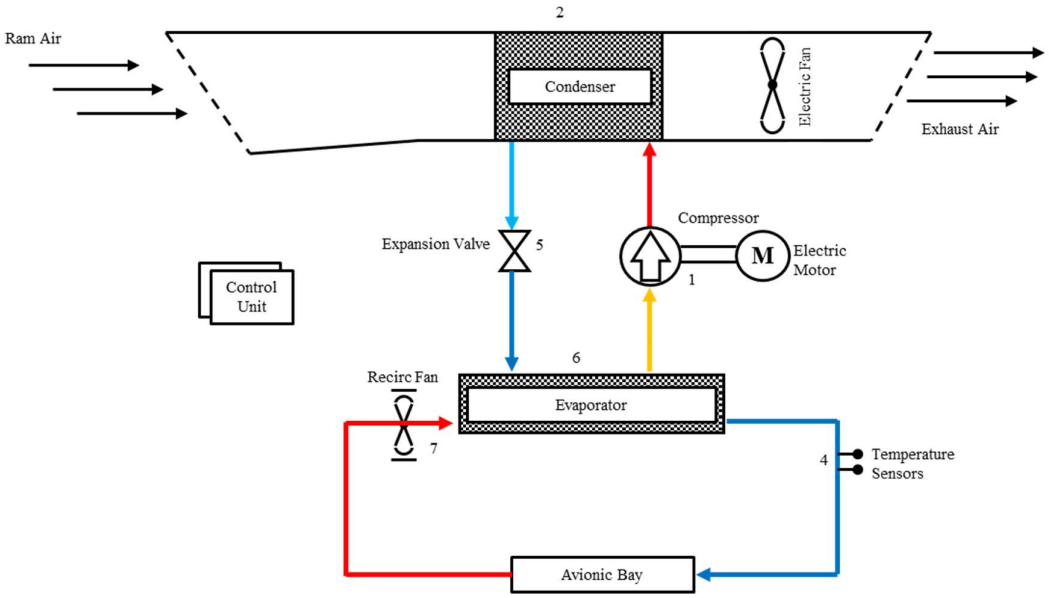

Figure 3.9: Vapour Cycle System Architecture

The same numbers identifying the components will be used during the Failure Modes Effect and Criticality Analysis that will be described in the Safety Assessment. All the safety related analyses will indeed refer to the same architectures described in the present chapter.

Figure 3.10 reports the scheme of the Vapour Cycle Cooling System that has been implemented into the used performance analysis tool. Note that this model is linked to the Avionic Bay and mission profile model shown in the previous sections. It is indeed necessary, as will be soon shown, to test the proposed architecture for the entire mission both in the "hot" and in the "cold" conditions, coherently with what has been defined before.

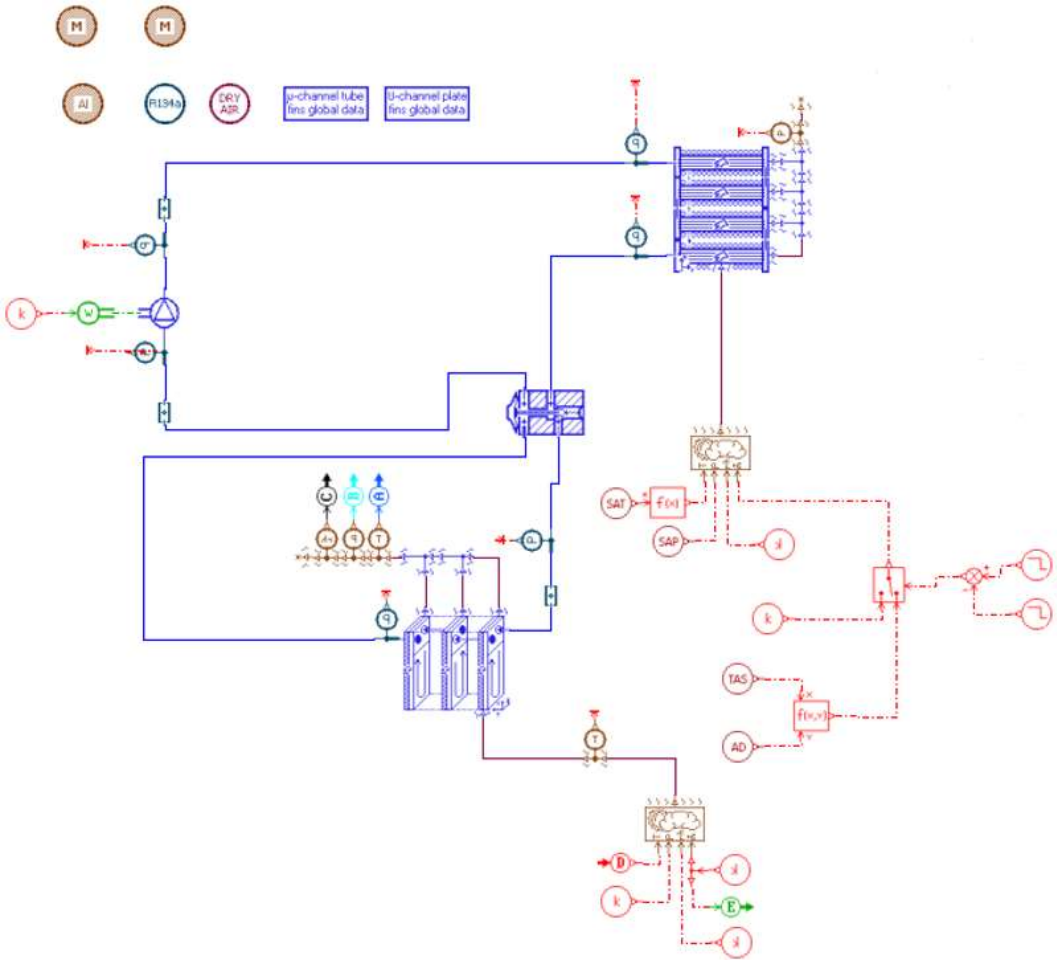

Figure 3.10: Vapour Cycle System

The following two sections report the results of the analysis, conducted with the adopted performance analysis tool, regarding the mentioned "hot" and "cold" conditions.

3.2.1 ISA + 35

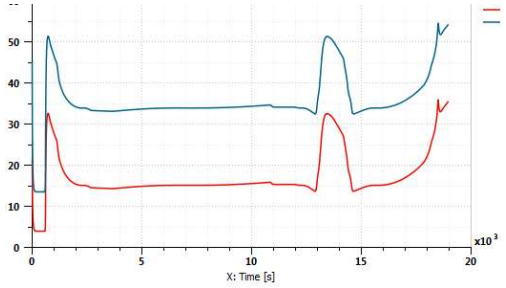

Figure 3.11: Inlet and Outlet Bay Temperature

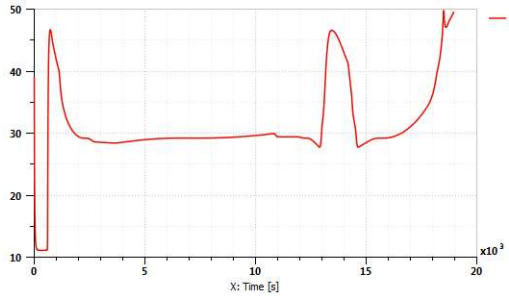

Figure 3.12: Mean Temperature

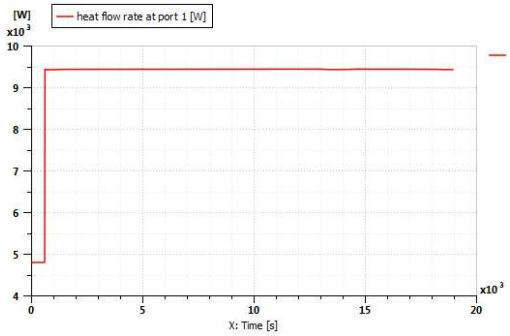

Figure 3.13: Bay Heat

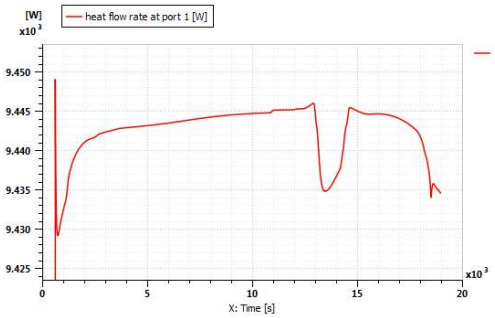

Figure 3.14: Bay Heat - Detail

3.2.2 ISA – 35

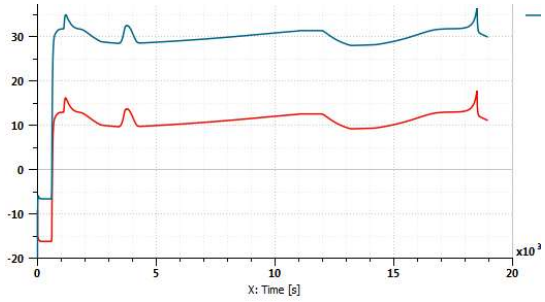

Figure 3.15: Inlet and Outlet Bay Temperature

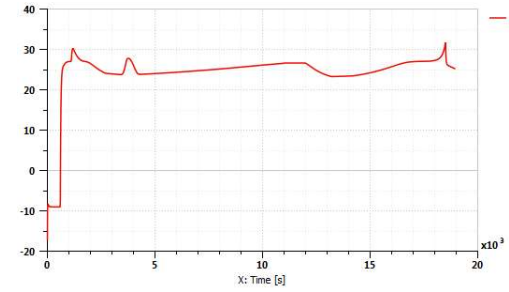

Figure 3.16: Mean Temperature

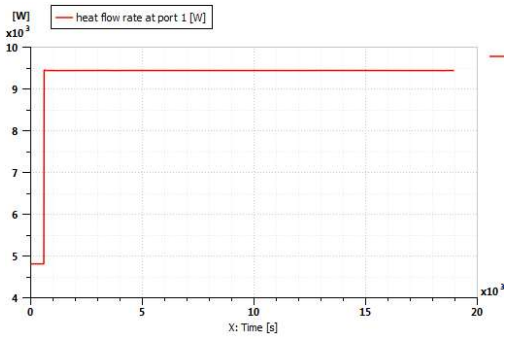

Figure 3.17: Bay Heat

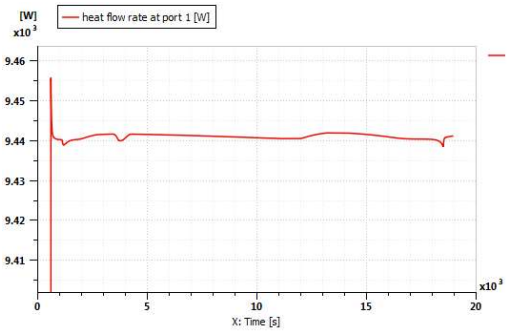

Figure 3.18: Bay Heat - Detail

3.3 Air Cycle System

The air cycle system that has been designed is reported in Figure 3.19. As has already been explained in 1.2.2, the air source is bleed air from engine number 1 and 2. The air passes through a combined pressure reducing and shut-off valve (PRSOV – 1 in the scheme): this unit is an in-line, pneumatically actuated valve which incorporates two valve heads which provide completely independent pressure regulating and shut-off function. This is indeed used to reduce pressure to 6 bar and, in case of an emergency, to shut-off the line. The following component present on the same line is a non-return valve which avoids air flux towards to engines. Subsequently, the air passes through a pre-cooler (3) which, exchanging heat with ram air, provides a first cooling of bleed air. At this stage, the line is endowed with a thermal control valve (TCV - 2) which, depending on the temperature at sensor 4, will determine the complete or partial by-pass of the pre-cooler. The process continues with air passing through the cold air unit (CAU - 12), made up of a compressor driven by a turbine. Specifically, as soon as air is compressed, it passes through a water separator device (1) and, subsequently, through the inter-cooler (8). Note that, as clearly visible in the scheme, the water obtained in this process is used with the aim of increasing the performance of the inter-cooler. The air is then subject to a turbine expansion which decreases its pressure and its temperature. The bay pass valve installed in this section of the line (TCV - 13) has been designed to guarantee a temperature of 2°C entering the avionic bay.

Coherently with what has been assumed dealing with the vapour cycle system, the ducts containing the heat exchangers are endowed with electric fans (27). These devices are necessary since, when the aircraft is flying below a determined air speed, the mass flow passing through the ducts would not be sufficient. This is particularly true before take-off, when electric fans are inevitable. However, it is possible to substitute those devices with pipes discharging hot bleed air from the engines in the duct outlet with the aim of generating the required flow.

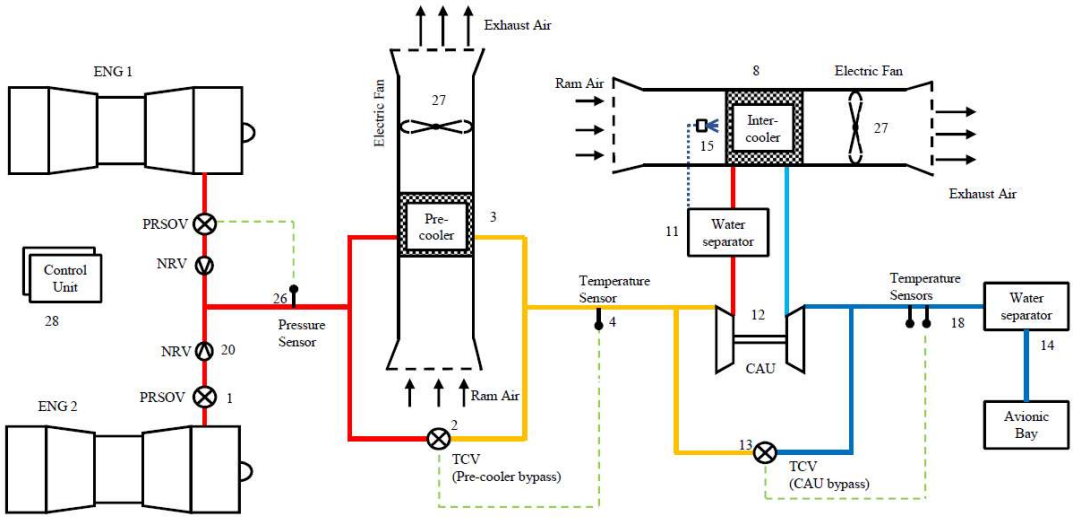

Figure 3.19: Air Cycle System Architecture

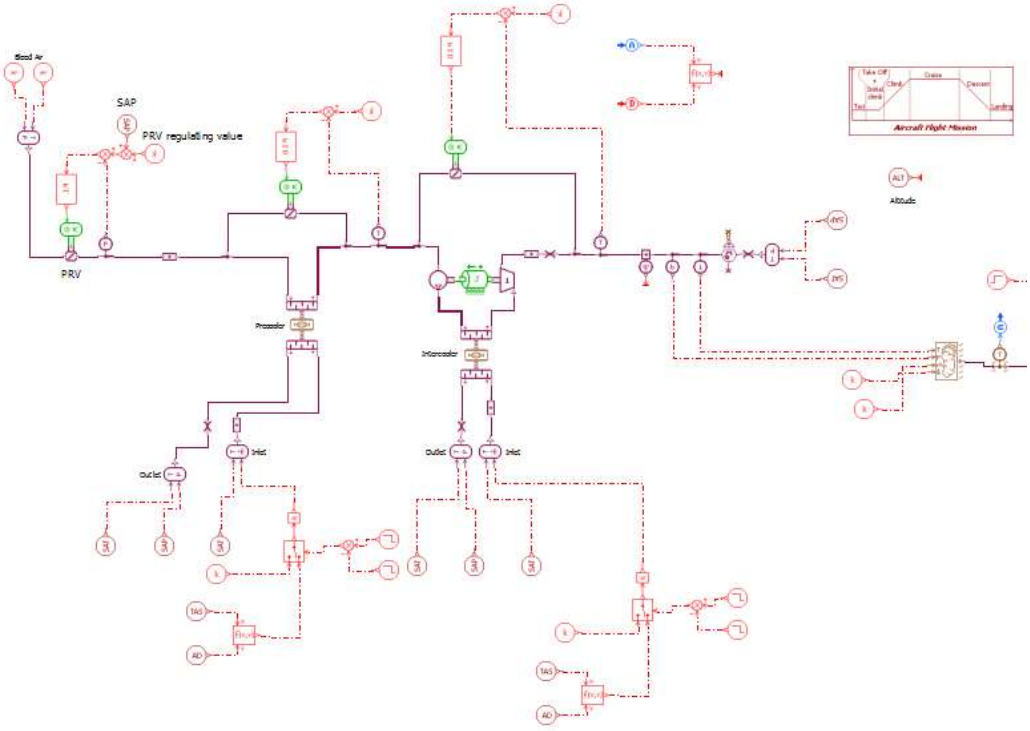

Figure 3.20: Air Cycle System

3.3.1 ISA + 35

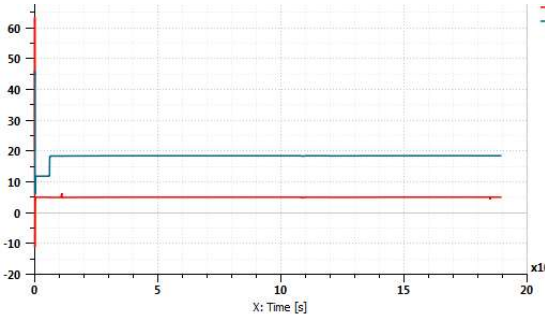

Figure 3.21: Inlet and Outlet Bay Temperature

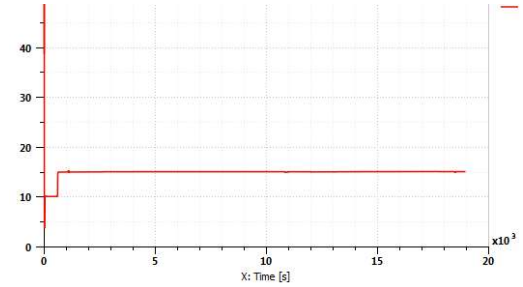

Figure 3.22: Mean Temperature

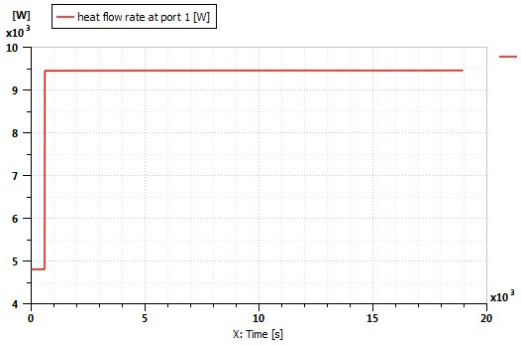

Figure 3.23: Bay Heat

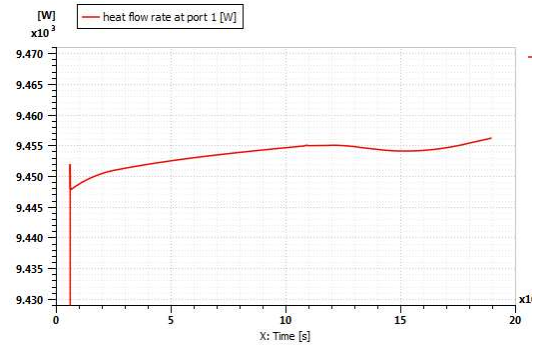

Figure 3.24: Bay Heat - Detail

3.3.2 ISA – 35

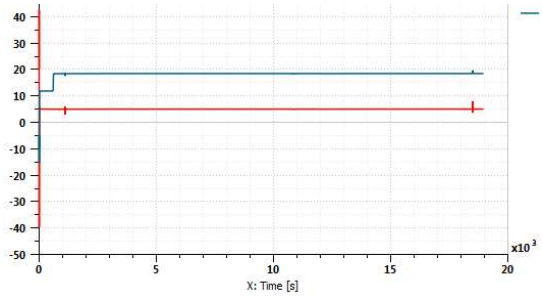

Figure 3.25: Inlet and Outlet Bay Temperature

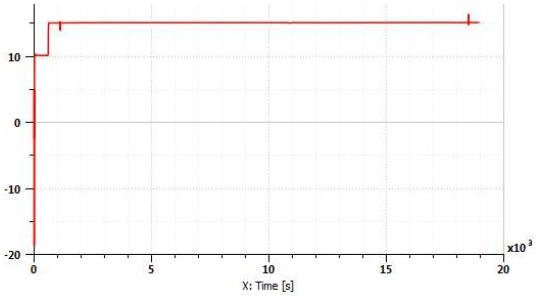

Figure 3.26: Mean Temperature

Differently from the graphics reported for the same conditions with the vapour cycle system, it is possible to notice how the avionic bay mean temperature is almost constant and equal to 15°C. This is due to the fact that the design air cycle system relies on two thermal control valves. This are controlled by the Control Unit (28) and, in the performance analysis tool scheme, are implemented using a P.I.D. whose gains have been determined with a trial and error procedure in order to obtain smooth and regular movements of the thermal control valves.

3.4 Airworthiness requirements

Dealing with the identification of the airworthiness requirements it is possible to refer to STANAG 4671 draft ed.3, "UAV Systems Airworthiness Requirements (USAR) for North Atlantic Treaty Organization (NATO) Military UAV Systems", 2014-09.

The section USAR.U1307 is indeed dedicated to Environmental Control Systems and states as cooling must be provided for equipment as required for it to meet its intended function and reliability for the intended lifetime. The airworthiness requirements that have been identified are reported in Table 3.1.

Those requirements led to the design of a back-up system (actually operated as emergency system) that, coherently with what is stated in the C requirement, is capable of cooling the avionic bay in case of a failure of the main system. This back-up system shall indeed guarantee the integrity of safety-critical avionics i.e. those related to flight controls and communications as stated in the F requirement.

With reference to the avionics equipment table reported in section 5.2.4.2 (Table 5.2 at page 92), it is possible to preliminary evaluate the heat loads generated by electronic equipment in case of a failure of the main system. Taking into account all of what has been said until know, it is possible to consider an heat load of 1.6 kW.

The back-up system chosen to cool the mentioned equipment exploits ram air. It is indeed made up of at least two air intakes, opened by dedicated actuators when the main system is shut down as a consequence of its malfunctioning. A schematization of the system at issue is reported in Figure 5.1 (page 86). It is indeed possible to notice how ram air enters the bay and, after having cooled the electric equipment, leaves the bay via the outlets. This system will be deeply described and validated in chapter 5, dedicated to the CFD analysis.

A	The ECS design shall incorporate the system safety requirements of the UAS.
B	The ECS shall meet all safety requirements when operating under installed conditions over the design envelope and maintain integration integrity to ensure the UAS safety-of-flight.
C	The UAS shall incorporate an alternate means of cooling of safety-critical avionics when the primary ECS is non-operational.
D	The ECS design (including emergency equipment and/or auxiliary methods) shall provide an acceptable pressure environment for equipment affecting safety-of-flight.
E	Normal and emergency pressurization requirements and status shall be indicated at the UCS.
F	Safety-critical items such as flight controls, avionics and communications shall function long enough to safely land the aircraft if ECS function is lost and alternate methods are not available to ensure airworthy operations.
G	ECS normal and emergency procedures shall be included in the UAS Flight Manual.
H	Adequate controls and displays for the ECS shall be installed in the UCS or other appropriate locations to allow the ECS to function as intended. Sufficient cautions, warnings, and advisories shall be provided to alert the UAS crew to problems in time for corrective action to be taken from a safety of flight perspective.
I	No single ECS subsystem failure (including UCS functions that are critical to aircraft flight safety) shall result in loss of UAS.
J	Bleed air or other compressed air duct system shall be monitored for leaks and structural integrity. Hot air leaking from damaged ducting shall not cause ignition of any flammable fluids or other materials or cause damage to safety-critical equipment. Shutdown capability, with an appropriate UCS alert, shall be provided when a potentially damaging or fire-producing leak occurs. The sensors for the leak detection system shall recover their required leak detection function following exposure to a leak.
K	The UAS thermal management system shall be stable for all flight conditions and environments. The mass flow and delivery temperature of cooling medium shall be sufficient for the aircraft heat loads and provide the necessary thermal stability to ensure safety-of-flight.

Table 3.1: Airworthiness Requirements

4 Safety Assessment

The safety assessment process provides a methodology aimed to the evaluation of the hazards associated to the functions of the aircraft, and to the design of the systems performing those functions. The analysis at issue shall indeed necessarily guarantee that all of the relevant failure conditions have been identified and that all significant combinations of failure, which could cause the cited failure conditions, have been taken in consideration. As will be deeply dealt with in the following sections, it is indeed fundamental to take into account sub-system complexities and interdependencies typical of highly integrated systems.

