POLITECNICO DI TORINO

Master's Degree in Aerospace Engineering
A.a 2023/2024

MBSE Approach in Aircraft Development

A SySML single model application for multi aircraft development

Academic Tutor
Prof. Paolo Maggiore

Company tutor
Ing. Claudio Pessa

Candidate
Mario Albert

Contents

Acronyms

ADF	Automatic Direction Finder
AF	Architecture Framework
ARINC	Aeronautical Radio Incorporated
ASD	Aerospace and Defence Industries Association of publications
AW	Airworthiness
BDD	Block Definition Diagrams
DBSE	Document Based System Engineering
DME	Distance Measuring Equipment
DoD	Departmet of Defense
DoDAF	US Departement of Defence Architertural Framework
DOORS	Dynamic Object-Oriented Requirements System
EASA	European Aviation Safety Agency
FAA	Federal Aviation Administration
FHA	Functional Hazard Analysis
FMECA	Failure Modes, Effects and Criticality Analysis
FTA	Fault Tree Analysis
GPS	Global Positioning System
GS	Ground Station
IBM	International Businnes Machines
IBS	Internal Definition Diagrams
ICAO	International Civil Aviation Organization

IDEF0	Integraded DEFintion Method 0
IEEE	Institute of Electrical and Electronics Engineers
IEC	International Electrotechnical Commission
IFR	Instrumental Flight Rules
ILRs	Integration/Interface Level Requirements
ILS	Instrumental Landing System
IMC	Instrumental Meteorological Conditions
INCOSE	International Council Of Systems Engineering
INS	Inertial Navigation System
ISO	International Organisation for Standardisation
MBSE	Model Based System Engineering
NAF	NATO Architecture Framework
NATO	North Atlantic Treaty Organization
NAVAIDs	Navigational Aids
NED	North-East-Down
PHA	Preliminary Hazard Analysis
PLRs	Prime Level Requirements
PBN	Performance Based Navigation
QFE	Atmospheric pressure at Field Elevation
QNH	Atmospheric Pressure at Nautical Height
RCM	Reliability Centered Maintenance
RF	Radio Frequency
RNAV	Area Navigation
RNP	Required Navigation Performance
SE	System Engineering
SLRs	Sub-Partner Level Requirements
SOI	System of Interest

SOS	System of Systems
SRBs	Solid Rocket Boosters
SysML	System Moldel Language
TACAN	Tactical Air Navigation System
UHF	Ultra High Frequency
ULM	Unified Modeling Language
VFR	Visual Flight Rules
VMC	Visual Meterorological Conditions
VOR	Very high frequency omnidirectional range

Introduction

The following paper is the result of the work conducted during the thesis period at Leonardo Velivoli. Leader company in the Aerospace, Defense and Security sector, who's activities comprehend project, development, production and support of civil and military aircraft.

System Evolution

In the first 30-40 years of the aviation history, a single man as Bartini, Caproni, or more other, was able to imagine and project an airplane. During the WWII with the radar invention, for the first time, the airplane was able to interface with another system, was although still seen through a non holistic approach. At these days the complexity of systems continues to increase to unprecedented levels, leading to new opportunities, but also to new challenges for the organizations that create and utilize those systems. These challenges persists through all the phases of the life cycle and at any levels of detail. For extremely long life cycles, as those of aircraft, the level of complexity introduces uncertain results, which must be managed. The holistic approach requires a deep comprehension of the interconnection between the aircraft and the external environment to identify the best design solution. This kind of solution development requires the interaction and the coordination of many specialists, companies and research centers. Systems can no longer be treated as stand-alone entities, but are a part of a whole that includes other systems and humans.

System Concepts

A system consists in a set of parts or elements that together exhibit behaviour or meaning that the individual constituents do not. It can be physical, conceptual, or a combination of both. The perception and definition of a particular system, its architecture and its system elements depend on a stakeholder's interest and responsibilities. The system engineering process is a multidisciplinary approach that must develop a balanced system that meet the stakeholder needs. It includes both the management, intended to ensure the cost, schedule and performance are met, and the technical process, used to understand the problem, analyse it, and design the system to achieve the objectives of the hole.[1][2][3]

Depending on the viewpoint a stakeholder's system of interest (SOI) can be viewed as a system element, a being part or a constituent system in a system of systems (SoS) or some times a SoS.[4] [5]

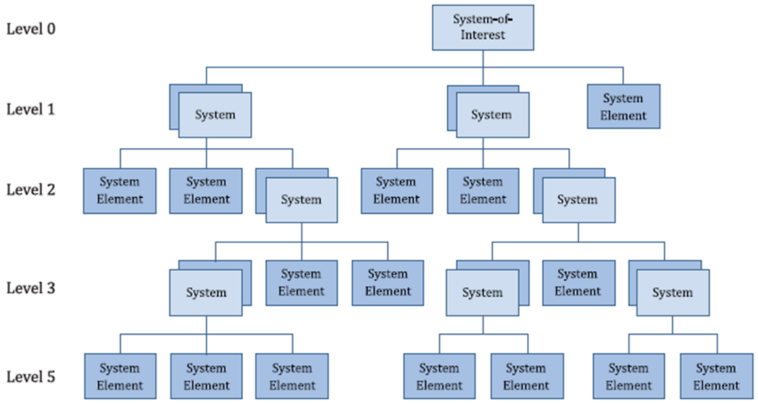


Figure 1: System of interest structure

System elements may include software, hardware, services, and utilization and support resources. Each of which can be implemented to fulfill its requirements. There are different kind of relations between system elements as hierarchies and networks. As in figure 1 a system can be decomposed in his elements due to a better comprehension of the SoI, and so on until the achievement of a level of structure in which all the system elements are understandable and manageable. Which intend also that the specific component or subsystem can be subcontracted to a external company.[6] While in the figure 1 is shown a hierarchical decomposition of the SoI, there are many integrated systems that are more distributed or in network form, a immediate comprehension of what a network form are the satellite systems, in which there aren't principal and sub-systems, but everything works on the same level.

Systems can be classified, any one sharing an interface of any kind with the SoI during any stage of the SoI's life cycle is an interfacing system. Every interfacing system must be considered in the system development. Throughout the life cycle of an SoI, enabling systems must provide essential services. Each of whom supports one or more lifecycle processes of the SoI, often during life cycle stages other than operations. Systems that interact to perform a function are called interoperating systems, which are an important aspect in the context of systems of systems. Interoperating systems are a subset of the interfacing systems.[5]

Products and services are often considered in system families and product line with identification of elements common to different projects, and variants and options per project. Thus variants and options shall be specified for the SoI, to address the solution. This kind of development often benefit from the identification of reuse opportunities between projects, including entire systems, just think at the commercial airplane families, in which there are common projects developed with some differences. The focus of this work is thus to create a model of an airplane system that ca be the basis of multiple different projects.