As reported in SAE[2] ARP4671 "G*uidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*", and showed in Figure 4.1, the described process is arranged in the following analyses:

- Functional Hazard Assessment (FHA)
- Preliminary System Safety Assessment (PSSA)
- System Safety Assessment (SSA)

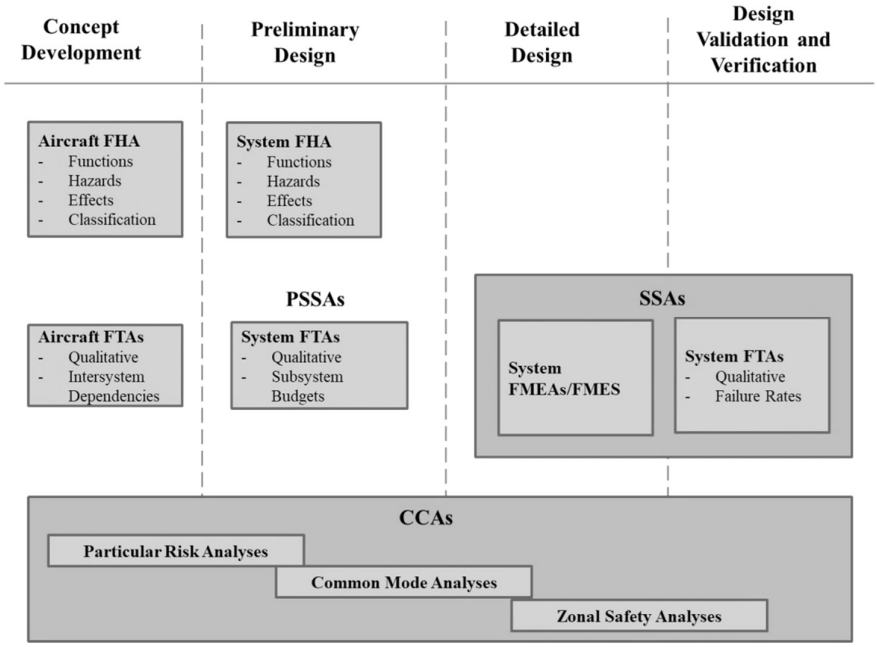

Figure 4.1: Safety Assessment Process (ref. [6])

Since the safety assessment process is undertaken in parallel with the design of the aircraft, it inherits its iterative nature. The process begins, indeed, during the concept design focusing on the related derivation of safety requirements, and it ends with the verification that the design meets the identified safety requirements.

[2] The Engineering Society For Advancing Mobility Land Sea Air and Space

As will be treated in detail in the following section, the Functional Hazard Assessment is conducted at the beginning of the design of the aircraft/subsystem at issue. It is aimed to the identification and to the classification of the failure conditions associated with the functions of the aircraft/subsystem. The output of this analysis is indeed the mentioned classification which is aimed to the establishment of the safety requirements that will be ascertained in the following phases of the system assessment process. Moreover, this phase of the process should comprehend the definition and the allocation, based on the severity classification, of the Development Assurance Level (DAL) of the function of the aircraft, and of the physical item of the subsystem.

The outcome of the FHA is indeed identifiable as the starting point for the conduction of the Preliminary System Safety Assessment (PSSA). The latter consist of a systematic approach intended to analyse the possible subsystem architectures with the aim of determining how the possible failure may cause the functional hazard that have been identified by the Functional Hazard Assessment. The PSSA is indeed used to complete the failure conditions list. In light of what has been considered, it is clear how the PSSA is a process used to validate the chosen architecture, determining if it can reasonably be expected to meet the safety objectives as defined by the FHA. The Preliminary System Safety Assessment can be performed at higher and lower levels (system, subsystem, item, software) and it is generally carried out using Fault Tree Analysis or, equivalently, Dependence Diagrams or Markov Analysis. Moreover, the PSSA should include common cause analysis. Another important outcome of the PSSA consists of the identification of several protecting strategies (e.g. partitioning, fail safe design, redundancies, built-in-test, dissimilarity, monitoring). Reflecting the entire safety process, the PSSA is highly iterative and it concurs to the allocation of risk to items, hardware and software. The outcome of this allocation will result in the determination of hardware reliability requirements and, as has already been anticipated, to the definition of DALs.

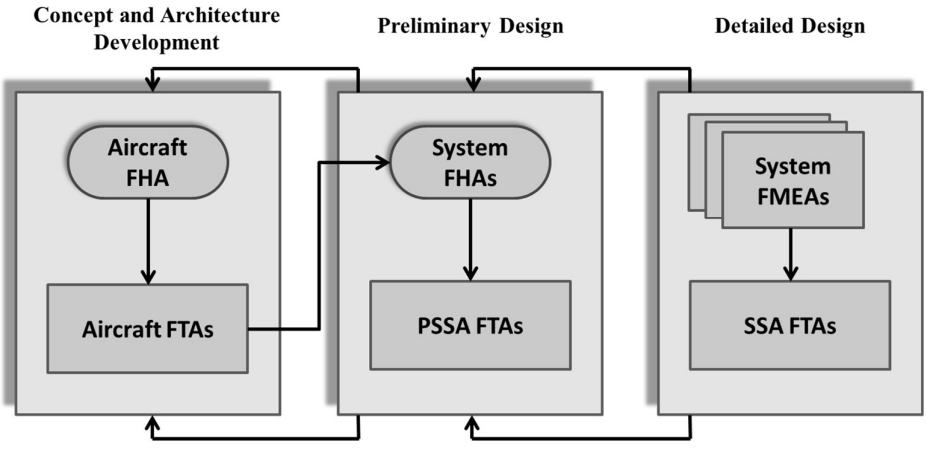

Figure 4.2: Relations Between FHAs, FTAs, FMEAs (ref. [6])

Moving to System Safety Assessment (SSA), it takes as input the PSSA FTA (or alternative method) and makes use of the quantitative results that have been obtained from the Failure Modes, Effects and Criticality Analysis (FMECA). All of these elements are computed together in order to validate the compliance of the safety objectives determined by the FHA and the

derived safety requirements from the PSSA. The SSA should also include the results obtained by the common cause analysis.

The Common Cause Analysis (CCA) is executed referring to a specific system architecture and evaluates its vulnerability to common cause events. It is indeed an analysis intended to verify that there actually exists independence between failure modes of different components. In other words, it is necessary to ensure that the risk associate with dependence is acceptably small.

Common Cause Analysis consist of three different analyses:

- Particular Risk Analysis (PRA). This analysis takes in consideration those events whose verification may violate failure independence. Moreover, these events are not specific characteristic of the system, instead they are usually external event such as fire, leaking fluids, ice, bird strike, lightning. Each of these events must be examined and risk-mitigating strategies shall be developed.
- Zonal Safety Analysis (ZSA). It is carried out focusing on all of the zones of the aircraft in order to verify that the equipment installation meets the safety requirements considering:
    - Interference Between Systems: the failure of an equipment shall not impact other subsystem or structure of the aircraft installed near to the system at issue
    - Maintenance Errors
- Common Mode Analysis (CMA). This analysis shall be carried out with the aim of verifying that those events (or conditions) that are linked with an "AND" operator in the FTAs are actually independent. Note that in this phase it is necessary to consider design, manufacturing and maintenance errors.

4.1 Functional Hazard Assessment (FHA)

The Functional Hazard Assessment has been carried out at system level, the ECS has been indeed considered. To begin with, it is necessary to identify the different function of the system. Since this has already been made as part of the functional analysis of the ECS, it is possible to refer to the obtained functions. Furthermore, in order to link the safety assessment with the functional model built in the functional analysis tool, it is convenient to refer to the identified use cases which correspond to the macro-functions of the system.

The FHA implies indeed the evaluation of the hazards linked with the total (or partial) loss of the system functions. Once that they have been identified it is indeed necessary to consider the possible mode of functional failure. The considered conditions are:

- Function loss detected
- Function loss undetected
- Function erroneous detected
- Function erroneous undetected
- Function inadvertent activation detected
- Function inadvertent activation undetected

- Function other(s) failure(s) detected
- Function other(s) failure(s) undetected

After having identified, where applicable, the mentioned conditions, it is necessary to determine the effect for every flight phase (if different) and the category of severity that needs to be considered and that determines the safety requirement objective. Moreover, the FHA implies to identify the possible contributing events and:

- Crew action
- Crew detection
- Ground detection

Dealing with the classification of the safety requirements, reference has been made to STANAG 4671 draft ed.3, "UAV Systems Airworthiness Requirements (USAR) for North Atlantic Treaty Organization (NATO) Military UAV Systems", 2014-09. The document reports indeed the following severity reference system (AMC.1309(b) – (3) – (c)), here reported in Table 4.1.

I	**Catastrophic**	Failure conditions that are expected to result in at least uncontrolled flight (including flight outside of pre-planned or contingency flight profiles/areas) and/or uncontrolled crash, Or Failure conditions which may result in a fatality to UAS crew, ground staff, or third parties.
II	**Hazardous**	Failure conditions that either by themselves or in conjunction with increased crew workload, are expected to result in a controlled-trajectory termination or forced landing potentially leading to the loss of the UAS where it can be reasonably expected that a fatality will not occur. Or Failure conditions for which it can reasonably expected that a fatality to UAS crew, ground staff or third parties will not occur.
III	**Major**	Failure conditions that either by themselves or in conjunction with increased crew workload, are expected to result in an emergency landing of the UAS on a predefined site where it can be reasonably expected that a serious injury will not occur. Or Failure conditions which could potentially result in injury to UAS crew, ground staff, or third parties.
IV	**Minor**	Failure conditions that do not significantly reduce UAS safety and involve UAS crew actions that are well within their capabilities. These conditions may include a slight reduction in safety margins or functional capabilities, and a slight increase in UAS crew workload.
V	**No Safety Effect**	Failure conditions that have no effect on safety.

Table 4.1: Severity Reference System

Note that the phrase "are expected to result in" is not intended to require 100% certainty that the effects will always be, for instance, Catastrophic. On the contrary, just because the effects of a

given failure, or combination of failures, could conceivably be Catastrophic in extreme circumstances, it is not intended to imply that the failure condition will necessarily be considered Catastrophic.

Once that the severity classification has been ascertained, it is necessary to determine a numerical safety objective that will need to be pursued in the design. It is indeed fundamental to consider the maximum probability that can be considered acceptable for the given severity classification. For this purpose, the risk reference system is extracted from the same abovementioned document (AMC.1309(b) – (4) – (c)):

Aircraft weight (MTOM)			CAT (I)	HAZ (II)	MAJ (III)	MIN (IV)	NSE (V)
	<5670 kg	>5670 kg					
Frequent	p<10e-3 FH^{-1}	p<10e-3 FH^{-1}					
Probable	p<10e-3 FH^{-1}	p<10e-3 FH^{-1}					
Remote	p<10e-4 FH^{-1}	p<10e-4 FH^{-1}					
Extremely remote	p<10e-5 FH^{-1}	p<10e-6 FH^{-1}					
Extremely improbable	p<10e-6 FH^{-1}	p<10e-7 FH^{-1}					

	Unacceptable
	Acceptable

Taking into account all of what has been said until now, it is finally possible to carry out the FHA for the ECS at issue[3]. At this purpose, the evaluation of each failure condition should take account of:

- The failure of equipment or other functions performed by the sub-system
- Performance by interfacing sub-system
- Factors external to the system
- Operating phase and flight phase of the UAV
- Exposure time
- Human factors
- Potential for dormant fault, latent or hidden failures
- Common cause failures (systemic failure)

The following pages contain the FHA for every use-case. A brief and summarized description of each macro-functionality is reported for the sake of clarity.

[3] The considered UAV has a MTOM superior to 5670 kg

UC01 Start-up. the ECS shall start up and execute an initial built in test (IBIT). This test comprehends a preliminary check-up of the correct behaviour of the sub-systems that make up the ECS (it includes, for instance, a complete opening and closing of the air intake with the aim of verifying the correct functioning of the dedicated actuator). The results shall be sent to the Central Maintenance System (CMS).

<table>
<tr><th rowspan="2">ID</th><th rowspan="2">Title</th><th rowspan="2">A/C phase(s)</th><th colspan="2">Safety requirement</th></tr>
<tr><th>Category</th><th>Objective</th></tr>
<tr><td>UC01.A</td><td>Start-up – function loss detected</td><td>GRD</td><td>NO SAFETY EFFECT</td><td>$1 \cdot 10^{-3}\ FH^{-1}$</td></tr>
<tr><td colspan="5">Consequences (effects)
Maintenance is required and mission is aborted</td></tr>
<tr><td colspan="5">IN FLIGHT (worst case condition):
Pre-flight, start-up: NOGO and mission abort

ON GROUND (worst case condition):
Ground handling: dormant failure
Servicing, maintenance: unscheduled maintenance required</td></tr>
<tr><td colspan="2">Crew detection:</td><td colspan="3">Health status alert from Utility Management System</td></tr>
<tr><td colspan="2">Crew action:</td><td colspan="3">Mission abort</td></tr>
<tr><td colspan="2">Ground detection:</td><td colspan="3">Message to Central Maintenance System</td></tr>
<tr><td colspan="5">Classification</td></tr>
<tr><td colspan="5">Mission abort prior to take-off is considered to have no safety effect</td></tr>
<tr><td colspan="5">Contributing event(s)</td></tr>
<tr><td colspan="5">Loss of electrical power supplies and/or short circuits.
Mechanical jam or F.O.D.
Erroneous maintenance.</td></tr>
<tr><td colspan="5">Remarks</td></tr>
<tr><td colspan="5"></td></tr>
</table>

<table>
<tr><th>ID</th><th>Title</th><th>A/C phase(s)</th><th colspan="2">Safety requirement</th></tr>
<tr><th></th><th></th><th></th><th>Category</th><th>Objective</th></tr>
<tr><td>UC01.B</td><td>Start-up – function loss undetected</td><td>ALL</td><td>MAJOR</td><td>$1 \cdot 10^{-4}\, FH^{-1}$</td></tr>
<tr><td colspan="5">Consequences (effects)
Loss of avionic bay temperature control. Consequent avionic over/under temperature during taxi or take-off.</td></tr>
<tr><td colspan="5">IN FLIGHT (worst case condition):
Pre-flight, start-up: loss of avionic bay temperature control

ON GROUND (worst case condition):
Ground handling, servicing, maintenance: dormant failure</td></tr>
<tr><td>Crew detection:</td><td colspan="4">Over/under temperature alert from Utility Management System</td></tr>
<tr><td>Crew action:</td><td colspan="4">Mission abort.</td></tr>
<tr><td>Ground detection:</td><td colspan="4">Message to Central Maintenance System</td></tr>
<tr><td colspan="5">Classification</td></tr>
<tr><td colspan="5">Since in a cold day (ISA-35) the over temperature condition may take place soon after take-off, this failure may result in an emergency landing of the UAV on a predefined site where it can be reasonably expected that a serious injury will not occur. The failure is then considered to be major</td></tr>
<tr><td colspan="5">Contributing event(s)</td></tr>
<tr><td colspan="5">Sensor failure.
Loss of electrical power supplies and/or short circuits.
Mechanical jam or F.O.D.
Erroneous maintenance.</td></tr>
<tr><td colspan="5">Remarks</td></tr>
<tr><td colspan="5"></td></tr>
</table>

UC02 Provide air conditioning. When the ECS is operating, its primary function is to provide the avionic bay with enough conditioned air so its temperature does not exceed the allowed ranges. In the event of an over temperature or under temperature condition, the ECS shall be able to perform two recovery, or back up, actions. These includes powering off the system and autonomously controlling the air inlet area in order to increase or decrease, when needed, the quantity of external air, warm or cold depending on climatic and flight condition, that is sent to the avionic bay. This process has to be completely autonomous since it has to be correctly executed even in case of loss of communication between the vehicle and the ground station. Moreover, in case of avionic bay temperature outside the ranges, the system shall send an alert to the Utility Management System.

ID	Title	A/C phase(s)	Safety requirement	
			Category	Objective
UC02.A	Provide air conditioning – function loss detected	All	MAJOR	$1 \cdot 10^{-4}\ FH^{-1}$

Consequences (effects)

Loss of avionic bay temperature control, mission abort

IN FLIGHT (worst case condition):

Pre-flight, start-up: NOGO and mission abort

Taxi, take-off: mission abort

Climb, cruise, descent, landing: loss of avionic bay temperature control

Switch-off, post-flight: dormant failure

ON GROUND (worst case condition):

Ground handling: dormant failure

Servicing, maintenance: unscheduled maintenance required

Crew detection:	Health status alert from Utility Management System
Crew action:	Initiate emergency procedures, shut down ECS, mission abort and immediate landing
Ground detection:	Message to Central Maintenance System

Classification

Detected loss of avionic bay temperature control is assumed to be major since the back-up system shall guarantee that bay temperature remains inside permitted values. However, the aircraft shall perform an emergency landing.

Contributing event(s)

Sensor failure.

Loss of electrical power supplies and/or short circuits.

Mechanical jam or F.O.D.

Volcanic ash

Erroneous maintenance.

Remarks

In the event of a malfunction of the system which leads to overheating or overcooling of the avionic bay it is convenient to shut down the ECS and, as a back-up system, autonomously control the air inlet area in order to increase/decrease the external air flow depending on climatic and flight condition.

ID	Title	A/C phase(s)	Safety requirement	
			Category	Objective
UC02.B	Provide air conditioning – function loss undetected	All	CATASTROPHIC	$1 \cdot 10^{-7}\, FH^{-1}$

Consequences (effects)

Erroneous avionic bay temperature control. Consequent avionics over/under temperature

IN FLIGHT (worst case condition):

Pre-flight: dormant failure

Start-up, taxi, take-off, climb, cruise, descent, landing: erroneous avionic bay temperature control
Switch-off, post-flight: dormant failure

ON GROUND (worst case condition):

Ground handling, servicing, maintenance: dormant failure

Crew detection:	Over/under temperature alert from Utility Management System
Crew action:	Initiate emergency procedures, mission abort and immediate landing
Ground detection:	Message from Central Maintenance System

Classification

Avionics over/under temperature is assumed to be catastrophic since it may lead to uncontrolled flight and/or uncontrolled crash

Contributing event(s)

Sensor failure.

Loss of electrical power supplies and/or short circuits.

Mechanical jam or F.O.D.

Volcanic ash

Erroneous maintenance.

Remarks

UC03 Monitor its health status. The system shall continuously monitor the health status of its components computing the measurements of different sensor (e.g. temperatures, pressures, rates per minute, mass flow).

<table>
<tr><th rowspan="2">ID</th><th rowspan="2">Title</th><th rowspan="2">A/C phase(s)</th><th colspan="2">Safety requirement</th></tr>
<tr><th>Category</th><th>Objective</th></tr>
<tr><td>UC03.A</td><td>Monitor its health status – function loss (any mode)</td><td>All</td><td>MINOR</td><td>$1 \cdot 10^{-3}\ FH^{-1}$</td></tr>
<tr><td colspan="5">Consequences (effects)
Slight increase in crew workload and minor reduction in safety margin.</td></tr>
<tr><td colspan="5">IN FLIGHT (worst case condition):

Pre-flight: dormant failure
Start-up, taxi, take-off, climb, cruise, descent, landing: increase in crew workload
Switch-off, post-flight: dormant failure

ON GROUND (worst case condition):

Ground handling: dormant failure
Servicing, maintenance: unscheduled maintenance required</td></tr>
<tr><td colspan="2">Crew detection:</td><td colspan="3">Unavailable health status information from Utility Management System</td></tr>
<tr><td colspan="2">Crew action:</td><td colspan="3">More frequent monitoring of avionic bay temperature</td></tr>
<tr><td colspan="2">Ground detection:</td><td colspan="3">Unavailable health status information from Central Maintenance System</td></tr>
<tr><td colspan="5">Classification</td></tr>
<tr><td colspan="5">Inability to monitor components health status leads to a minor increase in crew workload.</td></tr>
<tr><td colspan="5">Contributing event(s)</td></tr>
<tr><td colspan="5">Sensor failure.
Loss of electrical power supplies and/or short circuits.
Mechanical jam or F.O.D.
Erroneous maintenance.</td></tr>
<tr><td colspan="5">Remarks</td></tr>
<tr><td colspan="5"></td></tr>
</table>

UC04 Monitor status of air filer. The air filter is necessary since it does not allow dust to reach the electronic equipment installed in the avionic bay. When the pressure difference between the entrance and the exit of the air filter exceeds a certain range the filter is considered clogged and a message is sent to the Central Maintenance System.

ID	Title	A/C phase(s)	Safety requirement	
			Category	Objective
UC04.A	Filter clogged	All	NO SAFETY EFFECT	$1 \cdot 10^{-3}\, FH^{-1}$
Consequences (effects)				
Possible equipment damage. Unscheduled maintenance required				
IN FLIGHT (worst case condition): Pre-flight: none Start-up, taxi, take-off, climb, cruise, descent, landing: possible equipment damage Switch-off, post-flight: dormant failure **ON GROUND (worst case condition):** Ground handling: dormant failure Servicing, maintenance: unscheduled maintenance required				
Crew detection:	Slight reduction of avionic bay air flow, health status alert from UMS			
Crew action:	Initiate emergency procedure			
Ground detection:	Alert from Central Maintenance System			
Classification				
Slight reduction in air flow entering the bay may cause minor damage to the electronic equipment				
Contributing event(s)				
Mechanical jam or F.O.D. Erroneous maintenance. Sensor failure.				
Remarks				

ID	Title	A/C phase(s)	Safety requirement	
			Category	Objective
UC04.B	Filtering – function loss	All	NO SAFETY EFFECT	$1 \cdot 10^{-3}\, FH^{-1}$

Consequences (effects)

Possible equipment damage. Unscheduled maintenance required

IN FLIGHT (worst case condition):

Pre-flight: none

Start-up, taxi, take-off, climb, cruise, descent, landing: possible equipment damage

Switch-off, post-flight: dormant failure

ON GROUND (worst case condition):

Ground handling: dormant failure

Servicing, maintenance: unscheduled maintenance required

Crew detection:	Health Status alert from UMS
Crew action:	Initiate emergency procedure
Ground detection:	Alert from Central Maintenance System

Classification

Dust entering the bay may cause minor damage to the electronic equipment

Contributing event(s)

Mechanical jam or F.O.D.

Erroneous maintenance.

Sensor failure.

Remarks

UC05 Provide maintenance. When required, the system shall perform a built in test (MBIT) and send its results to the CMS.

<table>
<tr><th rowspan="2">ID</th><th rowspan="2">Title</th><th rowspan="2">A/C phase(s)</th><th colspan="2">Safety requirement</th></tr>
<tr><th>Category</th><th>Objective</th></tr>
<tr><td>UC05.A</td><td>Inability to perform MBIT</td><td>All</td><td>NO SAFETY EFFECT</td><td>$1 \cdot 10^{-3}\, FH^{-1}$</td></tr>
<tr><td colspan="5">Consequences (effects)</td></tr>
<tr><td colspan="5">Unscheduled maintenance required</td></tr>
<tr><td colspan="5">IN FLIGHT (worst case condition):

Pre-flight, taxi, take-off, climb, cruise, descent, landing: none
Switch-off, post-flight: none

ON GROUND (worst case condition):

Ground handling: dormant failure
Servicing, maintenance: unscheduled maintenance required</td></tr>
<tr><td>Crew detection:</td><td colspan="4">Unavailable MBIT</td></tr>
<tr><td>Crew action:</td><td colspan="4">-</td></tr>
<tr><td>Ground detection:</td><td colspan="4">Central Maintenance System MBIT request is not accomplished</td></tr>
<tr><td colspan="5">Classification</td></tr>
<tr><td colspan="5">The inability to perform MBIT does not has a safety effect on the flight</td></tr>
<tr><td colspan="5">Contributing event(s)</td></tr>
<tr><td colspan="5">Erroneous maintenance.
Sensor failure.</td></tr>
<tr><td colspan="5">Remarks</td></tr>
<tr><td colspan="5"></td></tr>
</table>

UC06 Shut down. In nominal functioning, the system has be powered off once the flight is ended. Moreover, it may be convenient to shut down the ECS in the event of a malfunction of the system that leads to the provision of overheated/overcooled air to the avionic bay.

<table>
<tr><th rowspan="2">ID</th><th rowspan="2">Title</th><th rowspan="2">A/C phase(s)</th><th colspan="2">Safety requirement</th></tr>
<tr><th>Category</th><th>Objective</th></tr>
<tr><td>UC06.A</td><td>Inability to shut down</td><td>All</td><td>CATASTROPHIC</td><td>$1 \cdot 10^{-7}\ FH^{-1}$</td></tr>
<tr><td colspan="5">Consequences (effects)</td></tr>
<tr><td colspan="5">Overheating/overcooling of avionic bay</td></tr>
<tr><td colspan="5">IN FLIGHT (worst case condition):

Pre-flight, taxi, take-off, climb, cruise, descent, landing: overheating/overcooling of avionic bay
Switch-off, post-flight: none

ON GROUND (worst case condition):

Ground handling: dormant failure
Servicing, maintenance: unscheduled maintenance required</td></tr>
<tr><td>Crew detection:</td><td colspan="4">Message from Utility Management System</td></tr>
<tr><td>Crew action:</td><td colspan="4">Initiate emergency procedures</td></tr>
<tr><td>Ground detection:</td><td colspan="4">Health Status alert from Central Maintenance System</td></tr>
<tr><td colspan="5">Classification</td></tr>
<tr><td colspan="5">In case of a malfunction of the system which leads to the provision of overheated/overcooled air to the avionic bay, the inability to shut down the ECS may cause destructive damage on the avionics.</td></tr>
<tr><td colspan="5">Contributing event(s)</td></tr>
<tr><td colspan="5">Sensor failure.
Loss of electrical power supplies and/or short circuits.
Mechanical jam or F.O.D.
Erroneous maintenance.</td></tr>
<tr><td colspan="5">Remarks</td></tr>
<tr><td colspan="5"></td></tr>
</table>

ID	Title	A/C phase(s)	Safety requirement	
			Category	Objective
UC06.B	Inadvertent shut down - detected	FLT	MAJOR	$1 \cdot 10^{-4}\, FH^{-1}$

Consequences (effects)

Overheating/overcooling of avionic bay

IN FLIGHT (worst case condition):

Pre-flight, taxi, take-off, climb, cruise, descent, landing: overheating/overcooling of avionic bay

Switch-off, post-flight: none

Crew detection:	Message from Utility Management System
Crew action:	Immediately start-up the system, initiate emergency procedures
Ground detection:	Health Status alert from Central Maintenance System

Classification

The temporary inadvertent deactivation of avionic bay conditioning may lead to over/under temperature. Increase in crew workload.

Contributing event(s)

Sensor failure.

Loss of electrical power supplies and/or short circuits.

Remarks

ID	Title	A/C phase(s)	Safety requirement	
			Category	Objective
UC06.C	Inadvertent shut down - undetected	FLT	HAZARDOUS	$1 \cdot 10^{-6}\, FH^{-1}$
Consequences (effects)				
Overheating/overcooling of avionic bay				
IN FLIGHT (worst case condition): Pre-flight, taxi, take-off, climb, cruise, descent, landing: overheating/overcooling of avionic bay Switch-off, post-flight: none				
Crew detection:	Over/under temperature alert from Utility Management System			
Crew action:	Immediate start-up the system, initiate emergency procedures			
Ground detection:	Health Status alert from Central Maintenance System			
Classification				
The inadvertent and undetected shut down of the ECS may lead to avionic over/under temperature which may cause destructive damage on the avionics.				
Contributing event(s)				
Sensor failure. Loss of electrical power supplies and/or short circuits.				
Remarks				

4.1.1 MBSE approach

In parallel with the traditional FHA approach, whose outcome is reported in the previous section, the FHA has been conducted adopting the methodologies of Model Based System Engineering. The reason behind this process is imputable to the search for completeness and objectivity: the MBSE approach provides the safety analyst with a systematic method which is able to increase the reliability and the accuracy of the Functional Hazard Assessment.

The considered approach makes use of the functional model built in the adopted functional analysis tool according to IBM Harmony methodology and consist of the following steps:

1. Identification of every action reported in the activity diagram of every use-case
2. Definition, for every action identified, of the following functional failure modes:

- Function loss detected
- Function loss undetected
- Function erroneous detected
- Function erroneous undetected
- Function inadvertent activation detected
- Function inadvertent activation undetected
- Function other(s) failure(s) detected
- Function other(s) failure(s) undetected

3. Definition, for every functional failure mode of every action of the following characteristics:
   - Severity
   - Effect
   - Crew detection
   - Crew action
   - Ground detection
   - Contributing events
   - Remarks
4. Extraction of the worst case, based on severity, for every use-case

The outcome of this procedure shall correspond with the outcome of the traditional FHA. Moreover, this allows the safety analyst to directly make use of the functional analysis carried out by other designers, simplifying and optimizing the overall design process of a new aircraft.

To begin with step 1, it is possible to consider, as an example, the activity diagram of the use case *Monitor Status of Air Filter*, reported in Figure 4.3. Every action present in this specific diagram needs to be examined according to the methodology of the FHA. This means that it is necessary to define the functional failure modes (step 2) for every action identified (step 1) and finally determine the characteristic reported in step 3. This process needs to be executed for every activity diagram of every use case so to analyse all of the actions of the system.

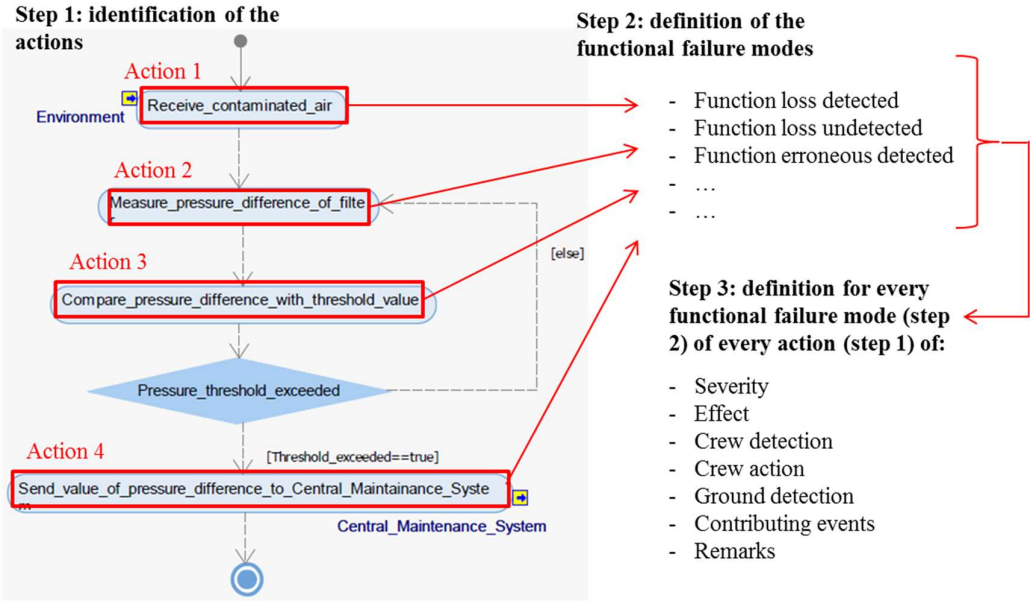

Figure 4.3: FHA MBSE approach

Dealing specifically with the procedure just described, it is possible to define, in the functional analysis tool , a new Stereotype, named “FailStereotype”, endowed with seven tags containing the abovementioned information related to safety (Severity, Effect, Crew detection, Crew action, Ground detection, Contributing events, Remarks). Subsequently, it is necessary to define a series of events named as the abovementioned failure modes (Function loss detected,

Function loss undetected, Function erroneous detected, Function erroneous undetected, Function inadvertent activation detected, Function inadvertent activation undetected, Function other(s) failure(s) detected, Function other(s) failure(s) undetected).

At this point, it is possible to build a Failure Matrix (Figure 4.4) reporting the just defined events on the rows and the actions (from activity diagrams) on the columns. It is then possible to create, for every action related to every cited event, the relative FailStereotype.

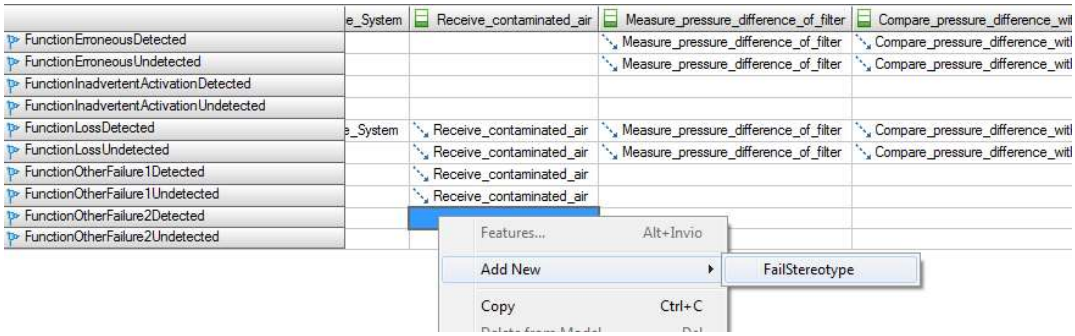

Figure 4.4: Failure Matrix

FunctionalAnalysisPkg	
FailStereotype	
ContributingEvents	Sensor failure.Loss of electrical power supplies and/or short circuits.Mechanical jam or F.O.D.Volcanic ashErroneous maintenance.
CrewAction	Initiate emergency procedures, mission abort and immediate landing
CrewDetection	Over/under temperature alert from UMS
Effect	Loss of avionic bay temperature control. Consequent avionics over/under temperature
GroundDetection	Message from CMS
Remarks	
Severity	Catastrophic
UC	UC02 Provide air conditioning

Figure 4.5: Fail Stereotype – Tags

The previous two pictures (Figure 4.4 and Figure 4.5) report, respectively, the failure matrix used to create the fail stereotype for each couple action-event, and the tool that allows the definition of the mentioned tags.

The next step is the creation of a new table containing the obtained FHA: it is generated autonomously by the functional analysis tool once that the failure matrix has been completely filled (where applicable). The layout of this table has been obtained recurring to the property "context pattern".

The result has been exported in Excel and it is reported below in Table 4.2. The functional failure modes are identified by the following acronyms:

Function loss detected:	LD	Function loss undetected:	LU
Function erroneous detected:	ED	Function erroneous undetected:	EU
Function inadvertent activation detected:	IAD	Function inadvertent activation undetected:	IAU
Function other(s) failure(s) detected:	OFD	Function other(s) failure(s) undetected:	OFU

Function	Fail	Severity	Effect	Crew Detection	Crew Action	Ground Detection	Contributing Events	Remarks
UC01 Start up								
Send IBIT result to Central Maintenance System	LD	**NSE**	Uncertainty on the initial health status of the system	Health status alert from UMS	Mission abort	Message from CMS	Loss of electrical power supplies and/or short circuits Sensor failure Erroneous maintenance	
Receive command to start up	LD	**NSE**	NOGO and mission abort	Health status alert from UMS	Mission abort	Message from CMS	Loss of electrical power supplies and/or short circuits Sensor failure Erroneous maintenance	
Receive command to start up	LD	**MAJ**	Inability to start-up the ECS. Consequent loss of avionic bay temperature control and avionic over/under temperature during taxi or take-off	Over/under temperature alert from UMS	Mission abort	Message from CMS	Loss of electrical power supplies and/or short circuits Sensor failure Erroneous maintenance	
Perform IBIT	LD	**NSE**	Uncertainty on the initial health status of the system	Health status alert from UMS	Mission abort	Message from CMS	Loss of electrical power supplies and/or short circuits Sensor failure Erroneous maintenance	
Send IBIT result to Central Maintenance System	LU	**MIN**	Uncertainty on the initial health status of the system	-	-	Unavailable IBIT	Loss of electrical power supplies and/or short circuits Sensor failure Erroneous maintenance	
Receive request for MBIT	IAD	**NSE**	-	-	-	-	Sensor failure	
Receive request for MBIT	IAU	**NSE**	-	-	-	-	Sensor failure	
Perform IBIT	LD	**MIN**	Uncertainty on the initial health status of the system	-	-	Unavailable IBIT	Loss of electrical power supplies and/or short circuits Sensor failure Erroneous maintenance	
UC02 Provide air conditioning								
Send an alert to Utility Management System	ED	**NSE**	-	health status alert from UMS	-	Alert from CMS	Sensor failure. Loss of electrical power supplies and/or short circuits. Erroneous maintenance.	Erroneous over/under temperature alert
Send an alert to Utility Management System	EU	**MIN**	Increase in crew workload	Health status alert from UMS	Health status data cross check	Alert from CMS	Sensor failure. Loss of electrical power supplies and/or short circuits. Erroneous maintenance.	Undetected erroneous over/under temperature alert
Send an alert to Utility Management System	LD	**MIN**	Increase in crew workload	Health status alert from UMS	More frequent monitoring of avionic bay temperature	Alert from CMS	Sensor failure. Loss of electrical power supplies and/or short circuits. Erroneous maintenance.	
Send an alert to Utility Management System	LU	**HAZ**	Possible avionic malfunctioning in case of unreported over/under temperature	Avionic malfunctioning, health status data cross check	Initiate emergency procedures	Alert from CMS	Sensor failure. Loss of electrical power supplies and/or short circuits. Erroneous maintenance.	In case of an over/under temperature, the system will not send an alert, hence the over/under temperature will be undetected
Send air conditioned to the bay	ED	**HAZ**	Erroneous avionic bay temperature control. Consequent avionics over/under temperature	Health Status alert from UMS	Initiate emergency procedures shut down ECS, mission abort and immediate landing	Message from CMS	Sensor failure. Loss of electrical power supplies and/or short circuits. Mechanical jam or F.O.D. Erroneous maintenance.	
Send air conditioned to the bay	EU	**CAT**	Avionics over/under temperature	Over/under temperature alert from UMS	Initiate emergency procedures shut down ECS, mission abort and immediate landing	Message from CMS	Sensor failure. Loss of electrical power supplies and/or short circuits. Mechanical jam or F.O.D. Erroneous maintenance.	
Send air conditioned	LD	**HAZ**	Loss of avionic bay temperature control.	Health status alert	Initiate emergency	Message from	Sensor failure. Loss of electrical power supplies	

to the bay			Consequent possible avionics over/under temperature	from UMS	procedures, mission abort	CMS	and/or short circuits. Mechanical jam or F.O.D. Volcanic ash Erroneous maintenance.	
Send air conditioned to the bay	LU	**CAT**	Loss of avionic bay temperature control. Consequent avionics over/under temperature	Over/under temperature alert from UMS	Initiate emergency procedure, mission abort and immediate landing	Message from CMS	Sensor failure. Loss of electrical power supplies and/or short circuits. Mechanical jam or F.O.D. Volcanic ash Erroneous maintenance.	
Receive command to increase or decrease air inlet area	ED	**HAZ**	Back-up cooling may be insufficient, consequent possible avionics over temperature	Health status message from UMS	Initiate emergency procedures, mission abort and immediate landing	Alert from CMS	Sensor failure. Loss of electrical power supplies and/or short circuits. Mechanical jam or F.O.D. Volcanic ash Erroneous maintenance.	In case of a malfunctioning of both main and back-up cooling system the avionic bay temperature will inevitably exceed the allowed limits
Receive command to increase or decrease air inlet area	EU	**HAZ**	Back-up cooling may be insufficient, consequent possible avionics over temperature	Avionics malfunctioning	Initiate emergency procedures, mission abort and immediate landing	Alert from CMS	Sensor failure. Loss of electrical power supplies and/or short circuits. Mechanical jam or F.O.D. Volcanic ash Erroneous maintenance.	In case of a malfunctioning of both main and back-up cooling system the avionic bay temperature will inevitably exceed the allowed limits
Receive command to increase or decrease air inlet area	IAD	**MIN**	Unscheduled maintenance required	Health status alert from UMS	-	Alert from CMS	Sensor failure. Loss of electrical power supplies and/or short circuits. Mechanical jam or F.O.D. Volcanic ash Erroneous maintenance.	
Receive command to increase or decrease air inlet area	IAD	**MIN**	Unscheduled maintenance required	Health status alert from UMS	-	Alert from CMS	Sensor failure. Loss of electrical power supplies and/or short circuits. Mechanical jam or F.O.D. Volcanic ash Erroneous maintenance.	
Receive command to increase or decrease air inlet area	LD	**CAT**	Back-up cooling unavailable, avionics over temperature	Health status message from UMS	Initiate emergency procedures, mission abort and immediate landing	Alert from CMS	Sensor failure. Loss of electrical power supplies and/or short circuits. Mechanical jam or F.O.D. Volcanic ash Erroneous maintenance.	In case of a malfunctioning of both main and back-up cooling system the avionic bay temperature will inevitably exceed the allowed limits
Receive command to increase or decrease air inlet area	LU	**CAT**	Back-up cooling unavailable, avionics over temperature	Avionics malfunctioning	Initiate emergency procedures, mission abort and immediate landing	Alert from CMS	Sensor failure. Loss of electrical power supplies and/or short circuits. Mechanical jam or F.O.D. Volcanic ash Erroneous maintenance.	In case of a malfunctioning of both main and back-up cooling system the avionic bay temperature will inevitably exceed the allowed limits
Measure of bay temperature	ED	**MAJ**	Loss of avionic bay temperature control. Consequent possible avionics over/under temperature	Health status alert from UMS	Initiate emergency procedures	Alert from CMS	Sensor failure. Loss of electrical power supplies and/or short circuits. Erroneous maintenance.	
Measure of bay temperature	EU	**HAZ**	Loss of avionic bay temperature control. Consequent avionics over/under temperature	Over/under temperature alert from UMS	Initiate emergency procedures	Alert from CMS	Sensor failure. Loss of electrical power supplies and/or short circuits. Erroneous maintenance.	Erroneous measurements, in particular if undetected, may lead to over/under temperature
Measure of bay temperature	LD	**MAJ**	Uncertainty on avionic bay temperature	Health status alert from UMS	Initiate emergency procedures	Message from CMS	Sensor failure. Loss of electrical power supplies and/or short circuits. Erroneous maintenance.	
Increase or decrease	LD	**HAZ**		Health status from	-		Sensor failure. Loss of	The inlet area variation is a back-

air inlet area				UMS			electrical power supplies and/or short circuits. Mechanical jam or F.O.D. Erroneous maintenance.	up system in case of a failure of the main cooling/heating system. The erroneous control of the area may lead to over/under temperature condition
Compare with threshold values	ED	**MAJ**	Loss of avionic bay temperature control. Consequent possible avionics over/under temperature	Health status alert from UMS	Initiate emergency procedures	Alert from CMS	Sensor failure. Loss of electrical power supplies and/or short circuits. Erroneous maintenance.	
Compare with threshold values	EU	**HAZ**	Loss of avionic bay temperature control. Consequent avionics over/under temperature	Over/under temperature alert from UMS	Initiate emergency procedures	Alert from CMS	Sensor failure. Loss of electrical power supplies and/or short circuits. Erroneous maintenance.	Erroneous comparison, in particular if undetected, may lead to over/under temperature
Compare with threshold values	LD	**MAJ**	Uncertainty on avionic bay temperature	Health status alert from UMS	Initiate emergency procedures	Uncertainty on avionic bay temperature	Sensor failure. Loss of electrical power supplies and/or short circuits. Erroneous maintenance.	

UC03 Monitor its health status

Send data to Utility Management System	ED	**MIN**	Minor reduction in safety margin	Unavailable health status information from UMS	More frequent monitoring of avionic bay temperature	Unavailable health status information from CMS	Sensor failure Loss of electrical power supplies and/or short circuits Mechanical jam or F.O.D. Erroneous maintenance	
Send data to Utility Management System	EU	**MIN**	Minor reduction in safety margin	Unavailable health status information from UMS	More frequent monitoring of avionic bay temperature	Unavailable health status information from CMS	Sensor failure Loss of electrical power supplies and/or short circuits Mechanical jam or F.O.D. Erroneous maintenance	
Send data to Utility Management System	LD	**MIN**	Minor reduction in safety margin	Unavailable health status information from UMS	More frequent monitoring of avionic bay temperature	Unavailable health status information from CMS	Sensor failure Loss of electrical power supplies and/or short circuits Mechanical jam or F.O.D. Erroneous maintenance	
Send data to Utility Management System	LU	**MIN**	Minor reduction in safety margin	Unavailable health status information from UMS	More frequent monitoring of avionic bay temperature	Unavailable health status information from CMS	Sensor failure Loss of electrical power supplies and/or short circuits Mechanical jam or F.O.D. Erroneous maintenance	
Send data to Central Maintenance System	ED	**MIN**	Minor reduction in safety margin	Unavailable health status information from UMS	More frequent monitoring of avionic bay temperature	Unavailable health status information from CMS	Sensor failure Loss of electrical power supplies and/or short circuits Mechanical jam or F.O.D. Erroneous maintenance	
Send data to Central Maintenance System	EU	**MIN**	Minor reduction in safety margin	Unavailable health status information from UMS	More frequent monitoring of avionic bay temperature	Unavailable health status information from CMS	Sensor failure Loss of electrical power supplies and/or short circuits Mechanical jam or F.O.D. Erroneous maintenance	
Send data to Central Maintenance System	LD	**MIN**	Minor reduction in safety margin	Unavailable health status information from UMS	More frequent monitoring of	Unavailable health status	Sensor failure Loss of electrical power supplies and/or short circuits Mechanical jam or F.O.D. Erroneous maintenance	

					avionic bay temperatur e	informat ion from CMS	
Send data to Central Maintenanc e System	LU	**MIN**	Minor reduction in safety margin	Unavailable health status information from UMS	More frequent monitorin g of avionic bay temperatur e	Unavail able health status informat ion from CMS	Sensor failure Loss of electrical power supplies and/or short circuits Mechanical jam or F.O.D. Erroneous maintenance
Measure data of its health status	ED	**MIN**	Minor reduction in safety margin	Unavailable health status information from UMS	More frequent monitorin g of avionic bay temperatur e	Unavail able health status informat ion from CMS	Sensor failure Loss of electrical power supplies and/or short circuits Mechanical jam or F.O.D. Erroneous maintenance
Measure data of its health status	EU	**MIN**	Minor reduction in safety margin	Unavailable health status information from UMS	More frequent monitorin g of avionic bay temperatur e	Unavail able health status informat ion from CMS	Sensor failure Loss of electrical power supplies and/or short circuits Mechanical jam or F.O.D. Erroneous maintenance
Measure data of its health status	LD	**MIN**	Minor reduction in safety margin	Unavailable health status information from UMS	More frequent monitorin g of avionic bay temperatur e	Unavail able health status informat ion from CMS	Sensor failure Loss of electrical power supplies and/or short circuits Mechanical jam or F.O.D. Erroneous maintenance
Measure data of its health status	LU	**MIN**	Minor reduction in safety margin	Unavailable health status information from UMS	More frequent monitorin g of avionic bay temperatur e	Unavail able health status informat ion from CMS	Sensor failure Loss of electrical power supplies and/or short circuits Mechanical jam or F.O.D. Erroneous maintenance
UC04 Monitor status of air filer							
Send value of pressure difference to Central Maintenanc e System	ED	**NSE**	Uncertainty on air filter health status	-	-	Alert from CMS	Loss of electrical power supplies and/or short circuits Sensor failure Erroneous maintenance
Send value of pressure difference to Central Maintenanc e System	EU	**NSE**	Uncertainty on air filter health status	-	-	Alert from CMS	Loss of electrical power supplies and/or short circuits Sensor failure Erroneous maintenance
Send value of pressure difference to Central Maintenanc e System	LD	**NSE**	Uncertainty on air filter health status	-	-	Alert from CMS	Loss of electrical power supplies and/or short circuits Sensor failure Erroneous maintenance
Send value of pressure difference to Central Maintenanc e System	LD	**NSE**	Uncertainty on air filter health status	-	-	Alert from CMS	Loss of electrical power supplies and/or short circuits Sensor failure Erroneous maintenance
Receive contaminat ed air	LD	**NSE**	Possible equipment damage. Unscheduled maintenance required	Health status alert from CMS	-	Alert from CMS	Mechanical jam or F.O.D. Sensor failure Erroneous maintenance Dust entering the bay may cause minor damage to electronic equipment
Receive contaminat ed air	LU	**NSE**	Possible equipment damage. Unscheduled maintenance required	-	-	Alert from CMS	Mechanical jam or F.O.D. Sensor failure Erroneous maintenance
Receive contaminat ed air	OF D	**NSE**	Slight reduction in air flow entering the bay may cause minor damage to the electronic equipment. Unscheduled maintenance	Health status alert from CMS	-	Alert from CMS	Mechanical jam or F.O.D. Sensor failure Erroneous maintenance Filter clogged - detected

			required					
Receive contaminated air	OFU	**NSE**	Slight reduction in air flow entering the bay may cause minor damage to the electronic equipment. Unscheduled maintenance required	Health status alert from UMS	-	Alert from CMS	Mechanical jam or F.O.D. Sensor failure Erroneous maintenance	Filter clogged - undetected
Measure pressure difference of filter	ED	**NSE**	Uncertainty on air filter health status	-	-	Alert from CMS	Loss of electrical power supplies and/or short circuits Sensor failure Erroneous maintenance	
Measure pressure difference of filter	EU	**NSE**	Uncertainty on air filter health status	-	-	Alert from CMS	Loss of electrical power supplies and/or short circuits Sensor failure Erroneous maintenance	
Measure pressure difference of filter	LD	**NSE**	Uncertainty on air filter health status	-	-	Alert from CMS	Loss of electrical power supplies and/or short circuits Sensor failure Erroneous maintenance	
Measure pressure difference of filter	LU	**NSE**	Uncertainty on air filter health status	-	-	Alert from CMS	Loss of electrical power supplies and/or short circuits Sensor failure Erroneous maintenance	
Compare pressure difference with threshold value	ED	**NSE**	Uncertainty on air filter health status	-	-	Alert from CMS	Loss of electrical power supplies and/or short circuits Sensor failure Erroneous maintenance	
Compare pressure difference with threshold value	EU	**NSE**	Uncertainty on air filter health status	-	-	Alert from CMS	Loss of electrical power supplies and/or short circuits Sensor failure Erroneous maintenance	
Compare pressure difference with threshold value	LD	**NSE**	Uncertainty on air filter health status	-	-	Alert from CMS	Loss of electrical power supplies and/or short circuits Sensor failure Erroneous maintenance	
Compare pressure difference with threshold value	LU	**NSE**	Uncertainty on air filter health status	-	-	Alert from CMS	Loss of electrical power supplies and/or short circuits Sensor failure Erroneous maintenance	

UC05 Provide maintenance

Send MBIT result to Central Maintenance System	LD	**NSE**	Unscheduled maintenance required	Unavailable MBIT	-	CMS MBIT request is not accomplished	Loss of electrical power supplies and/or short circuits Sensor failure Erroneous maintenance	
Receive request for MBIT	LD	**NSE**	Unscheduled maintenance required	Unavailable MBIT	-	CMS MBIT request is not accomplished	Loss of electrical power supplies and/or short circuits Sensor failure Erroneous maintenance	
Perform MBIT	LD	**NSE**	Unscheduled maintenance required	Unavailable MBIT	-	CMS MBIT request is not accomplished	Loss of electrical power supplies and/or short circuits Sensor failure Erroneous maintenance	

UC06 Shut down

System power off	IAF	**MAJ**	Overheating/overcooling of avionic bay	Message from UMS	Immediately start-up of the system, initiate emergency procedures	Health status alert from CMS	Sensor failure. Loss of electrical power supplies and/or short circuits.	The temporary inadvertent deactivation of avionic bay conditioning may lead to over/under temperature. Increase in crew workload.
System power off	IAU	**HAZ**	Overheating/overcooling of avionic bay	Over/under temperature alert from UMS	Immediately start-up the system, initiate emergency procedures	Health status alert from CMS	Sensor failure. Loss of electrical power supplies and/or short circuits.	The inadvertent and undetected shut down of the ECS may lead to avionic over/under temperature which may cause destructive damage on the avionics.
System power	LD	**HAZ**	Overheating/overcooling of avionic bay	Message from	Initiate emergency procedures	Health status alert	Sensor failure. Loss of	In case of a malfunction of the

off				UMS		from CMS	electrical power supplies and/or short circuits. Mechanical jam or F.O.D. Erroneous maintenance.	system which leads to the provision of overheated/overcooled air to the avionic bay, the inability to shut down the ECS may cause destructive damage on the avionics.
Command to shut down	IAD	**MAJ**	Overheating/overcooling of avionic bay	Message from UMS	Immediately start-up of the system, initiate emergency procedures	Health status alert from CMS	Sensor failure. Loss of electrical power supplies and/or short circuits.	The temporary inadvertent deactivation of avionic bay conditioning may lead to over/under temperature. Increase in crew workload.
Command to shut down	IAU	**HAZ**	Overheating/overcooling of avionic bay	Over/under temperature alert from UMS	Immediately start-up the system, initiate emergency procedures	Health status alert from CMS	Sensor failure. Loss of electrical power supplies and/or short circuits.	The inadvertent and undetected shut down of the ECS may lead to avionic over/under temperature which may cause destructive damage on the avionics.
Command to shut down	LD	**HAZ**	Overheating/overcooling of avionic bay	Message from UMS	Initiate emergency procedures	Health status alert from CMS	Sensor failure. Loss of electrical power supplies and/or short circuits. Mechanical jam or F.O.D. Erroneous maintenance.	In case of a malfunction of the system which leads to the provision of overheated/overcooled air to the avionic bay, the inability to shut down the ECS may cause destructive damage on the avionics.
System power off	LU	**CAT**	Overheating/overcooling of avionic bay	Over/under temperature alert from UMS	Initiate emergency procedures	Message from CMS	Sensor failure. Loss of electrical power supplies and/or short circuits. Mechanical jam or F.O.D. Erroneous maintenance.	In case of a malfunction of the system which leads to the provision of overheated/overcooled air to the avionic bay, the inability to shut down the ECS may cause destructive damage on the avionics.
Command to shut down	LU	**CAT**	Overheating/overcooling of avionic bay	Over/under temperature alert from UMS	Initiate emergency procedures	Message from CMS	Sensor failure. Loss of electrical power supplies and/or short circuits. Mechanical jam or F.O.D. Erroneous maintenance.	In case of a malfunction of the system which leads to the provision of overheated/overcooled air to the avionic bay, the inability to shut down the ECS may cause destructive damage on the avionics.