System and System of Systems

A system of systems (SoS) is a set of systems that interact to provide a unique capability that none of the constituent systems can accomplish on its own. Thus an SoS consists of some constituent systems and any inter-system infrastructure, facilities, and processes necessary to integrate the systems. Each constituent system can be part of also other SoS and have its own life cycle with its own goal and tasks, but interact with the SoS to provide the unique capability to the SoS, different from a collection of systems. [5]

A System can be considered an SoS under the following hypothesis:

- Operational independence: each constituent element of the system works autonomously from the others, fulfilling its own task.
- Managerial independence: each constituent element of the system can be managed autonomously from the others, fulfilling its own task.
- Geographical independence: the constituent elements are not forced to be in the same location, they can be distributed in different places.
- Emergent behavior: the capabilities of the SoS can't be fulfilled from a single constituent.
- Evolutionary development: the system design may change, during its operative life, trough upgrades, and/or modifies of the existing components.

[7][5]

For the development of systems and SoIs are used many computer tools, often released from different companies, or in-house developed. This entails that they were not intended to collaborate with other tools. It is obvious that due to this non-collaboration, during a system development, all the data must be transferred manually trough models and tools. This step involves high human error risks, and it follows that eventual change in a late phase of development implies a high re-work on the other models. Both the manually transfer of data and the re-work are highly time-consuming processes and weighs on the project cost. Additionally this two steps are not engineered for different tools and are susceptible to different software release. In order to manage all these problems in this work will be used a single software in which, tanks to the SYStem Modelling Language, can be developed all the life cycle of a system.

Life Cycle

Every system has a life cycle. It can be described using a model that represent the needs for the system. It includes the activity spectrum for a system, from the first idea, trough the definition of the design, development, production of the system itself and the production plant, the operative life, support, maintenance to the disposal and disassembly.[5] Each of these phases is deeply interconnected to the other, thus, during the development, is necessary to consider the entire life cycle of the system.[1] Especially for a correct evaluation of the risks and the costs of the project. The life cycle comprises one or more stages, that are assembled as a sequence. This phases are iterative, concurrent, or overlapping as needed for the SoI's purpose. [8]

In figure 2 are shown the principal phases of the development of a complex system. A progression trough the life cycle must pass all the reviews and decision gate in terms of processes and performance, both relevant: the first in terms of efficiency and the second in terms of effectiveness of a good developing. Each stage has a specific purpose and each review must verify the satisfaction of the stage's requirements. The decision gates apply specific decision criteria and are used to understand and manage the uncertainties and risk associated to a system.

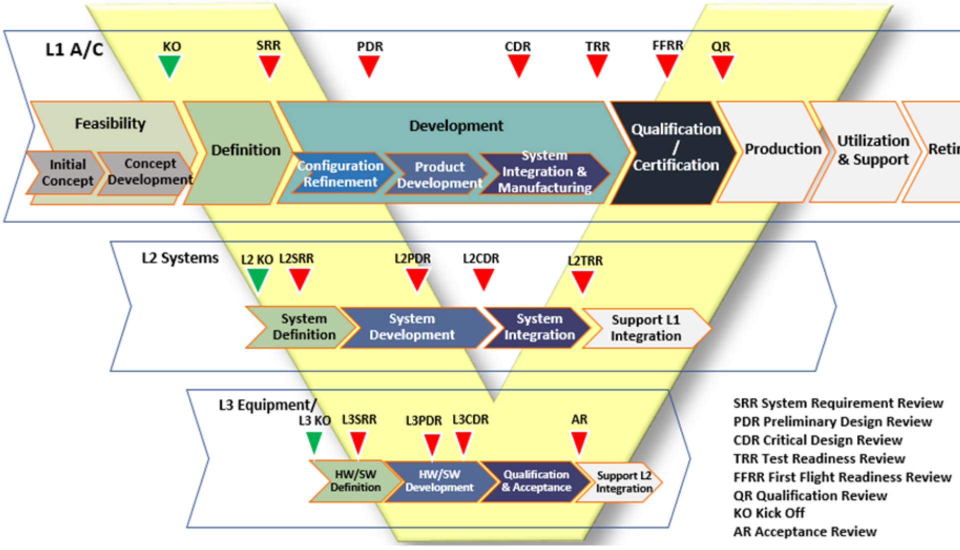


Figure 2: Life Cycle

It is important to specify that each life cycle process is executable, but not mandatory, by a single organization and is strongly related to its outcomes, activities and tasks. Witch can be defined as:

- The outcomes are observable results expected from a process.
- The activities are sets of tasks of a process.
- The tasks are requirements intended to support the achievement of the outcomes.

[5]

The processes that can be performed during the life cycle of a system are divided in four groups as shown in figure 3.

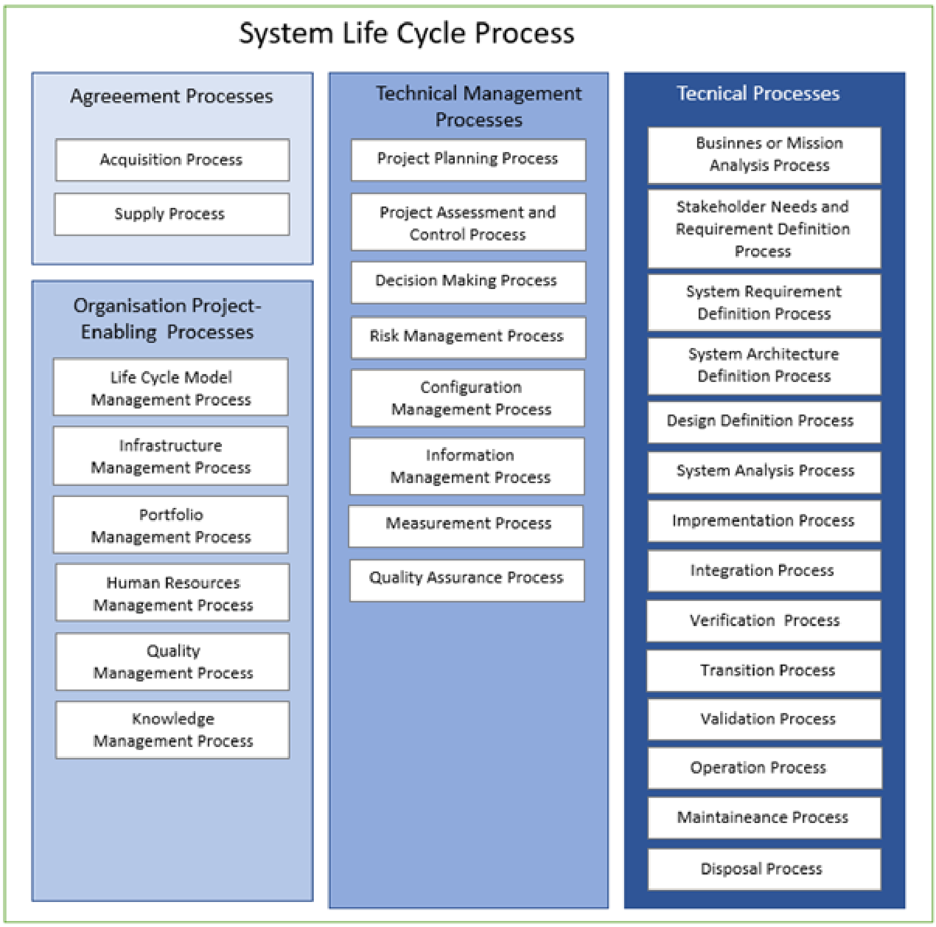


Figure 3: System Life Cycle Process as in[5]

During the agreement processes one organization can act as an acquirer and task another for product or services using agreements. Those allow both to realise value and support strategies for their own. During the organizational project-enabling processes the organization is focused to identify and provide the resource needed to meet the expectation of the stakeholder's. Thus the processes are typically concerned at a strategic level with assets and the risk management for uncertain situations. During the technical management processes the organization decide how to apply the allocated resources to fulfill the agreements. Technical management refers to the process of planning in terms of costs, timescales and achievements; to the identification of the checking criteria of the actions and to the identification of the corrective actions for shortfalls during the project. The technical processes are focused on the technical actions trough the life cycle. Those processes transform the needs into products or services.