Table 4.2: FHA – MBSE approach

Taking all of this into account, it is possible to verify how the safety requirements deriving from the traditional FHA correspond to the worst case, for every use-case, determined with the MBSE approach thanks to Table 4.2.

4.1.2 Development Assurance Level (DAL)

As can be summarized from SAE ARP4754A, the Development Assurance Level measures the level of rigorousness that is guaranteed in the development process. This is particularly useful to ensure an acceptable level of safety since a high value of DAL minimizes the development errors. In addition to that, it is fundamental to underline how the Development Assurance Level of a function of an aircraft is not limited to the function itself, but also regards the development of the interfaces between functions/items.

The assignment of the DAL is carried out basing on the results of the FHA: higher severity conditions shall require higher Development Assurance Levels. At this purpose, it is possible to refer to the following correspondence:

Severity	FDAL
CAT	A
HAZ	B
MAJ	C
MIN	D
NSE	E

Table 4.3: Severity and FDAL

Specifically, the FHA is used to determine the FDAL (Functional Development Assurance Level) as part of the Preliminary System Safety Assessment process. The Model Based System Engineering approach appeared to be particularly useful in this phase since the use-cases, representing the macro-functions of the subsystems, have been deeply developed in the functional analysis. As has already been explained in the dedicated chapter, every use-case has indeed been used to identify a specific activity diagram. The latter contains the sub-functions, or actions, which are allocated to the physical item (or group of items) that carries out that action. This functional/physical decomposition is perfectly suitable to the assignment of Development Assurance Levels: the FDAL are assigned to the sub-function making up the activity diagrams. Subsequently, it is possible to use the functional analysis tool to autonomously assign Item Development Assurance Level (IDAL) considering the items which execute the relative action. The outcome of this process is exported in Excel and is reported in Table 4.4.

Sub-function	**Item**	**FDAL**
Command to shut down	Control Unit: Supply subunit	A
Compare pressure difference with threshold value	Control Unit: Elaboration subunit	E
Compare with threshold values	Control Unit: Elaboration subunit	B
Increase or decrease air inlet area	Back-up System	B
Measure data of its health status	Sensors	D
Measure of bay temperature	Sensors	B
Measure pressure difference of filter	Sensors	E
Perform IBIT	Control Unit: Elaboration subunit	D
Perform MBIT	Control Unit: Elaboration subunit	E
Receive command to increase or decrease air inlet area	Control Unit: Communications subunit	A
Receive command to start up	Control Unit: Communications subunit	C
Receive contaminated air	Filter	E
Receive request for MBIT	Control Unit: Communications subunit	E
Send air conditioned to the bay	Main system	A

Send an alert to Utility Management System	Control Unit: Communications subunit	B
Send data to Central Maintenance System	Control Unit: Communications subunit	D
Send data to Utility Management System	Control Unit: Communications subunit	D
Send IBIT result to Central Maintenance System	Control Unit: Communications subunit	D
Send MBIT result to Central Maintenance System	Control Unit: Communications subunit	E
Send value of pressure difference to Central Maintenance System	Control Unit: Communications subunit	E
System power off	Control Unit: Supply subunit	A

Table 4.4: FDAL Allocation

At this point it is possible to determine the IDAL basing on the highest item-associated requirement listed in the table above. The result is reported in Table 4.5.

Item		IDAL
Control Unit	Supply subunit	A
	Elaboration subunit	A
	Communications subunit	A
Conditioning equipment	Main system	A
	Back-up System	B
	Sensors	B
	Filter	E

Table 4.5: IDAL Allocation

4.2 Failure Modes, Effects and Criticality Analysis (FMECA)

Failure Modes, Effects and Criticality Analysis (FMECA) is a systematic, bottom up process intended to identify the failure modes of the system at issue. Moreover, it is fundamental to determine the effects on the next higher level and the end effect, and to classify the consequences for every considered failure. This analysis can be undertaken at different design level (system, aircraft, subsystem, item, component, software). Specifically, we will consider all of the components making up the two different possible architectures (air cycle and vapour cycle) of ECS and their failure effect on the ECS (next higher level) and on the aircraft (end effect). The outcome of the conducted FMECA will be used to support the subsequent FTAs since it provides a complete list of failure modes and their relative failure rates.

Once the FMECA has been completely carried out, it is possible to perform the Failure Modes and Effects Summary. It consists of a reorganization of the failure modes identified thanks to the FMECA. Specifically, it appears to be convenient to group the failure modes that concurs to the same end effect.

4.2.1 Air Cycle System FMECA

Table 4.6 reports the FMECA that has been carried out with reference to the Air Cycle System architecture that has been already described in the dedicated chapter.

Item Name	*FMI*	*FR_{tot}*	*FR_{fmi}*	*$FR_{\%}$*	*FM Description*	*Next Higher Effect*	*End Effect*	*Severity*
PRV/ SOV	1.1	1,75e -05	3,50e-06	20%	PRV Full Open	Unregulated Air Pressure, Consequent Shut-Off and Inoperative ECS	Loss of Air Conditioning. Loss of Pneumatic Air.	MAJ
	1.2		3,50E-06	20%	PRV Partially Closed	Bleed Air Flow Reduction	Possible Insufficient Air Conditioning.	MAJ
	1.3		3,50E-06	20%	PRV Full Closed	Unavailable Bleed Air, Consequent Inoperative ECS	Loss of Air Conditioning. Loss of Pneumatic Air.	HAZ
	1.4		3,50E-06	20%	SOV Full Open	Inability to Shut-Off	Avionic Damage in The Event of Overheated Air Flow	HAZ
	1.5		3,50E-06	20%	SOV Full Closed	Unavailable Bleed Air, Consequent Inoperative ECS	Loss of Air Conditioning. Loss of Pneumatic Air.	HAZ
Pre-Cooler TCV	2.1	4,30 E-05	1,43E-05	33%	Full Closed	Loss of Temperature Control at Pre-Cooler Exit	Possible Avionics Overcooling	MIN
	2.2		1,43E-05	33%	Full Open	Over-Temperature at Pre-Cooler Exit	Possible Avionics Overheating	MAJ
	2.3		1,43E-05	33%	Minor Leakage	Inter-Cooler Performance Reduction	None	MIN
Pre-Cooler	3.1	6,70 E-06	3,35E-06	50%	Minor Air Leakage	Slight Reduction in Air Flow	None	MIN
	3.2		3,35E-06	50%	Sever Air Leakage	Unavailable Bleed Air, Consequent Inoperative ECS	Possible Fire and Components Damage	CAT
Pre-Cooler Outlet Temperature Sensor	4.1	9,90 E -07	3,30E-07	33%	Unavailable Measurement	Loss of Temperature Control at Pre-Cooler Exit	Avionics Overcooling	MIN
	4.2		3,30E -07	33%	Erroneous Over-Temperature Measurement	Loss of Temperature Control at Pre-Cooler Exit	Possible Avionics Overcooling	MIN
	4.3		3,30E -07	33%	Erroneous Under-Temperature Measurement	Loss of Temperature Control at Pre-Cooler Exit	Un-Protection from Over-Temperature	MAJ
Bleed Air Pressure Sensor	26.1	8,60 E-07	2,87E-07	33%	Unavailable Measurement	Unregulated Air Pressure	Possible Avionics Overheating and Component Damage	MAJ
	26.2		2,87E-07	33%	Erroneous Overpressure Measurement	SOV Closure (Automatic Back-Up Action)	Loss of Air Conditioning. Loss of Pneumatic Air.	HAZ
	26.3		2,87E-07	33%	Erroneous Under-Pressure Measurement	None	Un-Protection from Overpressure	MAJ
Intercooler	8.1	6,70 E-06	3,35E-06	50%	Minor Air Leakage	Slight Reduction in Air Flow	Possible Avionics Overheating	MAJ
	8.2		3,35E-06	50%	Sever Air Leakage	Unavailable Bleed Air, Consequent Inoperative ECS	Loss of Air Conditioning.	HAZ
Turbine Inlet Water Separator	11.1	2,10 E-06	1,05E-06	50%	Insufficient Water Separation	Reduction in Inter-Cooler Efficiency	Possible Injection of Liquid Water In Avionic Bay	MIN
	11.2		1,05E-06	50%	Air Leakage	Cooling Performance Reduction	Possible Avionics Overheating	MAJ
Cold Air	12.1	2,70e	5,94e-06	22%	Mechanical Jam	Sever Air Flow Reduction, Insufficient	Avionics Overheating	HAZ

Unit		-05				Cooling		
	12.2		1,08E-06	4%	Explosion	Severe Over-Temperature	Avionics Overheating, Possible Fire	CAT
	12.3		9,72E-06	36%	Air Leakage	Sever Air Flow Reduction, Insufficient Cooling	Possible Avionics Overheating	MAJ
	12.4		1,03E-05	38%	Oil Leakage	Unavailable Shaft Lubrication	Oil Contamination	MIN
Avionic Bay Tcv	13.1	4,30e -05	1,43e-05	33%	Full Open	Over-Temperature at Pre-Cooler Exit	Possible Avionics Overheating	MAJ
	13.2		1,43E-05	33%	Full Closed	Loss of Temperature Control at Pre-Cooler Exit	Possible Avionics Overcooling	MIN
	13.3		1,43E-05	33%	Minor Leakage	Minor Performance Reduction	None	MIN
Bay Inlet Water Separator	14.1	2,10 E-06	1,05E-06	50%	Insufficient Water Separation	Reduction in Inter-Cooler Efficiency	Possible Injection of Liquid Water In Avionic Bay	MIN
	14.2		1,05E-06	50%	Air Leakage	Cooling Performance Reduction	Possible Avionics Overheating	MAJ
Water Injector	15.1	N.A.	N.A.	100%	Obstructed	Minor Performance Reduction	None	MIN
Bay Inlet Temperature Sensor	18.1	8,60 E-07	4,30E-07	50%	Erroneous Over-Temperature Measurement	SOV Closure (Automatic Back-Up Action)	Loss of Air Conditioning. Loss of Pneumatic Air.	HAZ
	18.2		4,30E-07	50%	Erroneous Under-Temperature Measurement	None	Un-Protection from Over-Temperature	HAZ
Non Return Valve	2.1	1,10 E-06	5,50E-07	50%	Full Closed	Unavailable Bleed Air, Consequent Inoperative ECS	Loss of Air Conditioning. Loss of Pneumatic Air.	HAZ
	2.2		5,50E-07	50%	Full Open	None	None	NSE
Fan	27.1	4,00 E-05	2,00E-05	50%	Fan Unavailable (Inflight)	None	None	NSE
	27.2		2,00E-05	50%	Fan Unavailable (On Ground)	Insufficient Pre-Cooler and Inter-Cooler Heat Exchanging	Possible Avionic Over-Temperature (On Ground)	MAJ
Control Unit	28.1	1,00e -04	1,00e-04	100%	Control Unit complete failure	Inability to Control Valve, See TCV Effects	See TCV Effects	HAZ
Engine	29.1	1,00 E-05	1,00E-05	100%	Engine Shut-Down	Unavailable Bleed Air, Consequent Inoperative ECS	Loss of Air Conditioning. Loss of Pneumatic Air.	HAZ

Table 4.6: Air Cycle System FMECA

4.2.1.1 Failure Modes and Effects Summary (FMES)

End Effect	FMI	FR_{FMI}	*Item Name*	$FR_{Basic\ Event}$
Loss of air conditioning. Loss of pneumatic air.	1.1	4,20E-06	PRV/SOV	1,26E-05
	1.3	4,20E-06		
	1.6	4,20E-06		
	26.2	2,87E-07	Bleed Air Pressure Sensor	2,87E-07
	2.1	5,50E-07	Non Return Valve	5,50E-07
	29.1	1,00E-04	Engine	1,00E-04

	18.1	4,30E-07	Bay Inlet Temperature Sensor	4,30E-07
Possible insufficient air conditioning.	1.2	4,20E-06	PRV/SOV	4,20E-06
Avionic damage in the event of overheated air flow	1.5	4,20E-06	PRV/SOV	4,20E-06
Possible duct destruction, consequent structure and vital system damage	1.7	1,76E-11	PRV/SOV	1,76E-11
Possible Avionics overcooling	2.1	1,43E-05	Pre-cooler TCV	1,43E-05
	4.2	2,87E-07	Pre-cooler outlet temperature sensor	2,87E-07
	13.2	1,43E-05	Avionic Bay TCV	1,43E-05
Possible avionics overheating	2.2	1,43E-05	Pre-cooler TCV	1,43E-05
	11.2	1,05E-06	Turbine inlet water separator	1,05E-06
	12.3	6,75E-06	Cold Air Unit	6,75E-06
	13.1	1,43E-05	Avionic Bay TCV	1,43E-05
	14.2	1,05E-06	Bay Inlet Water Separator	1,05E-06
Possible fire and components damage	3.2	3,35E-06	Pre-cooler	3,35E-06
Avionics overcooling	4.1	2,87E-07	Pre-cooler outlet temperature sensor	2,87E-07
Un-protection from over-temperature	18.2	4,30E-07	Bay Inlet Temperature Sensor	4,30E-07
	4.3	2,87E-07	Pre-cooler outlet temperature sensor	2,87E-07
Possible avionics overheating and component damage	26.1	3,50E-07	Bleed Air Pressure Sensor	3,50E-07
Un-protection from overpressure	26.3	3,50E-07	Bleed Air Pressure Sensor	3,50E-07
Loss of air conditioning.	8.2	5,25E-07	Intercooler	5,25E-07
Possible injection of liquid water in avionic bay	11.1	1,44E-07	Turbine inlet water separator	1,44E-07
Avionics overheating	12.1	8,75E-08	Cold Air Unit	8,75E-08
Avionics overheating, possible fire	12.2	8,75E-08	Cold Air Unit	8,75E-08
Oil contamination	12.4	8,75E-08	Cold Air Unit	8,75E-08
Possible injection of liquid water in avionic bay	14.1	1,05E-06	Bay Inlet Water Separator	1,05E-06
Possible avionic over-temperature (on ground)	27.2	2,00E-05	Fan	2,00E-05

Table 4.7: Air Cycle System FMES

Vapour Cycle System FMECATable 4.8 reports the Failure Modes, Effects and Criticality analysis that has been carried out referring to the architecture of the vapour cycle system that has been described in the dedicated chapter.

Item Name	***FMI***	***FR_{TOT}***	***FR_{FMI}***	***FR%***	***FM Description***	***Next Higher Effect***	***End Effect***	***Severity***
Condenser	2.1	1,01E-05	9,75E-06	96,63%	Refrigerant fluid external leakage	reduction in refrigerant fluid mass, consequent insufficient cooling	Loss of air conditioning	HAZ
	2.2		3,40E-07	3,37%	Refrigerant section partially clogged	Slight condensation reduction	Degradation of cooling performance	MIN
Compressor	1.1	1,42E-04	1,31E-04	92,40%	worn out bearing and seals	decrease of compression performance	Degradation of cooling performance	MIN

	1.2		3,40E-07	0,24%	Refrigerant fluid external leakage	reduction in refrigerant fluid mass, consequent insufficient cooling	Loss of air conditioning	HAZ
	1.3		5,12E-06	3,60%	Compressor blocked	loss of refrigerant compression, consequent insufficient cooling	Loss of air conditioning	HAZ
	1.4		5,36E-06	3,77%	compressor motor failure	loss of refrigerant compression, consequent insufficient cooling	Loss of air conditioning	HAZ
Evaporator	6.1	2,52E-05	6,41E-06	25,46%	Refrigerant fluid external leakage	reduction in refrigerant fluid mass, consequent insufficient cooling	Loss of air conditioning	HAZ
	6.2		1,08E-06	4,29%	Refrigerant section partially clogged	slight evaporation reduction	Degradation of cooling performance	MIN
Recirc fan	7.1	1,77E-05	1,77E-05	100,00%	Mechanical failure	Severe decrease in avionic bay air flow	Loss of air conditioning	HAZ
Control Unit	3.1	2,00E-04	2,00E-04	99,91%	Erroneous detection of temperature	loss of evaporator inlet temperature acquisition	Loss of air conditioning	HAZ
	3.2		1,10E-07	0,05%	Loss of compressor command	loss of refrigerant compression, consequent insufficient cooling	Loss of air conditioning	HAZ
	3.3		8,00E-08	0,04%	Loss of fan command	Severe decrease in avionic bay air flow	Loss of air conditioning	HAZ
Temperature sensor	4.1	9,90E-07	3,30E-07	33,33%	Unavailable Measurement	loss of temperature control at evaporator inlet	Un-protection from over/under-temperature	MAJ
	4.2		6,60E-07	66,67%	Erroneous measurement	loss of temperature control at evaporator inlet	Un-protection from over/under-temperature	MAJ
Expansion valve	5.1	1,00E-5	5,00E-6	50%	Refrigerant fluid external leakage	reduction in refrigerant fluid mass, consequent insufficient cooling	Loss of air conditioning	HAZ
	5.2		5,00E-6	50%	Mechanical failure	Loss of refrigerant expansion, consequent insufficient cooling	Loss of air conditioning	HAZ

Table 4.8: Vapour Cycle System FMECA

4.2.1.2 Failure Modes and Effects Summary (FMES)

End Effect	FMI	FR_{FMI}	*Item Name*	$FR_{Basic\ Event}$
Loss of air conditioning	2.1	9,75E-06	Condenser	9,75E-06
	1.2	3,40E-07	Compressor	1,08E-05
	1.3	5,12E-06		
	1.4	5,36E-06		
	6.1	6,41E-06	Evaporator	6,41E-06
	6.1	5,00E-6	Expansion valve	1,00E-5
	6.2	5,00E-6		
	7.1	1,77E-05	Recirc Fan	1,77E-05

	3.1	2,00E-04	Control Unit	2,00E-04
	3.2	1,10E-07		
	3.3	8,00E-08		
Degradation of cooling performance	2.2	3,40E-07	Condenser	3,40E-07
	1.1	1,31E-04	Compressor	1,31E-04
	6.2	1,08E-06	Evaporator	1,08E-06
Un-protection from over/under-temperature	4.1	3,30E-07	temperature sensor	9,90E-07
	4.2	6,60E-07		

Table 4.9:Vapour Cycle System FMES

4.3 Fault Tre Analysis (FTA)

As has already been mentioned, Fault Tree Analysis is equivalent, hence replaceable, to Dependence Diagram (DD) or Makov Analysis (MA). All of these methods are top-down techniques whose aim is the determination of the combination of single failures that may result in one or more failure condition identified in the FHA, used as "top event". The basic events considered by the FTA shall comprehend all of the failure modes identified by the FMECA. The latter is also useful as source of failure rate computed in order to determine the probability of happening of the considered top event. Differently from the FMECA, which lists the possible failure conditions, including some which may be of no concern, the FTA (or the equivalent analyses) identifies the combination of the failure modes that, individually or collectively, lead to a hazardous or catastrophic event. Dealing with the probability of those undesired events, it is computed considering failure rates and exposure times.

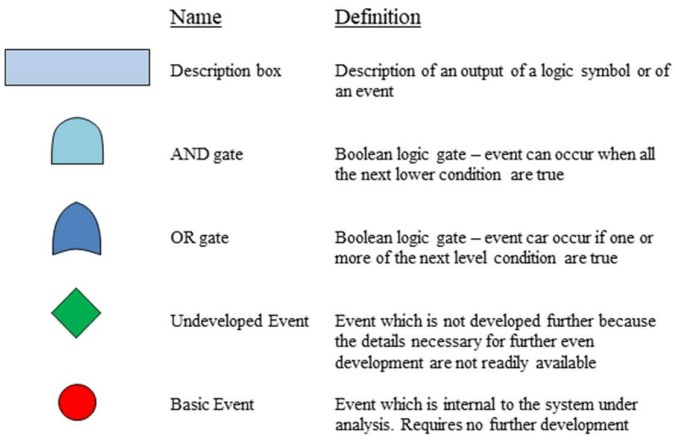

Figure 4.6: used FTA symbols (ref. [6])

Figure 4.6 reports the used FTA symbols. Moreover, it is possible to numerically determine the probability of the "top event" as a function of the failure rates of the basic events. In particular, the OR probability of n independent events that can occur simultaneously is given by the following expression:

$$P = 1 - \prod_{i}^{n} (1 - P_i)$$

As a general rule it is indeed necessary to subtract the probability that both A and B occur since it has been already taken in consideration twice when calculating P(A) and P(B).

Dealing with the AND door, the probability that two independent events will occur is $P(AB) = P(A) * P(B)$. It is possible to "solve" a fault tree using the latter expressions exclusively if it is made up of different and unique basic events. In case of one or more specific basic events appears more than once in the tree, it is necessary to refer to conditional probability.

4.3.1 Air Cycle System FTA

Figure 4.7 contains the fault tree which has been built referring to the air cycle architecture described in the dedicated chapter and to the failure modes of the components identified in the FMECA. Observing the fault tree it is possible to notice that there are some events (i.e. A, B, C, D) that appears more than once. For this reason, as has already been anticipated, conditioned probability has been used. Using $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$ to indicate the Boolean variable associated with A, B, C, D, it is possible to write the probability of "*Undetected total loss of air conditioning*" as follows[4]:

$$e_0 = \sum (e_{11}|_{\mathcal{ABCD}} \cdot e_{12}|_{\mathcal{ABCD}}) \, ABCD$$

The combinations of the repeated variables that lead to the verification of the top event are:

Sum index	$\mathcal{A}$	$\mathcal{B}$	$\mathcal{C}$	$\mathcal{D}$	$P(ABCD)$	$e_{12}\|_{\mathcal{ABCD}} = e_{32}\|_{\mathcal{ABCD}}$
$i = 1$	1	1	1	1	$ABCD$	1
$i = 2$	0	0	1	1	$(1-A)(1-B)CD$	1
$i = 3$	1	1	0	0	$AB(1-C)(1-D)$	1

Table 4.10: Conditioned Probability

Taking all of this into account it is possible to write the following expressions:

$$e_{11}|_{\mathcal{ABCD}} = 1 - (1 - e_{31})(1 - e_{33})(1 - e_{34})(1 - e_{35})(1 - e_{36})$$

Event	P(event)
e_{31}	RQ
$e_{33} = e_{34}$	$L + e_{51} - L * e_{51}$
e_{35}	$E + F - EF$
e_{36}	$1 - (1-G)(1-H)(1-I)$

Table 4.11: Event Probabilities

Finally, the catastrophic top event "*undetected total loss of air conditioning*" has the following failure rate:

$$e_0 = 8.46 \cdot 10^{-8} FH^{-1} < 10^{-7} FH^{-1} (CAT)$$

[4] For the sake of notation clarity, from this point on the probability of the event "A", usually expressed by P(A), is written as "A". Moreover, the events resulting from ANDs and ORs are identified by matrix indices e_{ij} (rows, columns): for instance, *total loss of air conditioning* is event "e_{11}", *erroneous information* is event "e_{12}", *emergency system failure* is event "e_{21}" and so on. The top event, which is *undetected total loss of air conditioning*, is called event 0 "e_0".

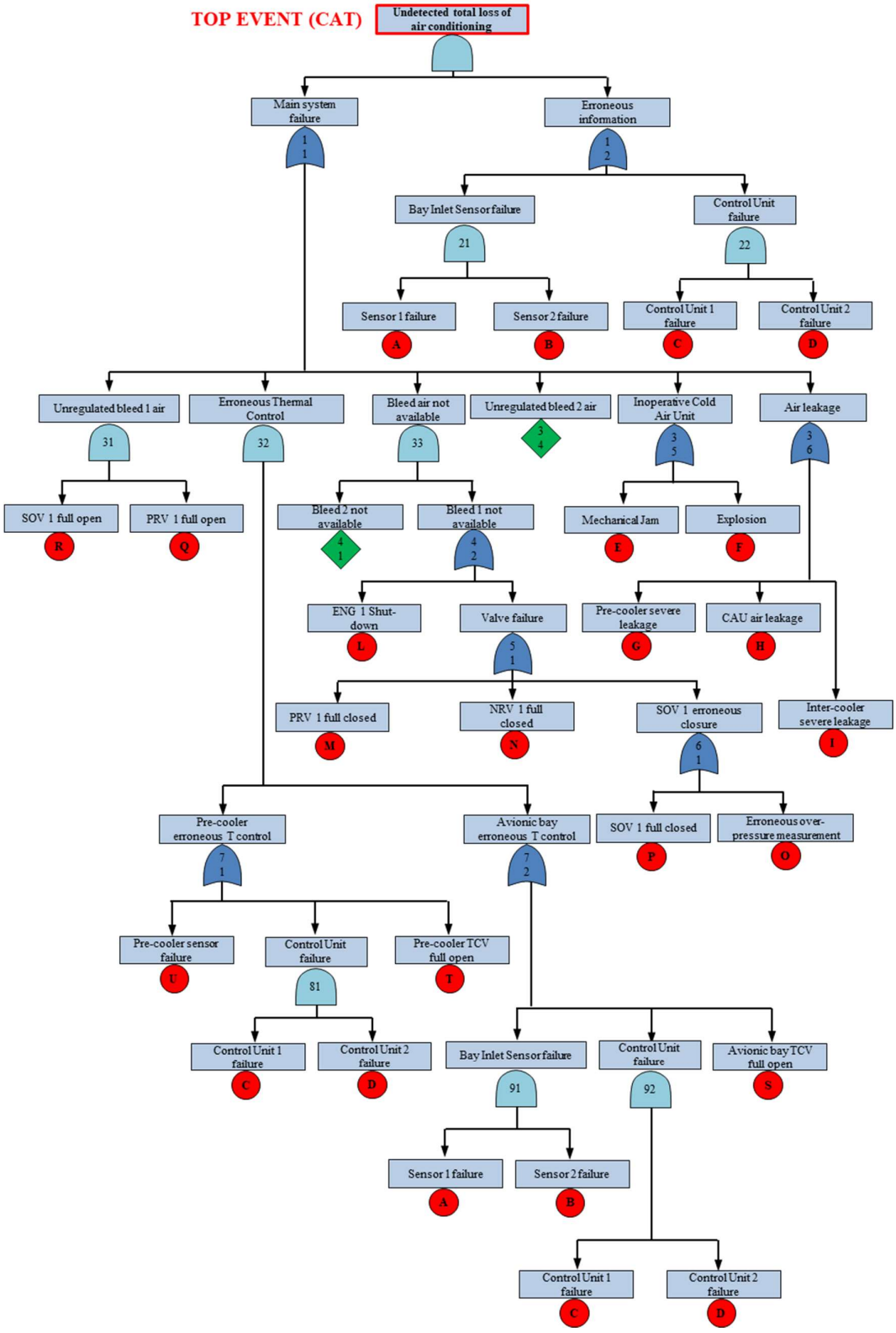

Figure 4.7: FTA - Air Cycle: *Undetected total loss of air conditioning*

Another important outcome of the FTA is the minimum cut set. This represents the minimum number of failure (basic events) that need to happen in order to cause the catastrophic top event. It is possible to compute this number applying the Boolean algebra:

$$topevent = (AB + CD)\big(RQ + GHI + EF + (L + M + N + P + O)^2 + (U + T + CD)(S + AB + CD)\big)$$

Since we are not interested in the computation of the probability, already determined above, it is possible to consider every event as a Boolean variable (0 or 1) depending on its happening (1) or not (0). For this reason, it is possible to eliminate some terms in order to obtain a sum of products of events. The minor number of multipliers making up the addends is equal to the minimum cut set:

From the previous expression it appears that it is sufficient the verification of three events. Note that every minimum combination is always characterized by the un-detection of the failure (AB or CD). In order to happen, the latter failure needs indeed at least two components (both sensors or both control units) to fail contemporarily.

It is now fundamental to pay attention to an important consideration related to sensors reliability and fault tolerance. As stated in NASA "*Reliable Dual-Redundant Sensor Failure Detection and Identification for the NASA F-8 DFBW Aircraft*", an advantageous solution, in terms of cost-effectiveness and maintenance, consist of two identical sensors. Because a single sensor has not the required level of reliability, common practise for fault tolerant systems relies on voting among three sensors: when a sensor gives abnormal measurements, with respect to the other two, it is assumed that the sensor at issue has failed. This means that a triplex system is tolerant to a single failure since, if two sensors fail, it is not possible to identify the working one. Although this solution is widely used, the third sensor is used only for vote, and provides no appreciable benefit in terms of performance under no-fail conditions, increasing cost and decreasing logistic reliability. The adopted solution sees the substitution of the third sensor with an analytic model, included in the control unit, which is able to determine whether and which of the two sensors has failed comparing its behaviour, both in static terms and in dynamic response, with the behaviour estimated by the digital model.

Moving to the hazardous condition of "*Detected total loss of air conditioning*", the fault tree is represented in Figure 4.8.

It is possible to compute the probability of the top event as follows:

$$e_0 = e_{11} * e_{12}$$

Where:

$$e_{11} = 1 - (1 - e_{31})(1 - e_{32})(1 - e_{33})(1 - e_{34})(1 - e_{35})(1 - e_{36})$$

The probability of all of the events contained in e_{11} are equal to the ones computed for the previous tree, the only one that changes is the following:

$$e_{32} = S(U + T - UT)$$

The event e_{12}, instead, is computed as follows:

$$e_{12} = \big(1 - (1 - A^C)(1 - B^C)\big)\big(1 - (1 - C^C)(1 - D^C)\big)$$

Note that the "*failure detected*" condition is determined by the complementary probability of sensor and control unit failure, corresponding to the operative state, and written as "A^C"[5].

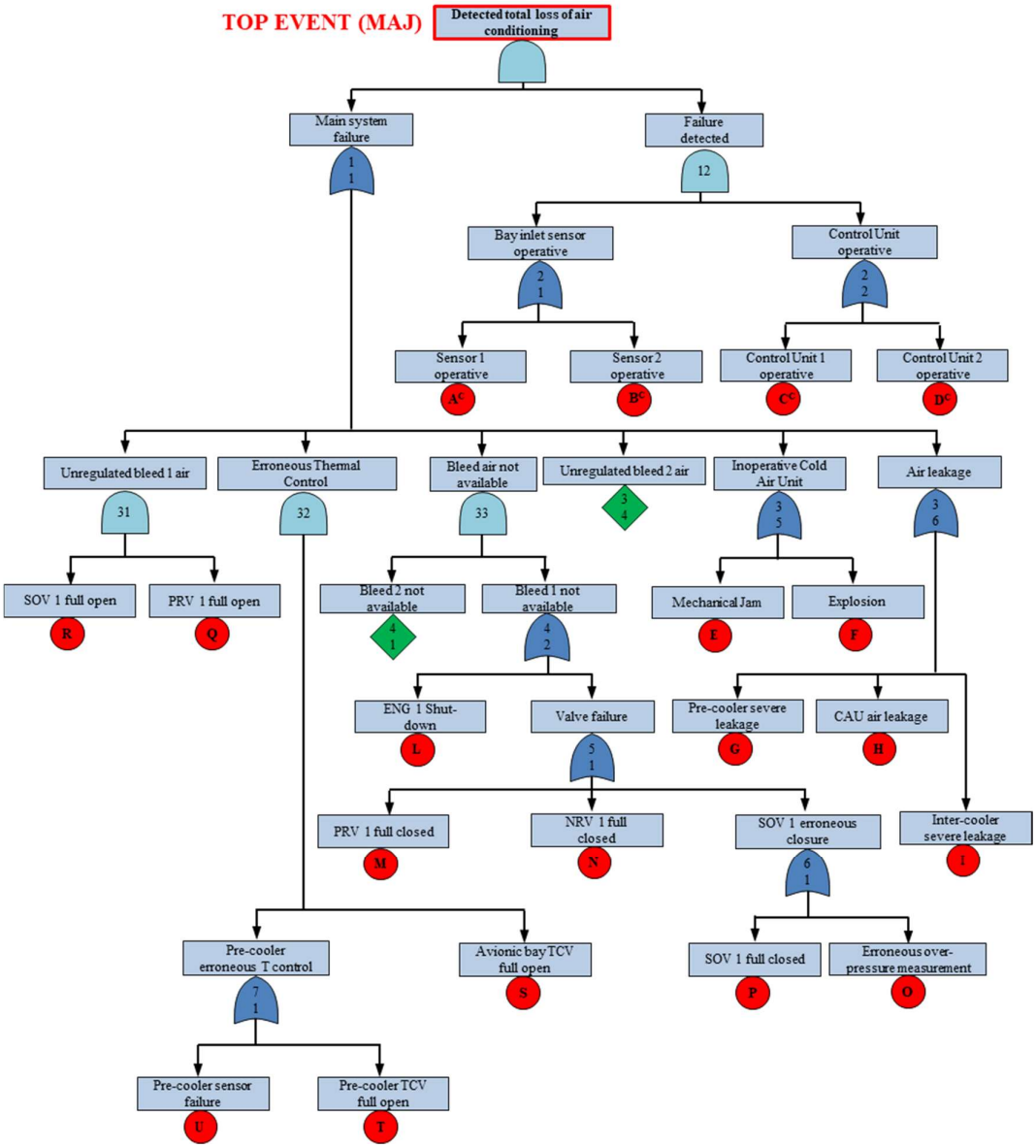

Figure 4.8: FTA - Air Cycle: *Detected total loss of air conditioning*

Finally, the major top event "*Detected total loss of air conditioning*" has the following failure rate:

$$e_0 = 5.15 \cdot 10^{-5} FH^{-1} < 10^{-4} FH^{-1}(MAJ)$$

[5] It yields that $A^C = (1 - A)$.

Note that this condition relies on the back-up system that is activated once that a failure of the main system is detected. Since the avionic bay overtemperature is considered catastrophic, the emergency system shall have a minimum reliability of $1.82 \cdot 10^{-3} FH^{-1}$. This reliability budget shall take into account the failure rate of the actuators used to the extension of the air intakes that leads the ram air to the avionic bay.

4.3.2 Vapour Cycle System FTA

Moving to the FTAs for the Vapour Cycle Cooling System, reported in Figure 4.9,the probability computation is analogue to the one described above, hence the sole results are reported. Dealing with the *Undetected total loss of air conditioning*, its probability is as follows:

$$e_0 = 4.00 \cdot 10^{-8} FH^{-1} < 10^{-7} FH^{-1}(CAT)$$

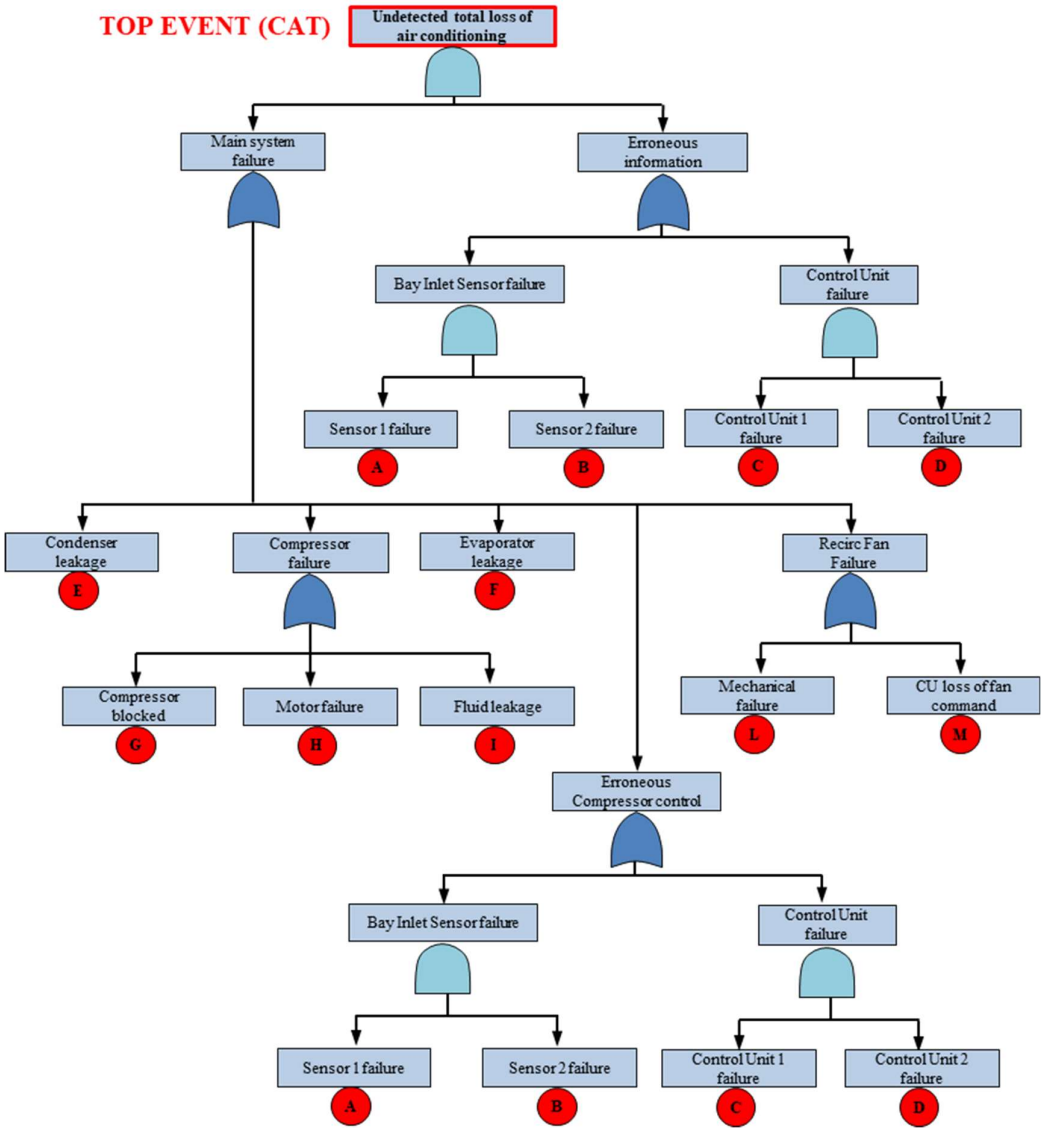

Figure 4.9: FTA - Vapour Cycle: *Undetected total loss of air conditioning*

In this case the minimal cut set is equal to 3 since, while a single failure is sufficient to lead to the main system failure, 2 other failures are necessary to avoid the detection of the malfunctioning at issue.

Dealing instead with the *Detected total loss of air conditioning* (Figure 4.10), its value is:

$$e_0 = 4.47 \cdot 10^{-5} FH^{-1} < 10^{-4} FH^{-1}(MAJ)$$

Even in this case the minimal cut set is 3 due to the exact same reason explained above.

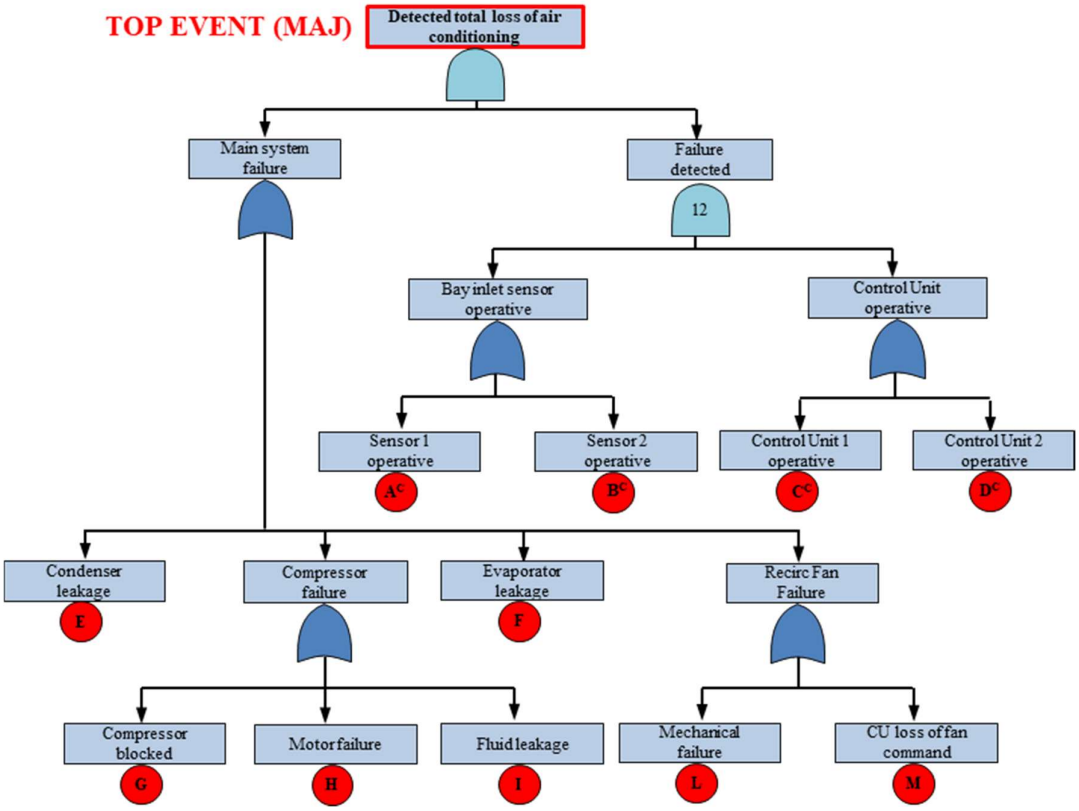

Figure 4.10: FTA - Vapour Cycle: *Detected total loss of air conditioning*

4.4 Functional Model

At this point it is possible to collect all the information obtained with the functional and performance analysis and with the safety assessment in the original functional model. In this way, there exist a single model containing the results of those analysis. In particular, it is possible to generate a father/son dependence between the *air conditioning equipment* and with the actual low-level physical components, differently for the air cycle and the vapour cycle systems. The obtained results are shown in the following figures. Moreover, each of these components is characterized by a series of values regarding performance analysis (e.g. weight, electrical power, size) safety assessment (i.e. IDAL, Failure Rates, FMECA ID) and part number. Specifically, Figure 4.11 reports the Control Unit decomposition, valid for both ACM and VCCS. Moreover, Figure 4.12, Figure 4.13 and Figure 4.14 report the same components that have been used in performance and safety analysis.

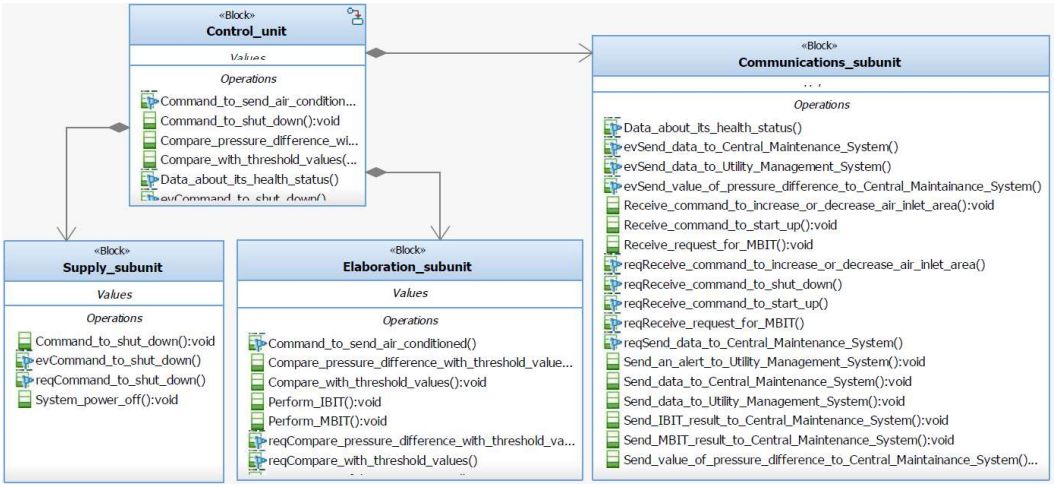

Figure 4.11: Control Unit Block Definition Diagram

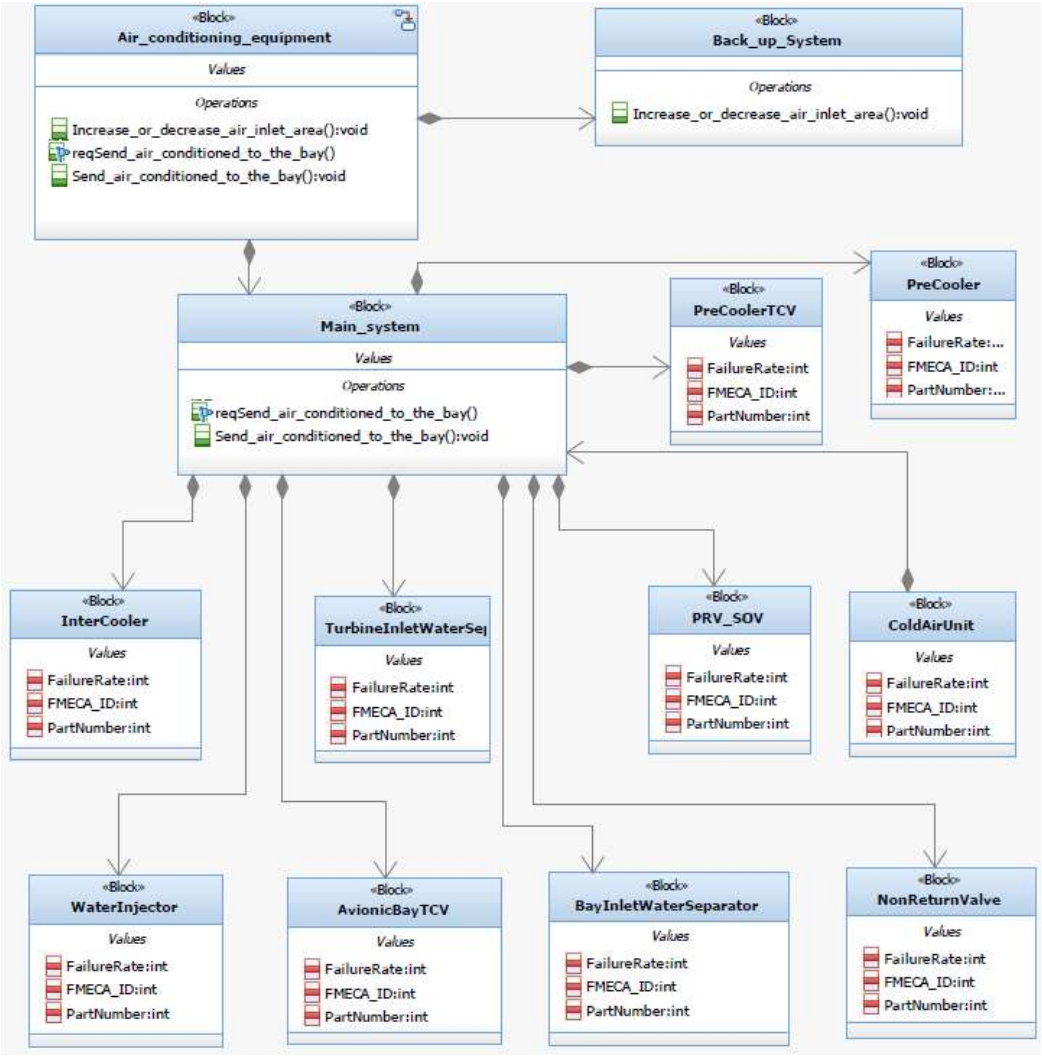

Figure 4.12: ACM Block Definition Diagram

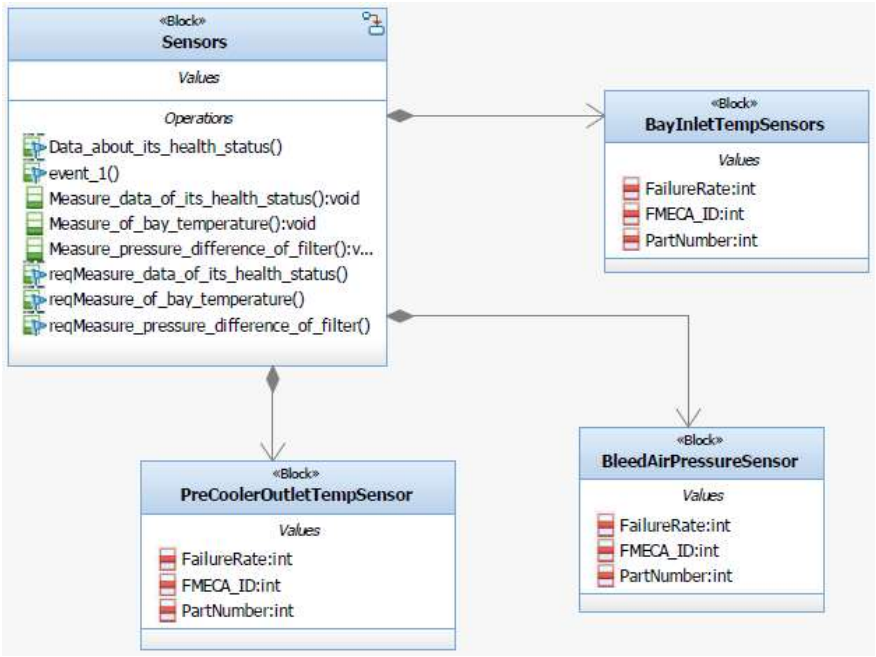

Figure 4.13: ACM Sensors Block Definition Diagram

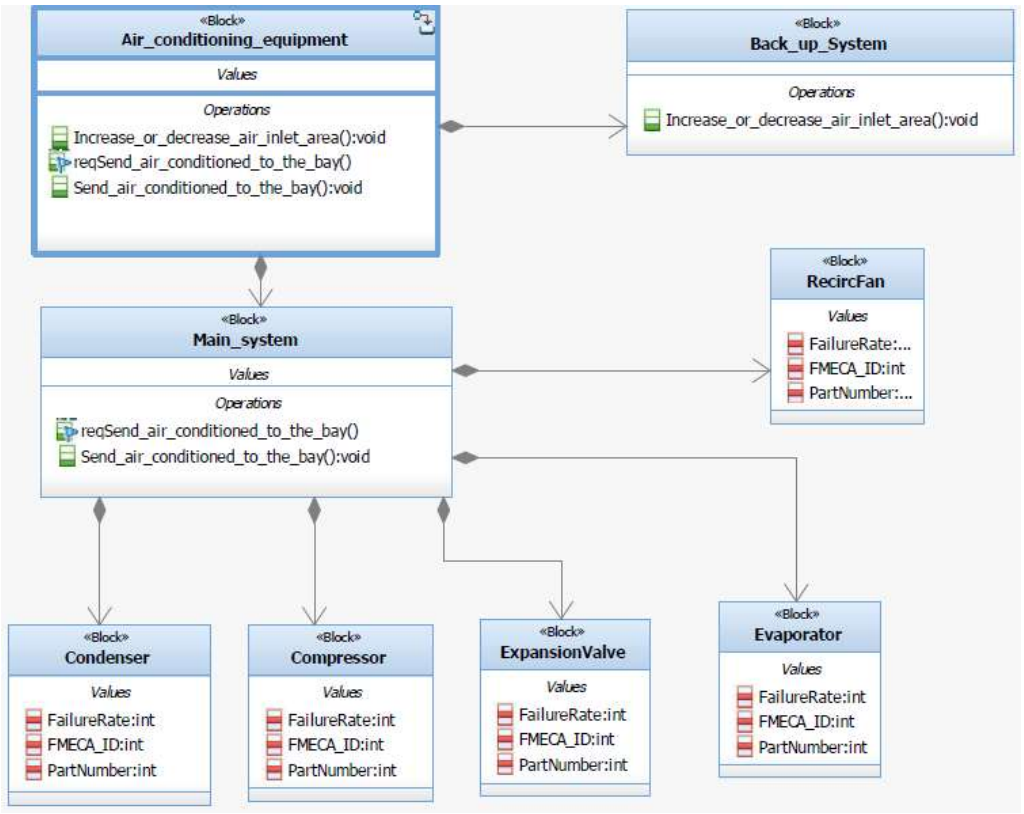

Figure 4.14: VCCS Block Definition Diagram

4.5 Future Developments

Dealing with potential future developments, it may be possible to furtherly integrate the system functional model with the safety assessment. Similarly to what has been made with the Functional Hazard Assessment (FHA) in the thesis, this can be realized developing procedures and programs which assist the safety analyst providing increased effectiveness and objectivity. The used functional analysis tool allows indeed to develop additional features using a determined programming language.