This work focuses especially on the following phases as defined in the ISO/IEC/IEEE 15288[5]:

- Knowledge management process
  The purpose of the knowledge management process is to create the capability and assets that enable the organization to exploit opportunities to re-apply existing knowledge. This encompasses knowledge, skills, and knowledge assets, including system elements.
- Information management process
  The purpose of the information management process is to generate, obtain, confirm, transform, retain, retrieve, disseminate, and dispose of information for designated stakeholders. Information management plans, executes, and controls the provision of information for designated stakeholders that is unambiguous, complete, verifiable, consistent, modifiable, traceable, and presentable. Information includes technical, project, organizational, agreement, and user information. Information is often derived from data records of the organization, system, process, or project.
- System architecture definition process
  The purpose of the system architecture definition process is to generate system architecture alternatives, select one or more alternative(s) that address stakeholder concerns and system requirements, and express this in consistent views and models. The system architecture definition activities define a solution based on principles, concepts, and properties logically related to and consistent with each other. The solution architecture has features, properties, and characteristics which satisfy, as far as possible, the problem or opportunity expressed by a set of system requirements (traceable to mission, business and stakeholder requirements) and life cycle concepts (e.g. operational, support). This process transforms related architectures (e.g. strategic, enterprise, reference, and SoS architectures), organizational and project policies and directives, life cycle concepts and constraints, stakeholder concerns and requirements, and system requirements

and constraints into the fundamental concepts and properties of the system and the governing principles for evolution of the system and its related life cycle processes.

- Verification process
  The purpose of the verification process is to provide objective evidence that a system, system element, or artefact fulfils its specified requirements and characteristics. The verification process identifies the anomalies in any artefact (e.g. system requirements, architecture description, or design description), implemented system elements, or life cycle processes using appropriate methods, techniques, standards, or rules. This process provides the necessary information to determine resolution of identified anomalies.

- Transition process
  The purpose of the transition process is to establish a capability for a system to provide services specified by stakeholder requirements in the operational environment. This process moves the system in an orderly, planned manner to be operable in the intended environment, which may be a new or changed environment, e.g., operations or validation. As a result of the transition, the system is functional and compatible with enabling, interfacing, and interoperating systems in the environment. It installs a verified system, together with relevant enabling systems (e.g. planning system, support system, operator training system, user training system), as defined in agreements. The transition process can be used every time the system or system elements are transitioned from one entity or environment to another.

SE and MBSE

New systems are characterised by longer life cycle while the life cycles of individual and specific technologies become shorter. Systems are been viewed ever more in terms of interoperability and SoS context. To respond this engineering requirements, there is an increasing need to develop and produce systems that are robust, reliable and high quality, supportable and cost-effective from a total life cycle prospective. The past experiences with errors in the initial phases that were highly impactfull in the operating phase (i.e the space shuttle program) and the previous factors have shown the critical need of a good developing process.

The System Engineering (SE) is an interdisciplinary branch of engineering that focus on development of complex systems. It can be defined in different ways:

INCOSE:[9] “System engineering is a transdisciplinary and integrative approach to enable the successful realization, use and retirement of engineered systems, using systems principles and concepts, and scientific, technological and management methods. It focuses on:

- establishing, balancing and integrating stakeholders' goals, purpose and success criteria, and defining actual or anticipated customer needs, operational concept and required functionality, starting early in the development cycle;
- establishing an appropriate lifecycle model, process approach and governance structures, considering the levels of complexity, uncertainty, change, and variety
- generating and evaluating alternative solution concepts and architectures;
- baselining and modelling requirements and selected solution architecture for each phase of the endeavor;
- performing design synthesis and system verification and validation;
- while considering both the problem and solution domains, taking into account necessary enabling systems and services, identifying the role that the parts and the relationships between the parts play with respect to the overall behavior and performance of the system, and determining how to balance all of these factors to achieve a satisfactory outcome.

Systems Engineering provides facilitation, guidance and leadership to integrate the relevant disciplines and specialty groups into a cohesive effort, forming an appropriately structured development process that proceeds from concept to production, operation, evolution and eventual disposal. Systems Engineering considers both the business and the technical needs of customers with the goal of providing a quality solution that meets the needs of users and other stakeholders, is fit for the intended purpose in real-world operation, and avoids or minimizes adverse unintended consequences.

EISNER:[10] “System engineering is an iterative process of top-down synthesis, development, and operation of real-world system that satisfies, in a near optimal manner, the full range of requirements for the system”

FAA:[11] ”System engineering is a discipline that concentrates on the design and application of the whole (System) as distinct from the parts. It involves looking at a problem in its entirety, taking into account all the facets and all the variables and relating the social to the technical aspect.”

System engineering is well applied if the following tasks are followed:[1]

- A top-down approach is required, viewing the system as a whole.

- A life cycle orientation is required, including all the other phase's impacts on the design.
- A deep comprehension of the requirement is needed to relate those to specific design goals.
- A team approach is required throughout the system development to ensure an effective and efficient design process.
- An interface management is required to monitor the design of the system and to highlight the problems.

In figure 4 is shown the relation between the committed life cycle cost due to defects fixing and the time (or phase of development). It is self-evident as the SE purpose of manage the project with a life cycle prospective is intended to identify and manage defects and criticality in the early phase of the project. Thus due to reduce the cost and to avoid errors propagation to a catastrophic status.