Moreover, it may be interesting to study the interaction of performance and safety analyses with other disciplines, such as cost estimate, and their effect on system design. One of the main outputs of the conducted safety assessment regards, indeed, the definition of redundancies and the allocation of Development Assurance Levels (DALs).

The number of redundancies must guarantee that a given top event has a probability of happening lower than the limit determined by the Functional Hazard Assessment. The Fault Tree Analyses (FTA), assisted by the Failure Modes Effect and Criticality Analyses (FMECA), are used to validate those probability requirements. The determined number of redundancies directly affects the weight of the system and its acquisition cost.

On the other hand, the Development Assurance Level of a component is determined by severity. The Functional Hazard Assessment determines indeed the severity of a specific function loss and, since the functional analysis allocated each function to a component, it is possible to determine the required Development Assurance Level. A higher DAL leads inevitably to a higher development cost.

Furthermore, the failure rate of each component does not only affect safety but even operative cost: a lower Mean Time Between Failures (MTBF) implies an increment of maintenance cost.

All of these considerations may be taken into account to determine the development, the acquisition and the operative cost of both Air Cycle and Vapour Cycle System. Besides from weight, performance and safety, another driver that shall be used to conduct a trade-off between the two considered ECS architectures is indeed the cost of the system.

5 Computational Fluid Dynamics Analysis

5.1 Introduction

This chapter is dedicated to the validation of the cooling back-up system via a Computational Fluid Dynamics analysis conducted in Siemens STAR CCM+ ®. The main outcome of the safety assessment carried out in the previous chapter is indeed the necessity of a solution capable of maintaining bay temperature under the limits even in the event of a complete ECS failure. Moreover, as has already been explained in section 3.4, the presence of a back-up system is required by airworthiness requirements as stated in USAR.U1307 – C of STANAG 4671 draft ed.3, "UAV Systems Airworthiness Requirements (USAR) for North Atlantic Treaty Organization (NATO) Military UAV Systems", 2014-09.

5.2 CFD Evaluation

5.2.1 Theoretical Background

The analytical model of fluid dynamics lies its fundament on the three equations that are reported below.

To begin with the continuity equation, it regards the mass conservation and it is expressed as follows:

$$\frac{\partial \rho}{\partial t} + \nabla \cdot (\rho \boldsymbol{V}) = 0$$

Where $\boldsymbol{V} = [u, v, w]^T$ is the velocity vector.

Moving to the momentum equation, it derives from Newton's second law and it is expressed as follows:

$$\frac{\partial(\rho u)}{\partial t} + \frac{\partial(\rho u^2)}{\partial x} + \frac{\partial(\rho uv)}{\partial y} \frac{\partial(\rho uw)}{\partial z} = -\frac{\partial p}{\partial x} + \frac{\partial}{\partial x}\left(\lambda \nabla \cdot \boldsymbol{V} + 2\mu \frac{\partial u}{\partial x}\right) + \frac{\partial}{\partial y}\left[\mu\left(\frac{\partial v}{\partial x} + \frac{\partial u}{\partial y}\right)\right] + \frac{\partial}{\partial z}\left[\mu\left(\frac{\partial u}{\partial z} + \frac{\partial w}{\partial x}\right)\right] + \rho f_x$$

$$\frac{\partial(\rho v)}{\partial t} + \frac{\partial(\rho uv)}{\partial x} + \frac{\partial(\rho v^2)}{\partial y} \frac{\partial(\rho vw)}{\partial z} = -\frac{\partial p}{\partial y} + \frac{\partial}{\partial y}\left(\lambda \nabla \cdot \boldsymbol{V} + 2\mu \frac{\partial v}{\partial y}\right) + \frac{\partial}{\partial x}\left[\mu\left(\frac{\partial v}{\partial x} + \frac{\partial u}{\partial y}\right)\right] + \frac{\partial}{\partial z}\left[\mu\left(\frac{\partial w}{\partial y} + \frac{\partial v}{\partial z}\right)\right] + \rho f_y$$

$$\frac{\partial(\rho w)}{\partial t} + \frac{\partial(\rho uw)}{\partial x} + \frac{\partial(\rho vw)}{\partial y} \frac{\partial(\rho w^2)}{\partial z} = -\frac{\partial p}{\partial z} + \frac{\partial}{\partial z}\left(\lambda \nabla \cdot \boldsymbol{V} + 2\mu \frac{\partial w}{\partial z}\right) + \frac{\partial}{\partial y}\left[\mu\left(\frac{\partial w}{\partial y} + \frac{\partial v}{\partial z}\right)\right] + \frac{\partial}{\partial x}\left[\mu\left(\frac{\partial u}{\partial} + \frac{\partial w}{\partial x}\right)\right] + \rho f_z$$

Where $\lambda = -2/3\,\mu$ and μ is the molecular viscosity coefficient. Those coefficients are used in the definition of surfaces forces, both shear stress (τ_{ij}) and normal stress (τ_{ii}) distributions acting on the fluid element surfaces:

$$\tau_{xx} = \lambda(\nabla \cdot \boldsymbol{V}) + 2\mu\frac{\partial u}{\partial x}$$

$$\tau_{yy} = \lambda(\nabla \cdot \boldsymbol{V}) + 2\mu\frac{\partial v}{\partial y}$$

$$\tau_{zz} = \lambda(\nabla \cdot \boldsymbol{V}) + 2\mu\frac{\partial w}{\partial z}$$

$$\tau_{xy} = \tau_{yx} = \mu\left[\frac{\partial v}{\partial x} + \frac{\partial u}{\partial y}\right]$$

$$\tau_{xz} = \tau_{zx} = \mu\left[\frac{\partial u}{\partial z} + \frac{\partial w}{\partial x}\right]$$

$$\tau_{yz} = \tau_{zy} = \mu\left[\frac{\partial w}{\partial y} + \frac{\partial v}{\partial z}\right]$$

The terms f_i represent instead body forces acting on the volumetric mass of the fluid elements.

The last equation is the energy equation which has the following form:

$$\frac{\partial}{\partial t}\left[\rho\left(e + \frac{V^2}{2}\right)\right] + \nabla \cdot \left[\rho\left(e + \frac{V^2}{2}\right)\boldsymbol{V}\right]$$
$$= \rho\dot{q} + \frac{\partial}{\partial x}\left(k\frac{\partial T}{\partial x}\right) + \frac{\partial}{\partial y}\left(k\frac{\partial T}{\partial y}\right) + \frac{\partial}{\partial z}\left(k\frac{\partial T}{\partial z}\right) - \frac{\partial(up)}{\partial x} - \frac{\partial(vp)}{\partial y} - \frac{\partial(wp)}{\partial z} + \frac{\partial(u\tau_{xx})}{\partial x} + \frac{\partial(u\tau_{xy})}{\partial y}$$
$$+ \frac{\partial(u\tau_{xz})}{\partial z} + \frac{\partial(v\tau_{xy})}{\partial x} + \frac{\partial(v\tau_{yy})}{\partial y} + \frac{\partial(v\tau_{zy})}{\partial z} + \frac{\partial(w\tau_{yz})}{\partial y} + \frac{\partial(w\tau_{zz})}{\partial z} + \rho\boldsymbol{f} \cdot \boldsymbol{V}$$

Where e is the internal energy per unit mass and $\dot{q}$ is the rate of volumetric heat addition per mass unit. Thermal conductivity is instead represented by k, thus Fourier's law of heat conduction states that:

$$\dot{q}_x = -k\frac{\partial T}{\partial x} \quad \dot{q}_y = -k\frac{\partial T}{\partial y} \quad \dot{q}_z = -k\frac{\partial T}{\partial z}$$

The numerical flow solution relies upon the finite volume method which divides to fluid domain into a finite number of control volumes with a reduced dimension. This is made with the aim of transforming the described mathematical model into a system of algebraic equation, applying a discretization in space and time domain. Every conservation equation can be written in terms of the following generic transport equation:

$$\frac{d}{dt}\int_V \rho\,\phi\,dV + \int_A \rho\,\boldsymbol{v}\,\phi\,d\boldsymbol{a} = \int_A \Gamma\,\nabla\phi\,d\boldsymbol{a} + \int_V S_\phi dV$$

The variable ϕ represents the transport of a scalar property and the equation is made up of four terms regarding the transient term, the convective flux, the diffusive flux and the source term. When the constitutive relations and the boundary conditions are introduced into the described equation a closed set of equation is obtained.

5.2.2 Geometry Model

The overall avionic bay architecture has already been introduced in section 3.1 and it is reported in Figure 5.1. Moreover, Figure 5.2 reports the CAD model generated in Dassault Systemes CATIA ®. In particular, the considered avionics components are Line Replaceable Units. They are designed in order to be quickly replaced even when the aircraft is ready to depart. Soon before the commencing of a mission, the different control units installed on the aircraft perform a series of Initial Built-in Tests. If an avionic failure is detected, then the failed component is briefly removed from the aircraft and replaced "in line" with a functioning one. In order to guarantee an easy access, the components have been positioned in two rows on each side of the vehicle. A total of 32 components has been used.

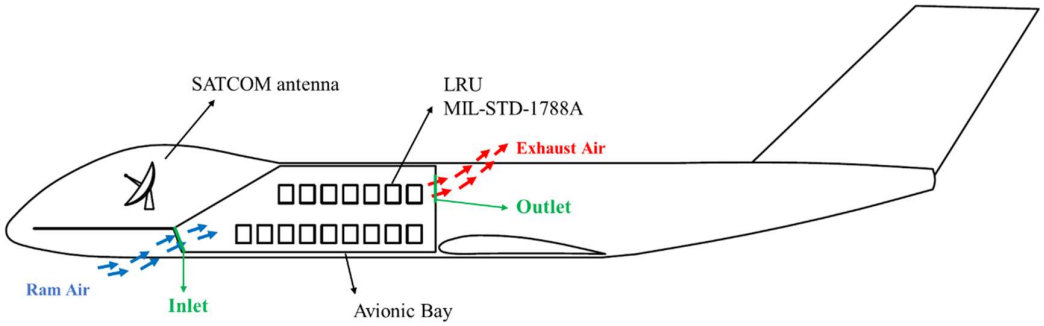

Figure 5.1: Aircraft configuration

The data regarding the LRU components has been determined referring to MIL-STD-1788A, "*Military Standard – Avionics Interface Design Standard*", United States of America Department of Defence, 1985. The abovementioned document standardizes the dimensions and the temperature limits of those components. In particular, as reported in

4.2.6.1.3 Low and high operating temperature:

"The low and high operating temperature, ground or flight, continuous, shall be -54°C to +71°C"

and

4.2.6.1.2 Short term operating temperature:

"The short term operating temperature, thirty minutes duration, shall be -54°C to +95°C"

Hence, in the event of an ECS failure, the ram air ventilation shall be sufficient to keep maximum temperature below 95°C for a maximum of 30 minutes. As emerged from the conducted analyses, the worst possible condition is the "hot day", thus the Computational Fluid Dynamics analysis will be effectuated considering an outside temperature of 50°C, hence a recovery temperature of 52°C (see chapter 3).

The considered skin can be schematized in Figure 5.3Figure 5.2 and it is made up of a layer of aluminium alloy and another of a Carbon Fibre Reinforced Polymer. Figure 5.2 reports the overall bay model

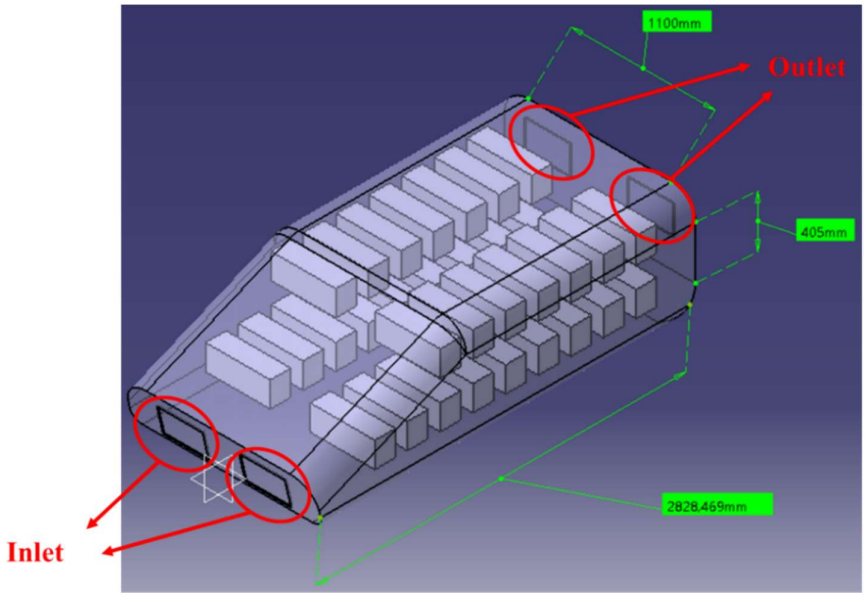

Figure 5.2: Avionic Bay CAD model

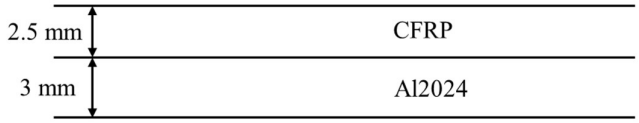

Figure 5.3: bay skin structure

The conduction heat passing through the skin is given by the following expression:

$$q_{cond} = A \cdot U \cdot (T_{ext} - T_{int})$$

Where A is the exchange area and U is the thermal conductivity $[W/m^2K]$.

If, as in this particular case, the wall is composed by more than just one layer of material, U is computable as follows:

$$U = \frac{1}{\sum \frac{s_i}{k_i}} = \frac{1}{\frac{2.5}{K_{CFRP}} + \frac{3}{K_{Al}}}$$

Considering the following values, extracted respectively from reference [13] and [14]:

$$K_{CFRP} = 50\ W/mK$$

$$K_{Al} = 120\ W/mK$$

Yields

$$U = 13.33\ W/m^2K$$

Hence thermal resistance is equal to $0.075\ m^2K/W$.

Dealing with convective heat transfer between the skin and the air, both internal and external, it is expressed by Newton's law of cooling:

$$q_{conv} = h(T_s - T_{ref})$$

Where q_{conv} $[W/m^2]$ is the local surface heat flux and h $[W/m^2K]$ is the local convective heat transfer coefficient. The temperature of the skin is T_s and T_{ref} is a characteristic temperature of the fluid moving over the surface. The convective heat transfer coefficient has been computed according to [15]:

$$h = 0.185\rho_w c_p u_\infty (log_{10} Re_x)^{-2.584} Pr^{-2/3}$$

Where:

$Re_x =$ Local Reynolds number $1.0355 \cdot 10^7$ (@ $x = 2\ m$)

$Pr =$ Prandtl number = 0.705

$c_p =$ air constant-pressure specific heat = 1006 J/kgK

$\rho_w =$ ambient density @ $T^* = 1.092\ kg/m^3$

$u_\infty =$ airplane airspeed = $72\ m/s$

$T^* = \frac{T_{rec} + T_\infty}{2} + 0.22(T_{rec} - T_\infty) = 324.6\ K$

Yields:

$$h = 120\ W/m^2K$$

Those values will be used in the used CFD tool to characterize the thermal specification of the external surfaces of the bay. Figure 5.4 summarizes the heat transfers to which the bay is subject.

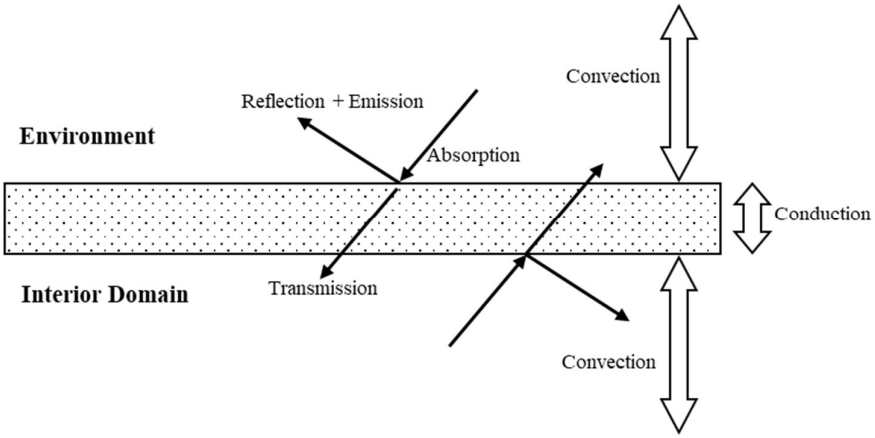

Figure 5.4: Heat Transfer Scheme (ref [11])

5.2.3 Grid Discretization

The first step is the realization of the three-dimensional CAD model, reported in 5.2.2. In order to import the geometry in the adopted CFD tool it is necessary to export it from Dassault Systemes CATIA ® as IGES format: the skin of the bay is modelled as a surface whose thermal characteristics have been calculated above.

At this point it is possible to generate the surface and volume meshes. A mesh sensitivity analysis has been carried out in order to obtain a mesh fine enough to provide numerically reliable results with an acceptable computational cost. At this purpose, it is possible to run the same case increasing gradually the mesh refinement and monitoring a characteristic variable such as the maximum temperature of a specific LRU.

Once that a certain value of mesh refinement has been reached, the mentioned characteristic variable will not be subject to considerable change, hence a further refinement will only lead to a higher computational cost without appreciably changing the actual result of the CFD analysis. Taking into account all of the above, the result of this mesh sensitivity analysis is reported in Table 5.1.

MODELS	**Notes**	
Polyhedral Mesh		
Prism Layer Mesher	Stretching function: geometric progression	
REFERENCE VALUES		
Base size	0.1 m	
Number of Prism Layers	8	
Prism Layer Stretching	1.2	
Prism Layer Thickness	0.020 m	
Surface size: relative minimum size	5% of base size	4% for inlet and outlet
Surface size: relative target size	25% of base size	22% for inlet and outlet
RESULTS		
Volume cells	665221	
Surface faces	120254	

Table 5.1: Mesh Specification

The Prism Layer refers to specialized thin cell that are important for resolving the boundary layer and that are determined by the homonym Mesher. The prism layer mesh model is indeed used as part of the volume mesh with the aim of generating orthogonal prismatic cells next to wall surfaces of boundaries. This is necessary in order to improve the accuracy of the flow solution near the walls. Since this is the zone affected by the boundary layer, those thin cells are critical to correctly determine heat transfer and flow separation. Prism layers also reduce numerical diffusion near the wall. The latter basically consists of a discretization error that smears discontinuities and steep gradients in a finite volume advection scheme.

In order to determine the number of prism layers, and their dimension, it is necessary to refer to the dimensionless wall distance y^+, defined as follows:

$$y^+ = \frac{y u_\tau}{\nu}$$

Where y is the actual absolute distance from the wall, ν is cinematic viscosity of the fluid and u_τ is the friction velocity, defined as a function of wall shear stress τ_w and fluid density ρ:

$$u_\tau = \sqrt{\frac{\tau_w}{\rho}} \qquad \tau_w = \rho\nu\left(\frac{du}{dy}\right)_{y=0}$$

Taking all of this into account, the value of y^+ that needs to be obtained in the first layer of cells near the wall shall be determined by the adopted turbulence model.

Figure 5.5 and Figure 5.6 report, respectively, the external and the internal view of the mesh generated with the specification reported in Table 5.1. Note that two fictional planes, each distant 0.4 m from the symmetry plane, have been added so to allow the visualization of the mesh and of the prism layer (Figure 5.6).

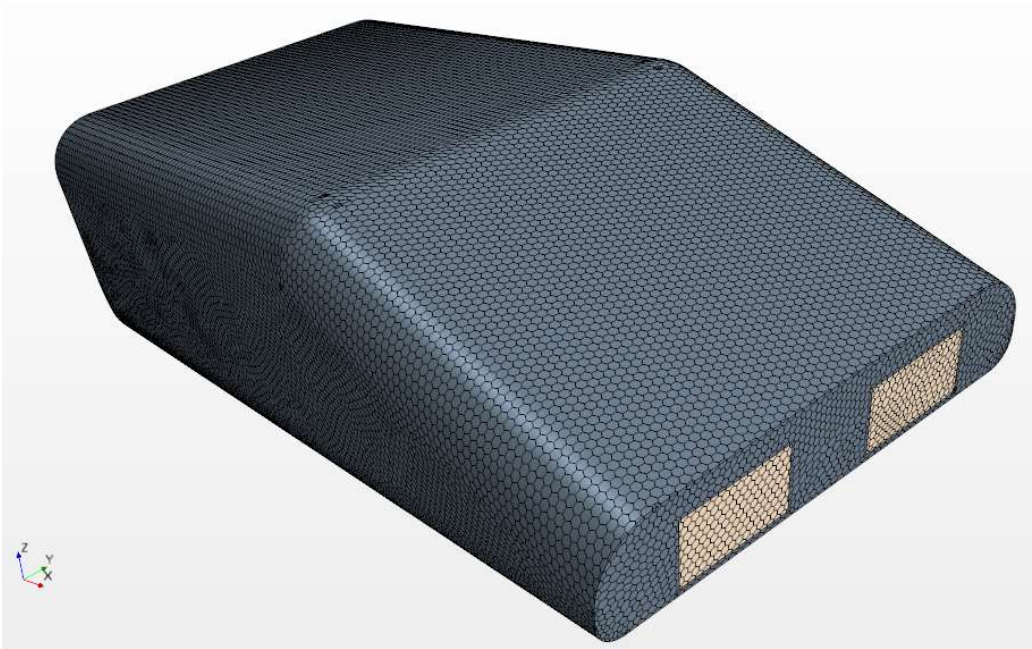

Figure 5.5: Mesh - External View

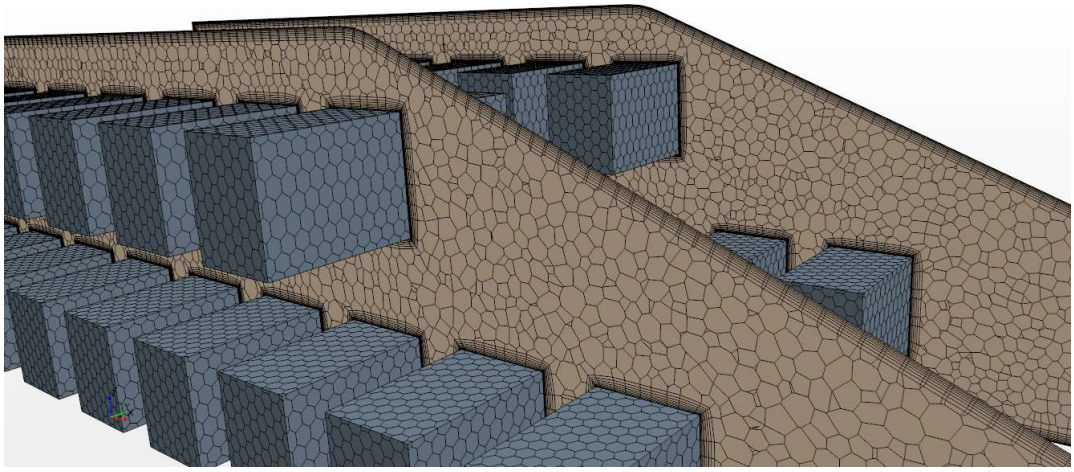

Figure 5.6: Mesh - Internal View

5.2.4 Physics Models

Moving to the models describing the physics of the simulation, air is modelled as a compressible ideal gas with gravity effect. The segregated flow solver has also been selected: it sequentially solves the integral conservation equations of mass and momentum relying upon a pressure-velocity coupling algorithm.

Dealing with heat transfer, the simulation always considers convection, conduction and Surface-to-Surface Radiation. In particular, the selected Grey Thermal Radiation models wavelength-independent radiation properties, thus considered invariant within the spectrum. Moreover, the considered Surface-to-Surface Radiation concerns only the radiating and absorbing surfaces, not any intervening medium. The model relies upon a spatial discretization of the boundary surfaces into patches and the determination of geometrical View Factors. They quantify, for each patch, the proportion of surface area that is illuminated by the other patches.

5.2.4.1 Turbulence Model

The considered turbulence models rely on Reynolds-Averaged Navier-Stokes (RANS) equations, based on the decomposition of each solution variable ϕ of the instantaneous Navier-Stokes equations into its averaged value $\overline{\phi}$ and its fluctuating component ϕ':

$$\phi = \overline{\phi} + \phi'$$

The models that have been considered belong to the family of K-Epsilon models, due to their good compromise between robustness, computational cost and accuracy and their suitability to the description of complex recirculation with heat transfer. Those models consist of two-equations solving transport equation for the turbulent kinetic energy k and the turbulent dissipation rate ε. The most used are High and Low Reynolds Number Approach and Two-Layer Approach. The latter formulation is an alternative to the low Re approach and works with either low y^+ or wall function type meshes ($y^+ > 30$). Another largely spread model variant is the Realizable K-Epsilon which provides more reliable and accurate simulation with respect to the standard models.

In conclusion, the used turbulence model is the Realizable Two-Layer K-Epsilon, an all-y^+ wall treatment which gives good results on fine meshes and produces the least inaccuracies for

intermediate meshes, characterized by $1 < y^+ < 30$ (ref. [11]). The reference values reported in Table 5.1 led the values of the dimensionless wall distance comprehended between 0.31 and 12, as shown in Figure 5.7, coherently with the specification of the chosen turbulence model.

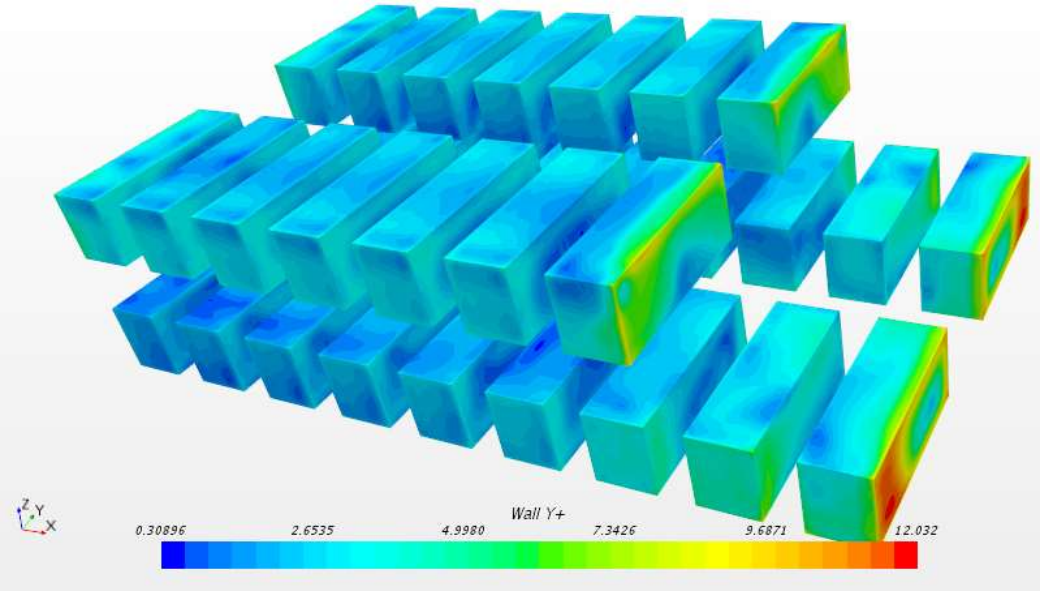

Figure 5.7: Wall y+

5.2.4.2 Boundary Specifications

The boundary specification of all of the boundaries is set to *wall* as air velocity will be tangent to those surfaces.

Moving to the surfaces representing the two air inlets of the bay, their boundary specification is set to *mass flow inlet*. In particular, the value of air flow is 0.75 kg/s. This value has been determined via several iterations with aim of minimizing the mass flow, hence minimizing the dimension of the inlet, keeping the maximum temperature in the range specified by the abovementioned requirements.

On the contrary, the surfaces which represent the outlets have been set to *pressure outlet*.

Dealing with the LRUs, as has already been explained in section 3.4, the emergency procedures imply the deactivation of those equipment which are not considered necessary to the safe termination of the flight. The considered equipment list is reported in Table 5.2.

In order to reproduce this peculiar situation in the CFD model, some of the LRUs have been set to *adiabatic*, since they represent switched-off equipment. The remaining LRUs have been set to *heat source* in order to provide a total heat load of 1530 W. The active LRUs will be easily identifiable in the following figures given their higher temperature.

Moving to the thermal specification of the external walls of the avionic bay, representing the skin of the aircraft, three different settings have been considered in test cases 1, 2 and 3

regarding the heat transfer with the external environment. Those set-ups are described in each subsection of 5.2.5 and are summarized in Table 5.3.

System in avionic bay	Item name	In flight heat load [W]	On ground heat load [W]	Emergency heat load [W]
Safe flight and landing system	Flight Control Computers (x4)	320	320	100
	GNSS (x4)	280	280	180
	SAHRS & IRS (x2)	170	170	80
	Radio Altimeter (x2)	30		30
	Air Data System	30	30	20
	Utilities Management System	180	180	50
Fly Management and Airspace Integration System	Flight Data Recorder	50	50	50
	DME T/R	42		
	Flight Management Computer (x4)	200	200	100
	Transponder	120	35	
	TCAS	60		
Communication system	V/UHF T/R	70	70	70
	SATCOM H/W	1010		550
	DLINK H/W	300		300
	Others	1120	300	
Airborne Mission System	Airborne Mission Management System	400	400	
	RADAR System	550		
	Surveillance System	300		
Airborne armament system	Airborne Armament Computer (x2)	300	300	
Electrical power system	Transformer Rectifier Unit	180	180	
	Others	3394	1495	
Total Heat Load [W]		**9094**	**4005**	**1530**

Table 5.2: Avionic Heat Loads

	Skin Thermal Specification	Notes
Test Case 1	*Adiabatic*	No thermal transfer between the bay and the external environment
Test Case 2	*Environment*	Conduction, convection and radiation according to Figure 5.4, no solar loads
Test Case 3	*Environment*	As test case 2, with solar loads

Table 5.3: Test Cases Specifications

Figure 5.8 summarizes the boundary and thermal specifications of the internal geometry imported into the used CFD tool. Those settings remains identical in all of the three test cases described in section 5.2.5.

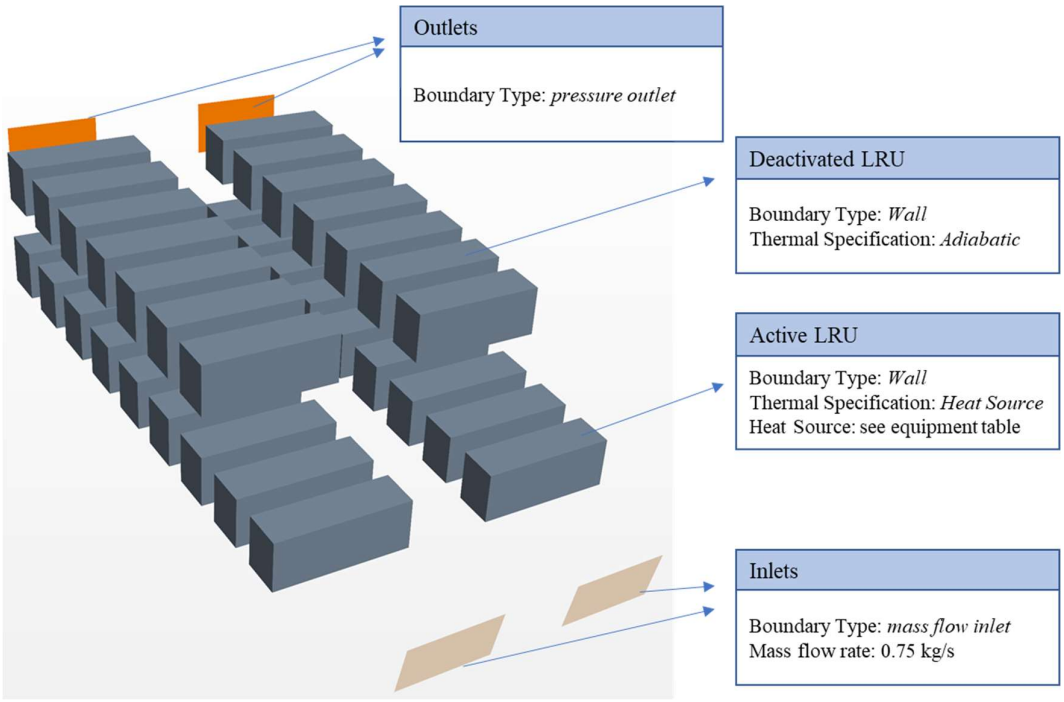

Figure 5.8: Boundary Specifications - Internal View

5.2.5 Test Cases

This section is aimed to the visualization of temperature and velocity fields of the volume of the bay. Once that the simulation is over and the software has converged, it is indeed possible to observe the air flow inside the bay plotting the streamlines from the inlet.

After the first simulations the maximum temperature reached by several LRUs was much higher than the allowable limit, even for short term operations. Studying the solved flow, it was possible to understand how this fact was due to the recirculation of air in certain zones of the avionic bay. This particular condition was pointed out by the streamlines which showed the mentioned recirculation. In order to solve this issue and allow air to reach the outlet without stagnating around some of the LRUs, hence causing their over-heating, it was necessary to carry out several iterations modifying the geometry of the inlet.

The conducted performance analysis (see chapter 3) has pointed out that the worst cooling condition is represented by flight at sea level on a hot day (ISA + 35). For this reason, all of the simulations have been carried out considering zero meters of altitude, 50°C of external temperature and a true airspeed of 140 knots.

5.2.5.1 Case 1

As a first case of simulation, the thermal specification of the skin is set to *adiabatic*, hence the skin of the aircraft does not provide any heat exchange with the external environment. This means that the skin is heated by the active LRUs installed inside the bay. In particular, the skin

is subject to radiation, from the LRUs, and to convection with the air heated by the avionics. Since it does not exchange heat with the external environment, it will be subject to an inevitable temperature increasement. Moreover, due to the adiabatic skin, the aircraft airspeed is irrelevant.

In order to ascertain the actual convergence of the simulation, two different plots have been studied. The first one, reported in Figure 5.9, represents the residuals of the numerical computation, measure of the local imbalance of a conserved variable in each control volume. Since those values settle around 10^{-5}, the simulation can be considered valid. A further confirmation comes from Figure 5.10, representing the maximum temperature of the most heated LRU. After a certain number of iterations its value is indeed subject to negligible variations and establishes around 86°C.

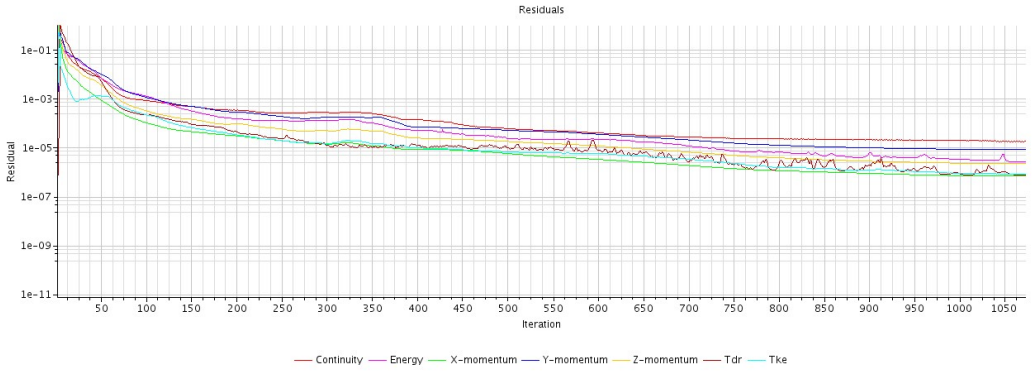

Figure 5.9: Residuals

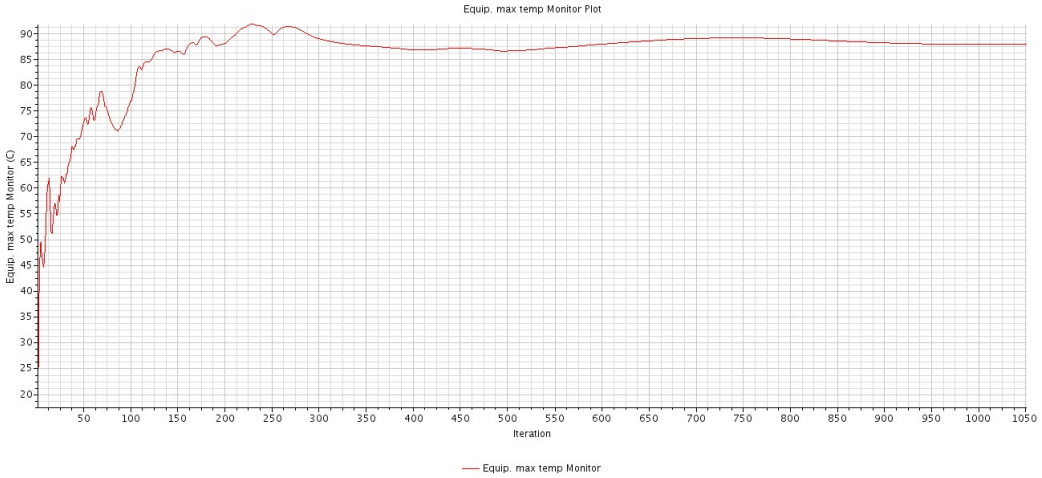

Figure 5.10: Maximum temperature of the most heated LRU

The scalar field representing the temperature is reported in Figure 5.11, Figure 5.12 and Figure 5.13. It is possible to observe the abovementioned heating of the external skin of the aircraft. Nevertheless, the temperature of the LRUs remains inside the allowable limits.

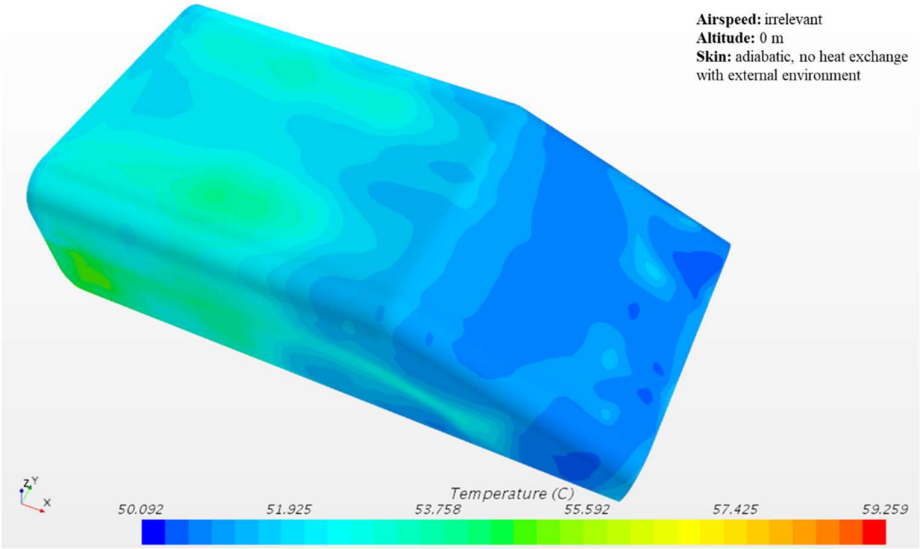

Figure 5.11: Test Case 1 - External Temperature

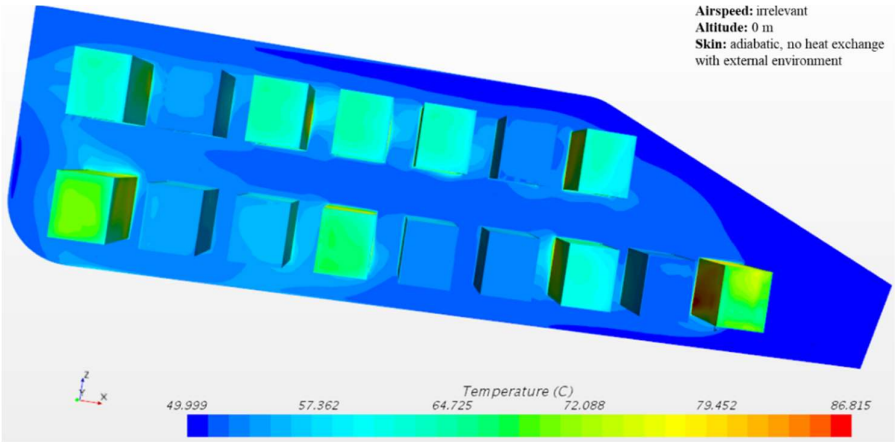

Figure 5.12: Test Case 1 - Internal Temperature - Lateral View

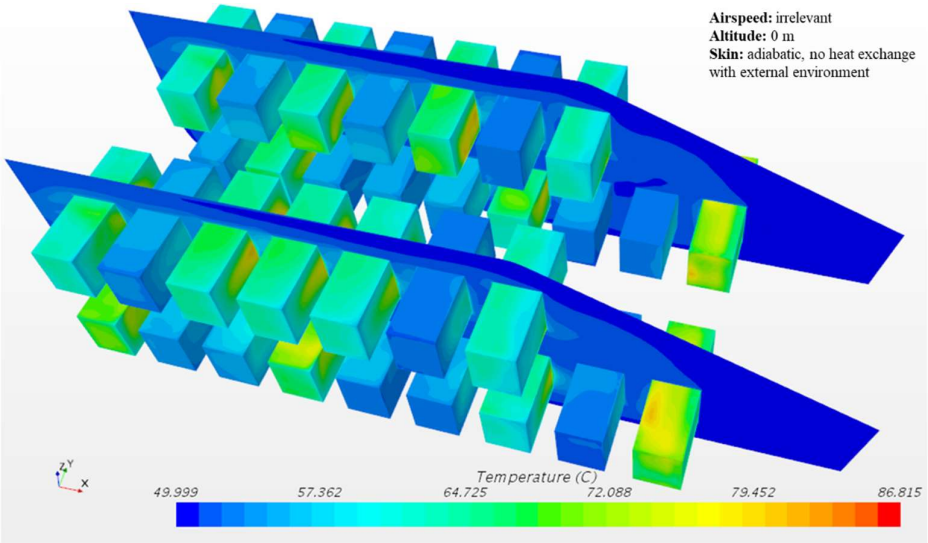

Figure 5.13: Test Case 1 - Internal Temperature

5.2.5.2 Case 2

In this case, the thermal specification of the skin is set to *environment*. This particular condition allows the modelling of heat transfer with external air, whose temperature is set to the recovery temperature of the external air flow (52°C). This model, whose specifications are reported in Figure 5.14, considers indeed the convection with external air but neglects the heat loads due to the solar radiation. Note that this does not necessarily represent an approximation but represents instead a night flight. Differently from case 1, the external skin is now cooled down by ram air, reasons that explains its lower temperature reported in Figure 5.15.

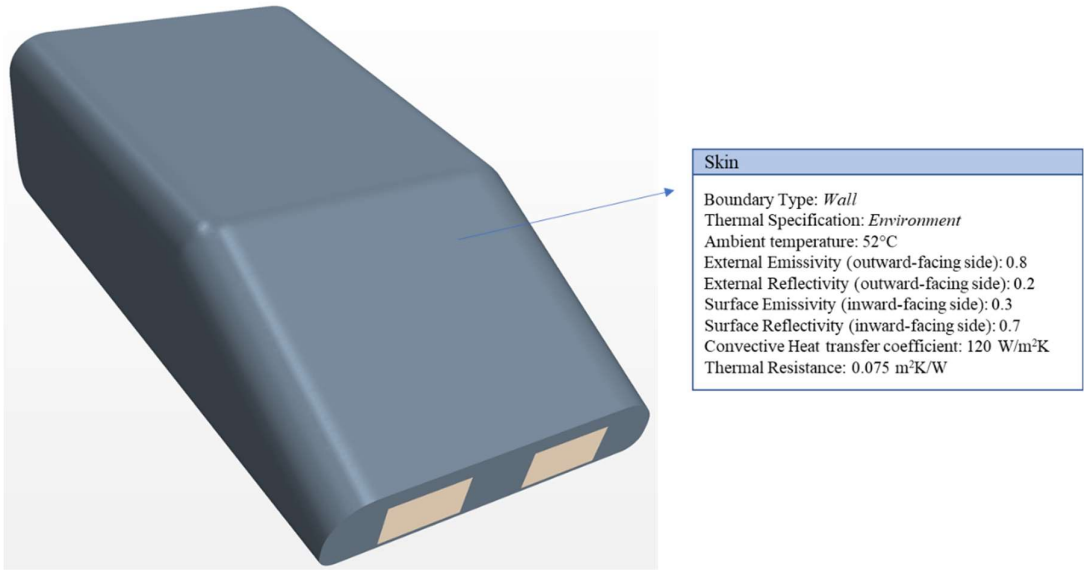

Figure 5.14: Boundary Specification - External View

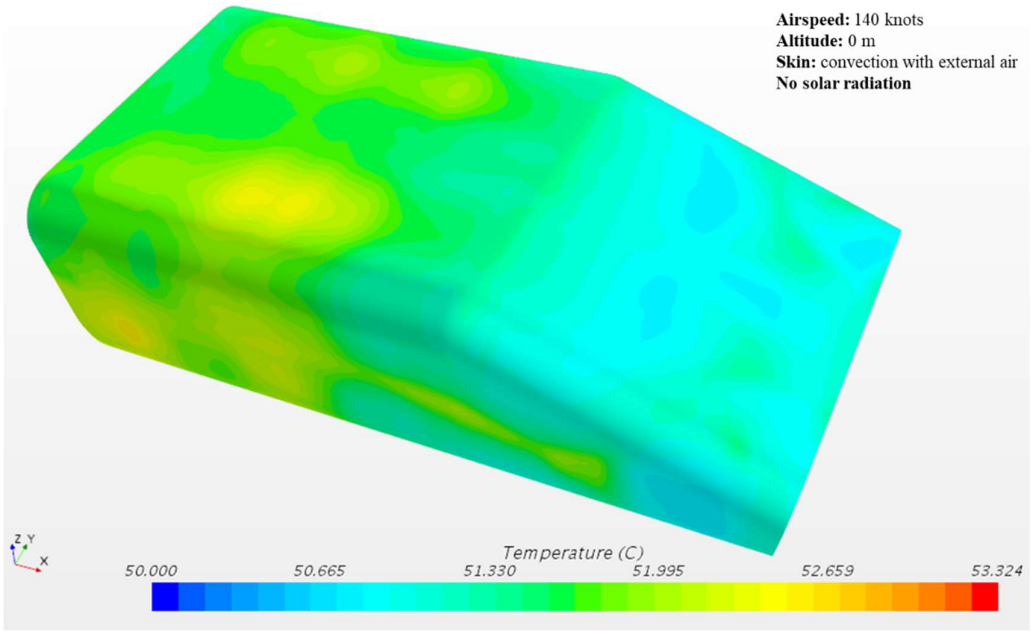

Figure 5.15: Test Case 2 - External Temperature

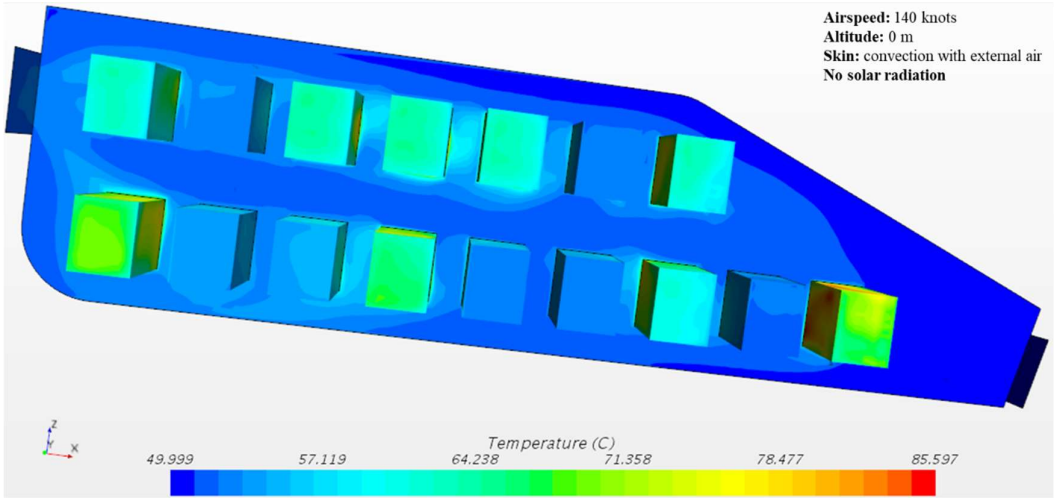

Figure 5.16: Test Case 2 - Internal Temperature – Lateral View

Confronting Figure 5.16 with Figure 5.12 it is possible to notice how the maximum temperature is almost the same: although there is a slight difference in the skin temperature, the internal field is specular. This is due to the low impact of the skin temperature with respect to the avionic heat loads, representing the most significative ones.