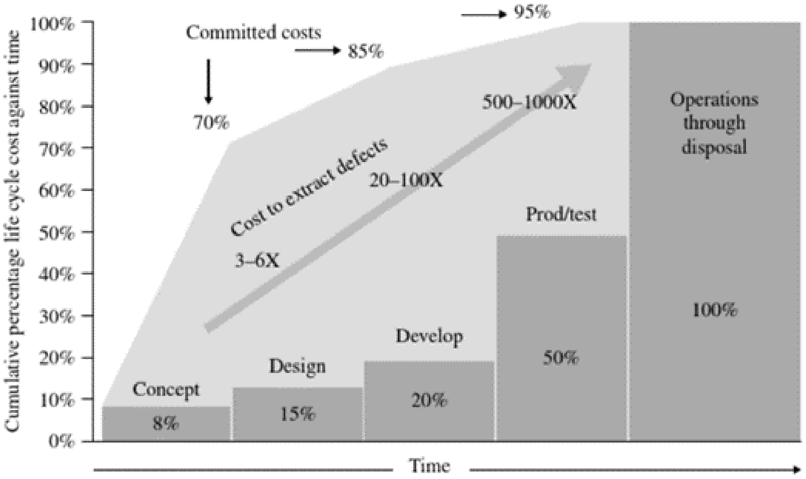


Figure 4: Cost vs Time

One of the advantages of the SE is to support the traceability through the development of the ideal model from the preliminary project to the definition of a specific system, not falling into errors like omissions or false assumptions. Thanks to its easy comprehension and interconnection it will simplify the configuration management process and the information management process. This method allows an immediate understanding of the impact of any modification on the entire system permitting an immediate error detection. The well-defined structure of the development phases guide the decision helping the integration of the results of the different subjects; as modelling, simulation, risk and cost analysis management, and more. The system engineering process includes the basic steps of requirement analysis, functional analysis, requirement allocation, design optimization and trade-offs, and so on. This steps are per se iterative but not necessarily performed in a serial sequence. [1] SE is not a discipline as aerospace engineering or mechanical engineering, but involves effort in optimization the developing processes in all the classical discipline. To support the SE and help understand all the connection trough the different areas were developed tools and new methodologies as Model Based System Engineering (MBSE).

Modelling refers to the process of developing a model as a conceptual representation of some physical phenomenon, with some affinities with the reality in the interest areas, and as simplification of the real phenomenon in the other fields. Conceptual models can be described using SysML, a visual language developed from the ULM. MBSE is a formalized method that uses models ad center of complex system's design, overcoming in managing capabilities the Document Based System Engineering (DBSE).[12] MBSE needs tree components to be effective: a platform on which the system can be modelled, a language capable to represent the system and a method through which the model can be implemented.[13][14] The platform used for this work is the software IBM Rhapsody, that support the language SysML.

Objectives

The goal of this work is to analyse and comprehend the process of modelling of a complex system as an aircraft through the MBSE, this model should work as basis for future different project, being a "black box" view of the functional and logic behavior of a so complex system.

It will be discussed a multi-level model with a higher focus on subsystem integration and function tracing to ensure the project consistency. Through the software IBM Rhapsody will be created a model of an aircraft to support the process and analyse the advantages of the MBSE compared to other engineering methods. And to identify and discuss possible future evolution of the possibilities ensured by this method. A key point of this work is to analyse the possibility of an integrated model that cover all the life cycle process, involving many different engineers that have to work effectively together, without going too deep in the performance optimization process, but to investigate the functional level.

Chapters Introduction

Chapter 1

In Chapter 1 will be presented The system engineering model, defining the general structure of the difference between the civil process and the military process in terms of user needs and partecipation through the developing process. Will be then discussed the stakeholders needs and the equivalent requirements and functions decomposition. In the end will be discussed the physical model of the Navigation System through the requirements and theyre allocation to physical subsystem.

Chapter 2

In Chapter 2 will be discussed the strategies of system analysis and the possible design optimisation process. In the firs section will be presented the hazard analysis that can be performed through the developing and will be presented an example of a FHA. Will be than analysed the system structure of the Navigation system, all the binding interconnections between functions, requirements, physical components, interface type, and more. Is finally discussed the system activities decomposition through an example of a fulfillment of a single function from the Navigation System.

Chapter 3

In this chapter will be presented the analysis and conclusion of the conducted work and the possible future possibilities that the MBSE can satisfy.

Chapter 1

The System Engineering model

The SE gives emphasis on a top-down, integrated, life-cycle approach to system design and development. The first step of this approach is an initial definition and the identification of the consumer needs, then it proceed with the feasibility analysis, development of operational requirement, functional analysis, allocation of requirements and development of the top-level architecture.[1] Follows an iterative process of assessment and validation. A special attention is placed on the requirements traceability. A new one may evolve or change throughout all the life cycle, i.e. a new system performance has been identified or the production rate is speeded up. In the event that this happens, it does require a change in approaching a system design.

The SE process generally starts with the identification of a need, based on a deficiency or on new targets. In the specific case of aircraft development, a differentiation between civil and military planes should be done .

- The civil process, most of the time, is commenced by the manufacturer company that identifies new market opportunities or improves the existing requirements. The user contribution is not considered in the first phases of development, but only once the project has already reached a final configuration and system design.
- The military process, instead, involves the final user from the early stages of the developing. The development process can start in two main ways. The manufacturer company responds to a specific final-user request or the manufacturer company starts a project in a joint-venture whit the country defence ministry and other foreign companies and they're countries.

Both military or civil user needs can be expressed trough Architecture Framework (AF) defined as:

> "An architecture framework establishes a common practice for creating, interpret-

> ing, analyzing and using architecture descriptions within a particular domain of application or stakeholder community.” The ISO/IEC/IEEE 42010[15]

The AF can be used to define different architectures in different system levels. It should describe a developing method to project systems in terms of set of elements, showing how this should be integrated and how they must interact to fulfill the required function. Because of the differences between different companies and different systems there is not a unique definition of AF and there is not only one AF, but more than 60 were developed to specify different needs. The more used in the Aerospace field are the NAF (NATO Architecture Framework) and the DoDAF (US Department of Defence Architectural Framework).[16]

1.1 Model building

The developing process starts with the identification of the stakeholders and their needs, including the purchase and the users of the system, which in the case of a plane includes the pilots and eventual passengers. The stakeholder needs depends also on the market segment, such as acrobatic, fighter, cargo or passenger aircraft. In fact at each segment belong different needs: i.e. a acrobatic must be highly maneuverable and light, a cargo instead must carry a high weight, totally in contrast with the acrobatich plane needs. For the purpose of this paper is not relevant which kind of airplane is, the developing process is common through all the different families. Other important stakeholders needs are the ones that may be affected throughout the system’s life cycle, including manufacturers and maintainers. The last kind of stakeholders are organisation and governments, that impose their needs via laws, regulation and standards. It is obvious that not each stakeholder’s concern is of equal importance, therefor they must be analysed to be properly weighted. Once identified and classified the stakeholders needs, the following step in the model building is the definition and analysis of the requirements, intended as the translation of those needs in a formalized form. An example of the importance of these analysis is the case of the SRBs of the space shuttle, which design was determined over two thousand years ago by the width of a horse’s as. In fact the SRBs were shipped by train from the factory to the launch site. The railroad line happens to run trough a tunnel in which the SRBs had to fit. The dimension of the railroad was decided because if they tried to use a different wheel spacing, the wagon wheels would brake more often on some of the old, long distance road in Europe. Those roads were build for the first time by the Imperial Rome for their legions. And so an important requirement for the most advanced transport system for the time was imposed by the Roman Empire.

There are different classification possibilities for the requirements. Surely is really important to understand the difference between airworthiness (AW) and performance requirements. The AW requirements are defined by the regional regulatory agency, such as EASA in Europe and FAA in USA, those requirements are clearly expressed in the regulation rules and does not need any translation. The missing compliance to one of more of this requirements implies the loss of the Type Certificates and thus the airworthiness of the plane. Instead, the performance requirements are, often, client side needs, are not involved in the certification process, are translated and decomposed in engineer useful requirements[16].

Another proposed classification is:

- Prime Level Requirements (PLRs)
- Sub-Partner Level Requirements (SLRs)
- Integration/Interface Level Requirements(ILRs)

It is necessary to point out one important thing: requirements are not defined only in a top-down approach. They are usually defined in the process in a cross-sectional way. This means that requirements are not always defined in the form of "parent-child", but more often, defined without a higher correlation to a parent. The PLRs are high level requirements derived from a higher level: the customer or the subcontractant company. The SLRs are developed from the decomposition of the PLRs and are necessary do break the requirements in manageable tasks, the SLRs are used to subcontract part of the work, and are seen as a PLRs by the low level company. The management of the requirements is a crucial step to guarantee the airworthiness of the aircraft because the higher level company does will not develop or manage the lowest level of systems and component, but will be responsible for the final integration of the full-scale aircraft. The ILRs are the basis for the correct development process of components that must interact in any way and are not developed from the same person/organization. In other words are the linkage between all the components and developing teams.

To analyse and manage the stakeholder needs the SySMl uses the Use-Case diagrams, which allows the developer to simply define in a black-box view all the stakeholder and their interaction with the system. Throughout this work those users and needs are assumed well known, so not analysed but just presented, because the case study is a common configuration of an airplane, not involving any special need, but instead assumed to be a common basis for many different types of airplane.

1.2 Functions

A function is one or a series of action that the system must perform or that must be performed to bring the system back to his operational status. It responds to the question "what" and not "how". It is very important to understand all the task required to the airplane in order to decompose them in functions, "objects" easy to analyse and allocate to physical systems. The decomposition of the function in levels it is not unique, there are always common elements as "to accelerate the airplane", or "to provide lift", but every one can decompose the tasks in a different way.

In figure 1.1 is represented a classical decomposition of the high level function of the aircraft. This representation is from a Pilot/user view, and shows a black-box[1] view of the tasks that a aircraft must fulfill. In this phase the classification of the functions does not follows any rule but the preferences of the developer or company in organizing them. [17] It is important to describe the customer requirements trough a functional viewpoint in order to avoid any commitment to a specific design concept in a preliminary phase. The basic objective is to define the required function before defining how this function will be accomplished. [1] In fact the physical definition of the system must be a consequence of the functional decomposition and must not influence it. It is obvious that the feasibility of a physical system should be considered, but in this phase only in a logic check of the coherence of the defined functions.

The functional analysis is a critical step in the early design, and serves as a basis for subsequent activities as FTA, FMECA, RCM, etc. Usually multiple functional analyses are performed to determinate the best system decomposition. But for the purpose of this study it is not required any transition from a black box view to a white box[2] view, therefore there were not performed any analyses. Should be pointed out that once performed all these analysis, there is not a unique design solution, instead are highlighted all the advantages and disadvantages of each analysed configuration. Will then the developer/company choose which one will fit better the company goals, in terms of performance, and the company possibilities, in terms of time and money that will be required.

---

[1] A black-box is a system that can be viewed in terms of input and outputs, without any knowledge of his internal components and behavior

[2] A white-box is a subsystem whose internals can be viewed but usually not altered.

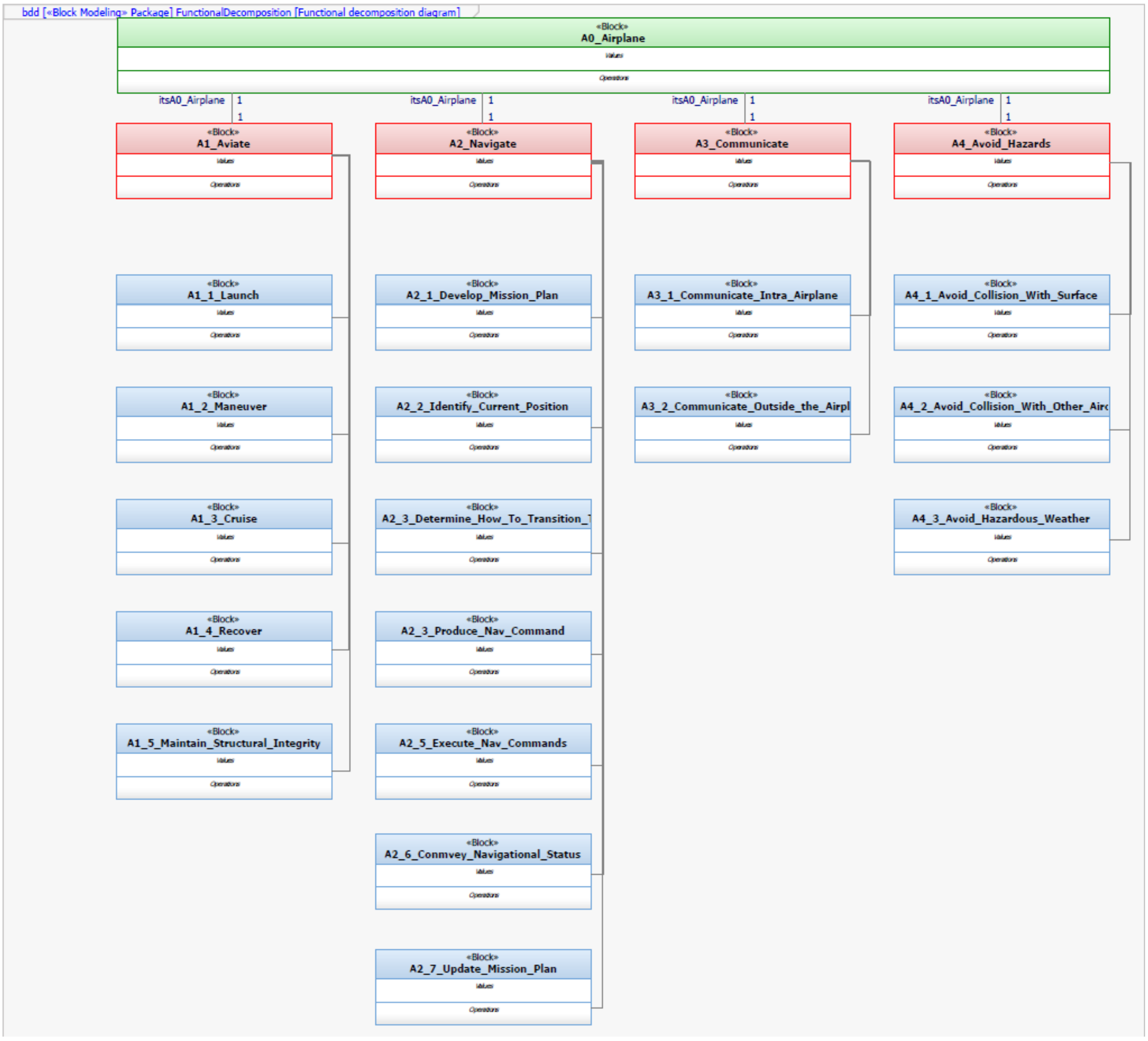


Figure 1.1: Functional Decomposition

1.3 Systems

Considering a plane as a well known system, a system decomposition of a aircraft can be the one proposed in the ASD S1000D[18] shown in figure 1.2. It represent all the aircraft systems except for the Helicopter's only ones, not considered in this work.This because the helicopters are too different to be considered in a common platform design basis. In red are represented the military only systems, typically tactical or armament management ones, and in blue all the common systems. In the figure all the boundaries between the systems are well defined, in the reality often it is not simple to identifies those boundaries, especially for low level components that can be parts of one or many different systems at the same time. The figure does not show the interface between all the systems, some of whom are often of the same kind (i.e. electric power transfer, hydraulic power transfer, information transfer, etc..)