5.2.5.3 Case 3

The *environment* skin specification used in Test Case 2 and test Case 3 also allows the computation of the solar irradiation as a function of the elevation of the sun. A series of iterations has been carried out in order to find that the worst condition is the one characterized by an elevation of 90°, reported in Figure 5.18. Figure 5.17 reports, as an example, the direct solar irradiation field for 60° of elevation.

Since we are interested in the worst cooling condition, the case with 90° of elevation it is the one that is used for the following analysis.

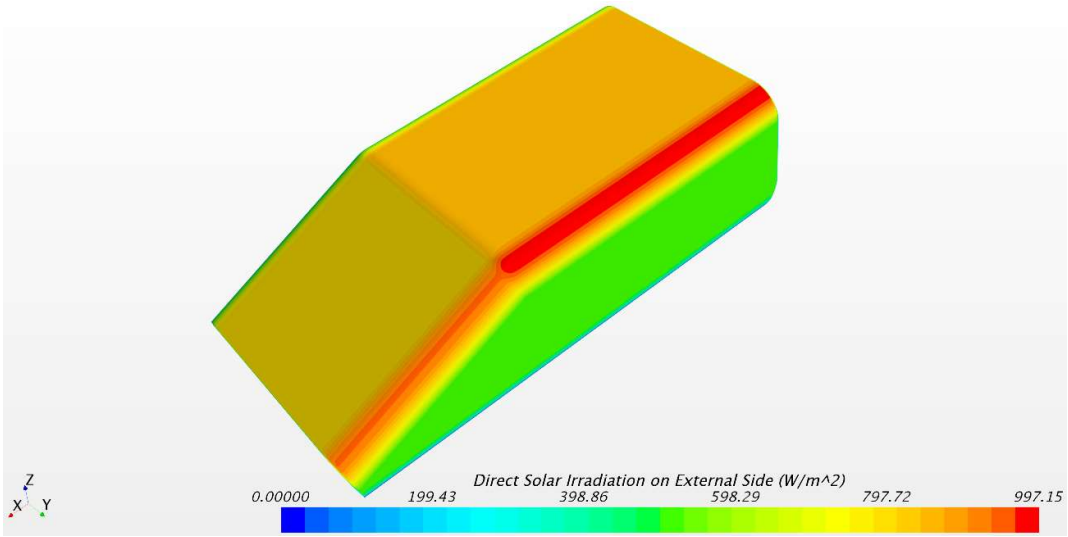

Figure 5.17: Direct Solar Irradiation, 60°

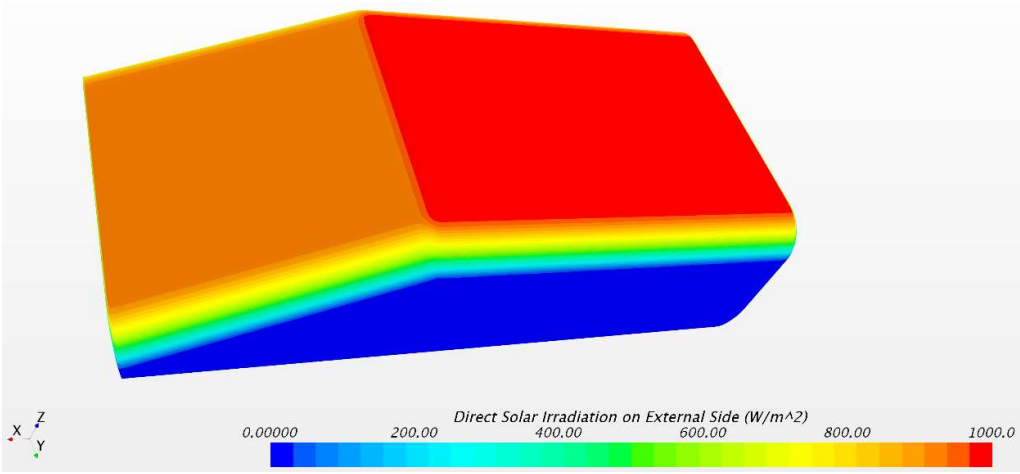

Figure 5.18: Direct Solar Irradiation, 90°

Observing Figure 5.17 and Figure 5.18 it is possible to notice how even the oblique surface of the bay is subject to solar irradiation. Although this is not precisely true, the part of the skin which covers the SATCOM antenna (see Figure 5.1) has a certain level of transmissivity. This means that a portion of solar irradiation actually affects the oblique surface. As a conservative approximation, the antenna cover has been considered completely transparent (transmissivity=1).

The external temperature of the skin is reported in Figure 5.19 and in Figure 5.20. Differently from Test Case 2, the solar irradiation led to an increasement of the skin temperature up to 60°C. Note that this increment is mitigated by the convection with ram air that continuously cools down the surface heated by the sun.

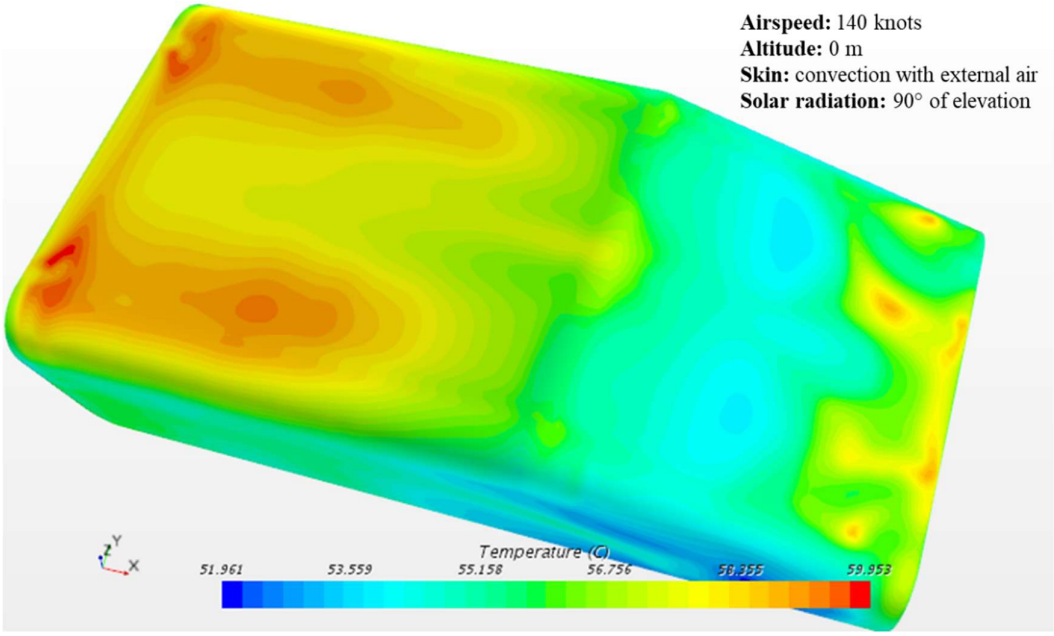

Figure 5.19: Test Case 3 - External Temperature

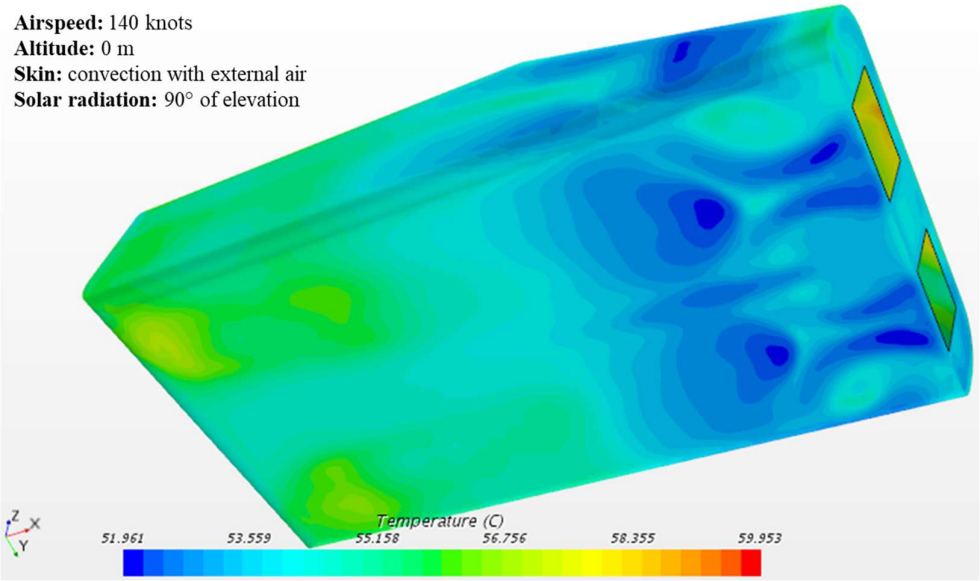

Figure 5.20: Test Case 3 - External Temperature - Inferior View

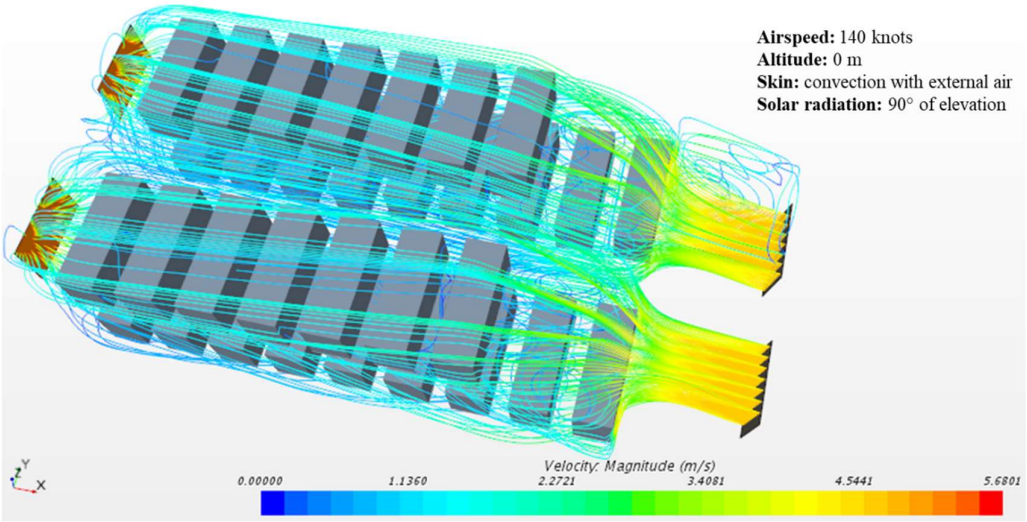

Figure 5.21: Test Case 3 - Velocity Streamlines

As clearly visible from Figure 5.21, Figure 5.22 and Figure 5.23, although the first two LRUs do represent an obstacle for the air flow and are a source of noticeable turbulence, the air does not stagnate around any LRU and guarantees acceptable cooling.

Figure 5.24, Figure 5.25 and Figure 5.26 show indeed the temperature field inside the bay, demonstrating how it reaches, in separated hotspots, a maximum value of almost 88°C. This means that the hypothesized mass flow of 0.75 kg/s is sufficient to be compliant with MIL-STD-1788A - 4.2.6.1.2 for short term operations. Note that the fictional planes, each distant 0.4m from the symmetry plane, allow the visualization of temperature not only on the LRUs but even in the air occupying the available volume of the bay.

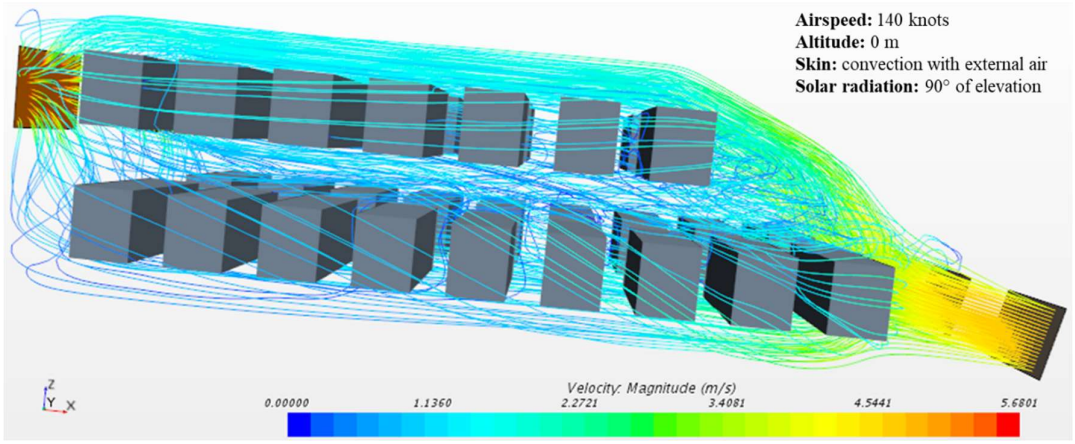

Figure 5.22: Test Case 3 - Velocity Streamlines - Lateral View

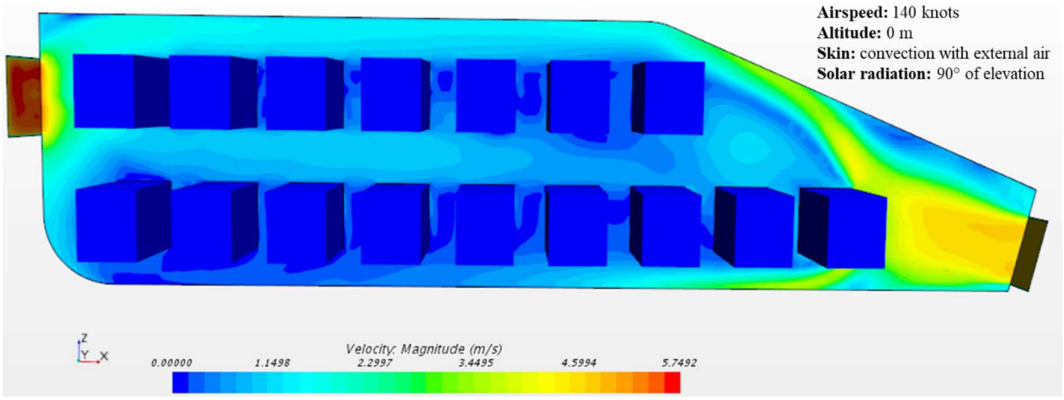

Figure 5.23: Test Case 3 - Velocity - Lateral View

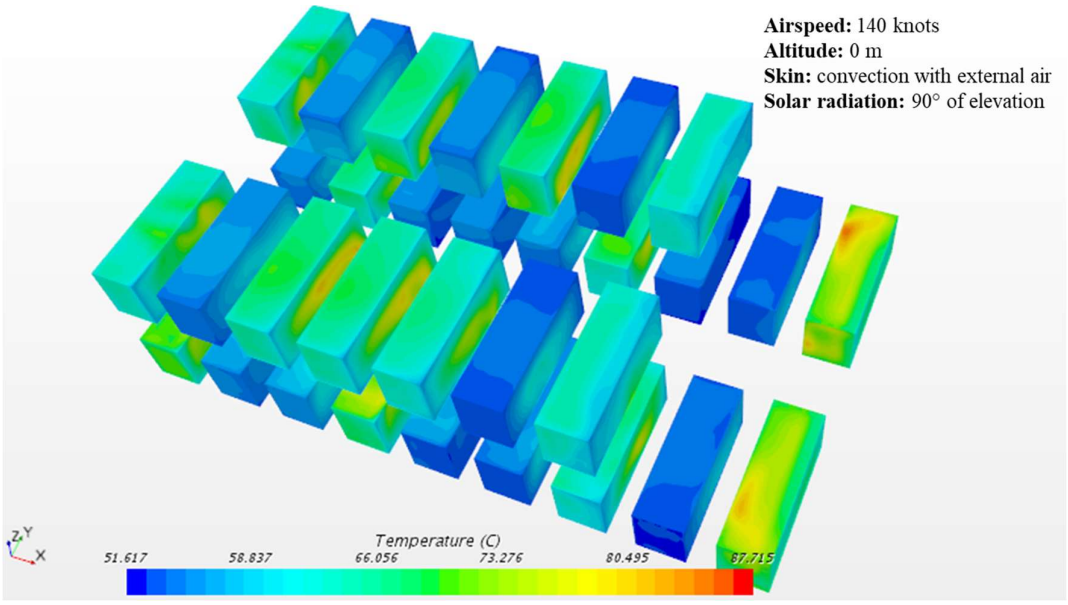

Figure 5.24: Test Case 3 - Internal Temperature – Upper View

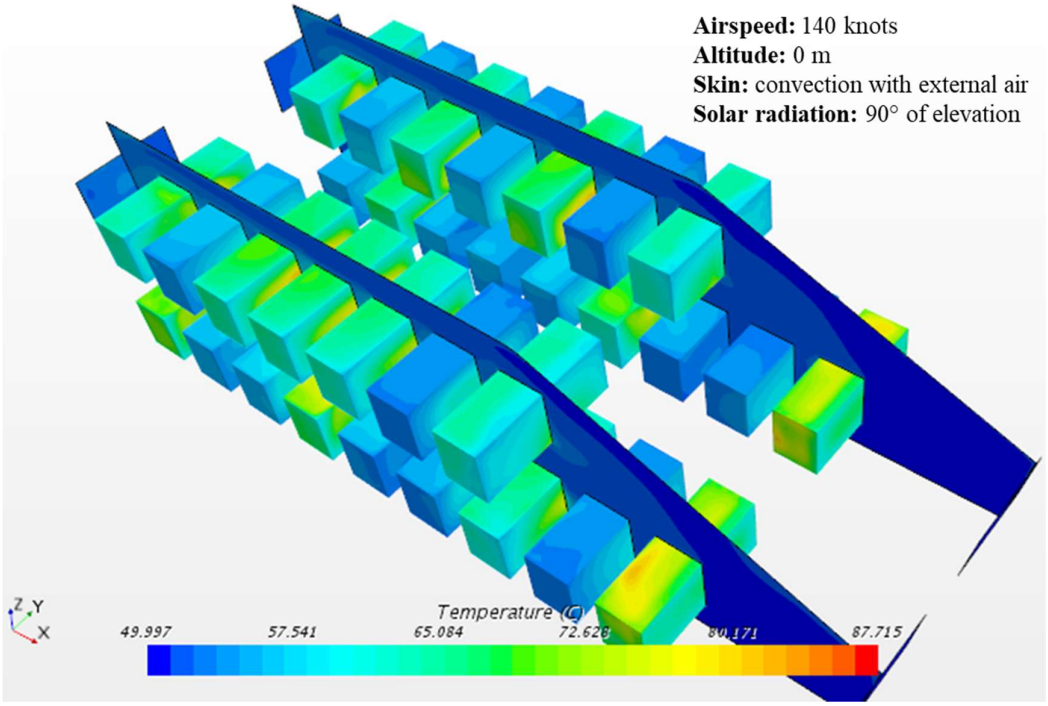

Figure 5.25: Test Case 3 - Internal Temperature

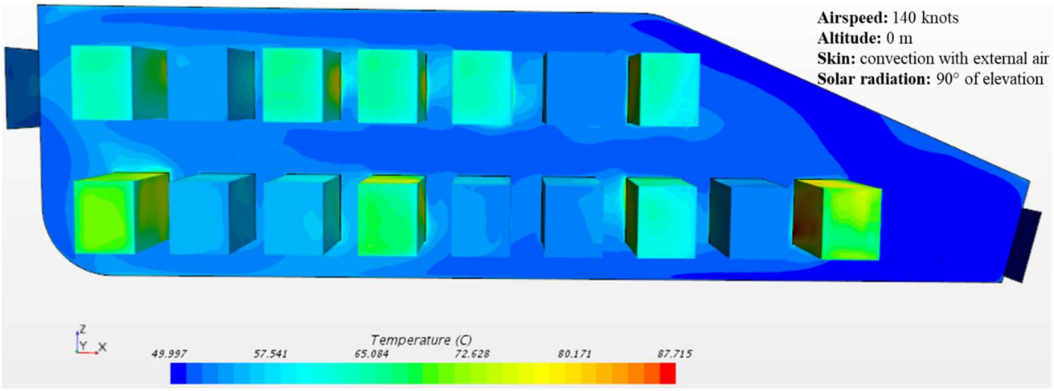

Figure 5.26: Test Case 3 - Internal Temperature - Lateral View

Comparing Figure 5.26 with Figure 5.16 it is possible to notice the effect of solar loads: while the temperature field is almost the same on the lower surface of the bay, the air passing near the upper surface has higher temperature in Figure 5.26.

6 Conclusions

The aim of the thesis was to demonstrate the effectiveness of the model-based approach to the disciplines that concur to the design of an aircraft sub-subsystem.

Every aspect of the design that has been considered relies upon a dedicated software or process. This thesis pointed out the points of interaction between functional analysis, performance analysis and safety assessment: the inputs of each analysis are represented by the outputs of the others. Specifically, the physical architecture is the basis for the FMECA/FMES and the Fault Tree Analyses (FTA). Those analyses concur to the definition of the redundancies and may result in modification of the physical architecture if the safety requirements are not respected.

This high level of integration and multidisciplinarity led to the choice of the functional model as a mean to collect the results deriving from all the conducted analyses. Gathering the fundamental information deriving from different aspects of the design, the functional model assumes indeed the role of a "general model" to which different specialists can refer to.

Moving to potential future developments, it may be possible to furtherly integrate the FMECA/FMES and the Fault Tree Analyses with the system functional model. Coherently with the Model Based System Engineering concept, the development of programs and procedures shall provide increased effectiveness and objectivity.

Moreover, another point of interest regards the interaction of performance and safety analyses with cost estimate. Both acquisition cost and operative cost, are indeed affected by the outputs of the safety assessment such as the number of redundancies and the Development Assurance Levels.

Dealing with the conducted CFD analysis, future development may regard the modelling of the surfaces as actual solids. It is indeed of great interest to ascertain the potential increased realism of the simulation with respect to the computational cost.

Bibliography

[1] STANAG 4671 draft ed.3, "*UAV Systems Airworthiness Requirements (USAR) for North Atlantic Treaty Organization (NATO) Military UAV Systems*", 2014-09

[2] R. Austin, "*Unmanned Aircraft Systems: UAVs design, development and deployment*", Wiley, 2010

[3] I. Moir, A. Seabridge, "*Aircraft Systems: mechanical, electrical, and avionics subsystem integration*", John Wiley & Sons, Ltd, 2008

[4] L. E. Hart, "*Introduction to Model-Based System Engineering (MBSE) and SysML*", Lockheed Martin, Delaware Valley INCOSE Chapter Meeting July 30, 2015

[5] C. Arcuti, "*Applicazione di processi, metodi e strumenti di Systems Engineering al velivolo UAV e ai suoi sottosistemi*", Politecnico di Torino, 2018

[6] SAE ARP4761, "G*uidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*", 1996-12

[7] SAE ARP4754A, "*Guidelines for Development of Civil Aircraft and Systems*", 2010-12

[8] MIL-STD-1788A, "*Military Standard – Avionics Interface Design Standard*", United States of America Department of Defence, 1985

[9] J. Deckert, M. Desai, J. Deyst, A. Willsky, "*Reliable Dual-Redundant Sensor Failure Detection and Identification for the NASA F-8 DFBW Aircraft*", NASA, 1978

[10] J. D. Anderson Jr, "*Computational Fluid Dynamics: The Basics with Applications*", McGraw-Hill, Inc., 1995

[11] Siemens, "*Simcenter STAR-CCM+ User Guide*"

[12] NASA, "Systems Engineering Handbook", 2007

[13] G. Yu, L. Wu, L. Feng, "*Enhancing the thermal conductivity of carbon fibre reinforced polymer composite laminates by coating highly oriented graphite films*", ScienceDirect, 2015

[14] Michael Bauccio, "*ASM Metals Reference Book*", Third edition, Ed. ASM International, Materials Park, OH, 1993

[15] ASHRAE Handbook, "*Heating, Ventilating, and Air-Conditioning Applications*", SI Edition, American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc., 2011