The ASD S100D has been chose for its purpose: is an international specification for the procurement and production of technical publication, useful also for non-technical publications. It was developed by the Aerospace and Defence Industries Association of Europe (ASD) emphasizing the accuracy of the classification proposed. Once defined the product, that can be any platform or system and the task to develop, it's purpose is to support the production of Operational and maintenance documentation, facilitate the information learning in the development process and the development of new skills. This classification and decomposition is the key start for any kind of airplane, in fact any major configuration choice has a direct impact in the white box view of this picture.

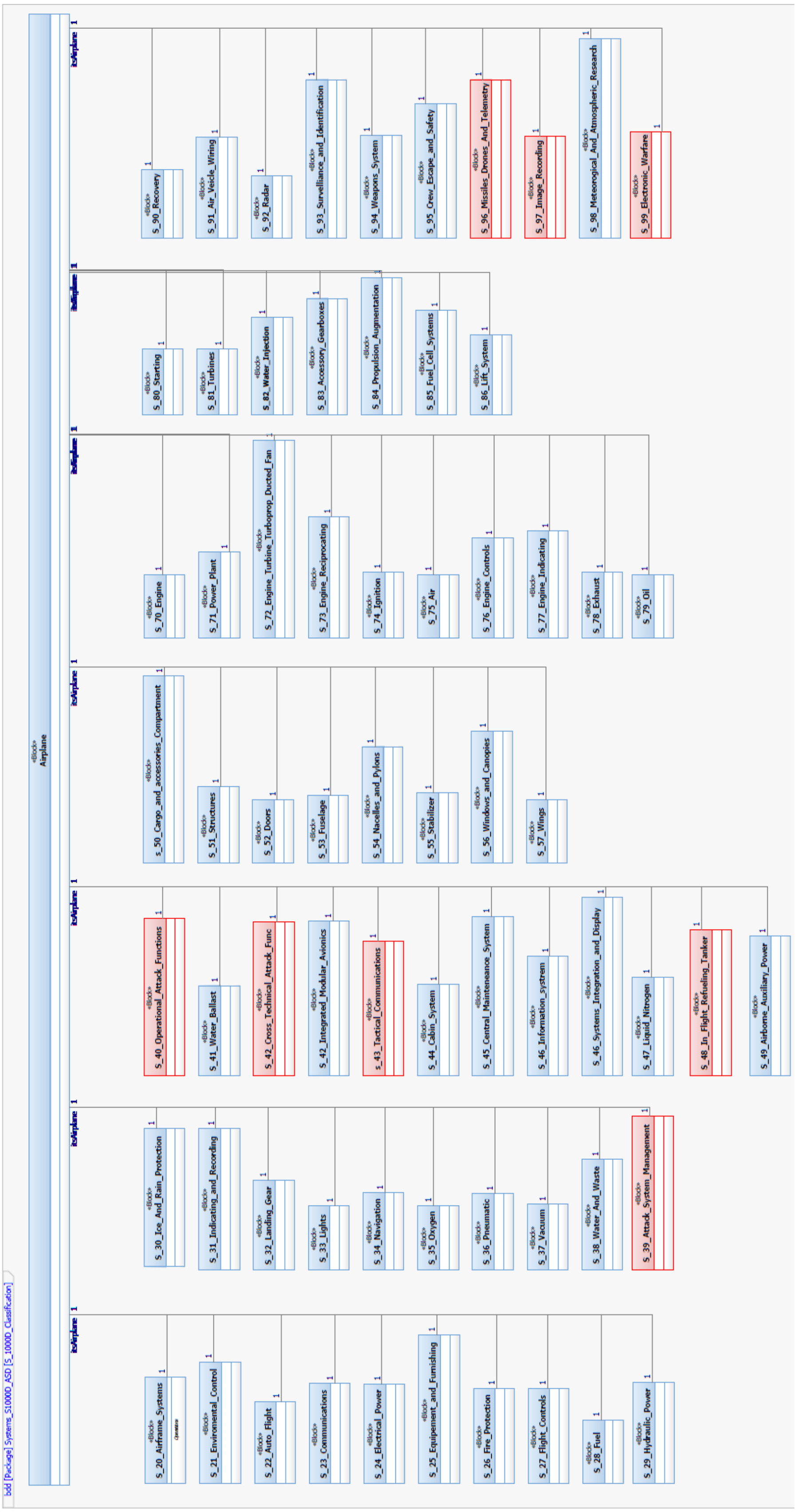


Figure 1.2: ASD S1000D

1.4 Navigation System

The navigation system can be defined as: ”Those units and components which provide air vehicle navigational information. Includes VOR, Pitot, Static, ILS, Flight Director, Compasses, Indicators, ecc.” ASD S100D[18]. It’s purpose is to provide information to the pilots or other systems about the position, velocities and accelerations of the aircraft, in order to help maintain a correct flight path.

This work will propose a analysis of the developing process in the MBSE approach of the Navigation System.[19][20]

1.4.1 Requirements

As seen above, one of the highest function of an aircraft is to provide navigation capabilities, this high level function so expressed is useless, it must be decomposed in smaller and manageable requirements which can be allocated to a specific phisycal system. In figure1.3 is shown a classical decomposition from the high level requirement for two levels, the first identifies the information desired by the dimensional unit of the data used such as distance, velocity, etc.. In this case the dimensional analysis of a data is used as a classification method, more often is one of the most important interface requirement, in can also be used as check for the data corruption. The second level associates to every information a physical meaning: the distance can be vertical distance from the sea, vertical distance from the airport, latitude, etc.. In figure are shown also the stereotypes of the connectors between different level’s requirements. It is important to note that different types of linkage can be used enabling differentiation and weighting to different relations.

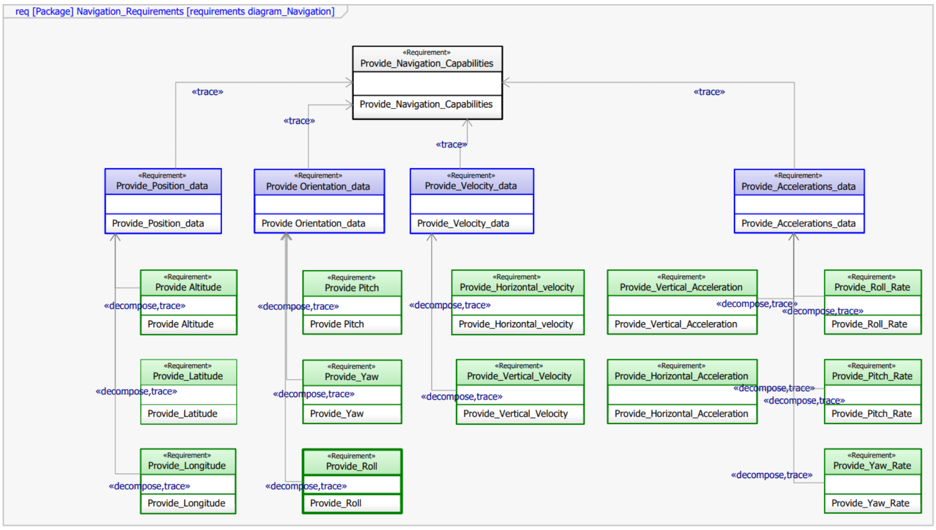


Figure 1.3: Navigation Requirements

This figure provide not only a clear decomposition of functions, but shows also how this splitting helps to identify in a unique way every sub-function needed to fulfill the higher level ones. It can be used as a "check list" in the validation or certification phases.

Once defined the level of detail needed to manage the requirements, the models must be translate in design solution verifying the fulfillment of each requirement throughout the process. The next step of the developing process is then to define the physical components that will constitute the navigation system, analyze them, implement improvements and test the hole system to validate it.

The choose of the subsystem was consequence of two consideration:

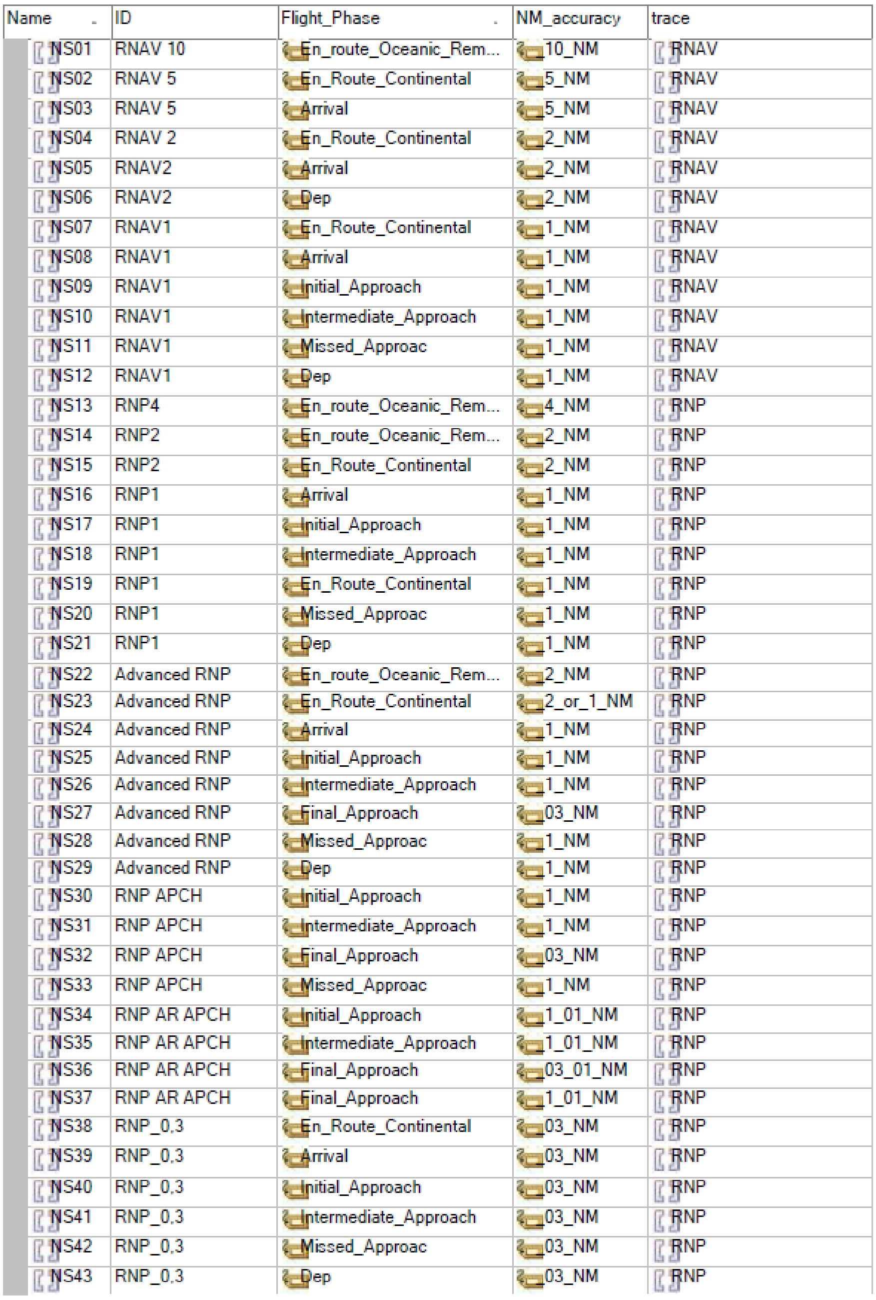
- The focus of this work is not the technical development of a single system, but the use of the MBSE approach through SySML to create a model of the developing process.
- The final system should be compliant to the navigation specification of the region in which it should be used. (i.e. ICAO Navigation specification).These specifications does not constitute regulatory guidance material against which either the aircraft or the operator will be assessed and approved.

  In other words: the navigation specification provides the technical and operational criteria but does not imply a need for re-certification. Those are performance requirements imposed by or countries or clients, they does not involve the certification type. Although the non-fulfillment of these requirements forecloses a country's airspace to that type of plane. [21]

Therefor it has been chose to use all existing subsystems.

In the figure1.4 are shown in example some ICAO Navigation Specification of two different families of Performance-Based Navigation (PBN): the Area Navigation Specification (RNAV) and the Required navigation performance specification (RNP). Both are expressed in terms of navigation minimal accuracy accepted for a specified class and a specified flight phase. [17]

The performance-based navigation is the basis for defining the requirements of the performance for navigation equipment. These Specification are used to provide specific implementation guidance in order to reduce the risks correlated to the uncertainly of navigation information. The area navigation (RNAV) enables airplanes to fly on any flight path using NAVAIDs, rather than fly through an airway. The Required Navigation Performance (RNP) allows the aircraft to fly along a precise flight path optimising the use of airspace due to the exceptional accuracy and important ability to determinate the airplane position with accuracy and integrity. The RNPs increase safety reducing operational costs and inefficiencies such as time and fuel saving avoiding non-precision approaches.



Name	ID	Flight_Phase	NM_accuracy	trace
NS01	RNAV 10	En_route_Oceanic_Rem...	10_NM	RNAV
NS02	RNAV 5	En_Route_Continental	5_NM	RNAV
NS03	RNAV 5	Arrival	5_NM	RNAV
NS04	RNAV 2	En_Route_Continental	2_NM	RNAV
NS05	RNAV2	Arrival	2_NM	RNAV
NS06	RNAV2	Dep	2_NM	RNAV
NS07	RNAV1	En_Route_Continental	1_NM	RNAV
NS08	RNAV1	Arrival	1_NM	RNAV
NS09	RNAV1	Initial_Approach	1_NM	RNAV
NS10	RNAV1	Intermediate_Approach	1_NM	RNAV
NS11	RNAV1	Missed_Approac	1_NM	RNAV
NS12	RNAV1	Dep	1_NM	RNAV
NS13	RNP4	En_route_Oceanic_Rem...	4_NM	RNP
NS14	RNP2	En_route_Oceanic_Rem...	2_NM	RNP
NS15	RNP2	En_Route_Continental	2_NM	RNP
NS16	RNP1	Arrival	1_NM	RNP
NS17	RNP1	Initial_Approach	1_NM	RNP
NS18	RNP1	Intermediate_Approach	1_NM	RNP
NS19	RNP1	En_Route_Continental	1_NM	RNP
NS20	RNP1	Missed_Approac	1_NM	RNP
NS21	RNP1	Dep	1_NM	RNP
NS22	Advanced RNP	En_route_Oceanic_Rem...	2_NM	RNP
NS23	Advanced RNP	En_Route_Continental	2_or_1_NM	RNP
NS24	Advanced RNP	Arrival	1_NM	RNP
NS25	Advanced RNP	Initial_Approach	1_NM	RNP
NS26	Advanced RNP	Intermediate_Approach	1_NM	RNP
NS27	Advanced RNP	Final_Approach	03_NM	RNP
NS28	Advanced RNP	Missed_Approac	1_NM	RNP
NS29	Advanced RNP	Dep	1_NM	RNP
NS30	RNP APCH	Initial_Approach	1_NM	RNP
NS31	RNP APCH	Intermediate_Approach	1_NM	RNP
NS32	RNP APCH	Final_Approach	03_NM	RNP
NS33	RNP APCH	Missed_Approac	1_NM	RNP
NS34	RNP AR APCH	Initial_Approach	1_01_NM	RNP
NS35	RNP AR APCH	Intermediate_Approach	1_01_NM	RNP
NS36	RNP AR APCH	Final_Approach	03_01_NM	RNP
NS37	RNP AR APCH	Final_Approach	1_01_NM	RNP
NS38	RNP_0,3	En_Route_Continental	03_NM	RNP
NS39	RNP_0,3	Arrival	03_NM	RNP
NS40	RNP_0,3	Initial_Approach	03_NM	RNP
NS41	RNP_0,3	Intermediate_Approach	03_NM	RNP
NS42	RNP_0,3	Missed_Approac	03_NM	RNP
NS43	RNP_0,3	Dep	03_NM	RNP

Figure 1.4: Navigation Specification Example

1.4.2 System Feasibility Analysis

In the early stages of the development the focus is on the creativity, every function proposed that can be useful to the final product is considered and studied. To ensure a good design from the beginning it is important to identify all the feasible functions from all the proposed. The most rigorous ones should be selected to define the design requirements. In other words the functions are classified in terms of stinginess, the design requirements reflects the crucial functions for the project, i.e. for the Bell X-1 one of the most important requirements was to be capable to breaking the sound barrier. It is important that all the design possibilities are evaluated to ensure that also the proper approach is selected. The feasibility analysis is accomplished to evaluate the different design possibilities through the technological approaches that may be considered to fulfill a specific requirement. [1] The overall process consists in the identification of all the possible design approaches to analyse them in terms of effectiveness, performance, production and maintenance cost, logistic support; and define the recommended approach, these analysis results are not mandatory and may be interpreted from the managerial chief of the project. In case sufficient information are not available a research project activity to develop new specific technologies may start. The feasibility analysis has a great impact on the project, not only in terms of future operational characteristics, but also though all the other life-cycle phases, in fact during the analysis the costs of the operational life and the maintenance are considered. Once again in this work, it is assumed that the systems in analysis are well known, and thus the system feasibility analysis was not conducted.

1.4.3 Subsystems

The navigation system can be decomposed, the most common subsystem[3] are:

- VOR: Consist in a ground station and a airborne equipment. The ground station transmits an RF signal with two 30 Hz modulated signals. The relative phase of the two 30 Hz signals defines radial lines in space with respect to the ground station. The VOR ground station antenna is normally aligned in such a manner that its 0 degree radial agrees with the area's magnetic north. Each VOR transmitter also transmits an identifier so it can be positively identified. The VOR airborne equipment receives, detects and presents this information in such a way that the relative bearing with respect to the ground transmitter can be determined. With this type of presentation, any bearing with respect to the ground station can be selected and flown. [4]

---

[3] the terms system and sub-systems are now on often used with the same meaning because of the easy exchange of the boundaries considered

[4] In this work is considered only the airborne component

- DME: Consist in a ground station and a airborne equipment. The ground station transmits an RF signal in the frequency band between 960 and 1215 MHz. The DME airborne component transmits a pulse pair to the ground station. Which once interrogated specifies on the same channel of the interrogation the carrier frequency and the spacing between the pulses. After a known delay the GS sends the pulse on the specified channel. The airborne equipment measures the time spacing between the pulses obtaining the slant range.[4]
- TACAN: Consist in a military system composed by a GS and an airborne equipment. In terms of functionalities it is a combination of VOR and DME, but works on UHF frequency band 962-1213 MHz, utilizing a pulse-pair transponder system. [4]
- ILS: Consist in a airborne equipment composed by one or more localizer that provides horizontal guidance, one or more glideslope that provides vertical guidance, approach light and Marker beacons.(the last two elements are not mandatory for the system)
- Pitot-static: Consist in a system capable to measure the fluid data using the dynamic and the static pressure of the air. [5]
- Flight Director: Consists in a flight instrument overlaid on the attitude indicator. It shows the pilot the required attitude to execute the desired flight path.
- Compasses: Consists in a set of electronic and magnetic compasses, the second of whom is considered a self-contained systems because it doesn't require any external input such as electricity.
- Indicators: Consists in a set of elements that must provide a human-machine interface, translating the relevant information in a human comprehensive language.
- ADF: Consists in a airborne system that uses a GS signal to identify a flight direction.
- GPS: Consists in a airborne systems that uses satellites to triangulate the exact spatial position of the plane.
- INS: Consists in a set of inertial instruments such as accelerometers and gyroscopes that constantly integrated by a computer calculate by dead reckoning the position, the orientation and the velocity of the aircraft.

Other components works to fulfill the task of the navigation system as data busses and

---

[5] The Pitot tube is only capable to measure the dynamic pressure of the air, but combined with the static port it capable to measure much more useful data

power suppliers, but are considerate components of other systems or effect-less in this model.

In figure1.5 are represented the systems just seen.

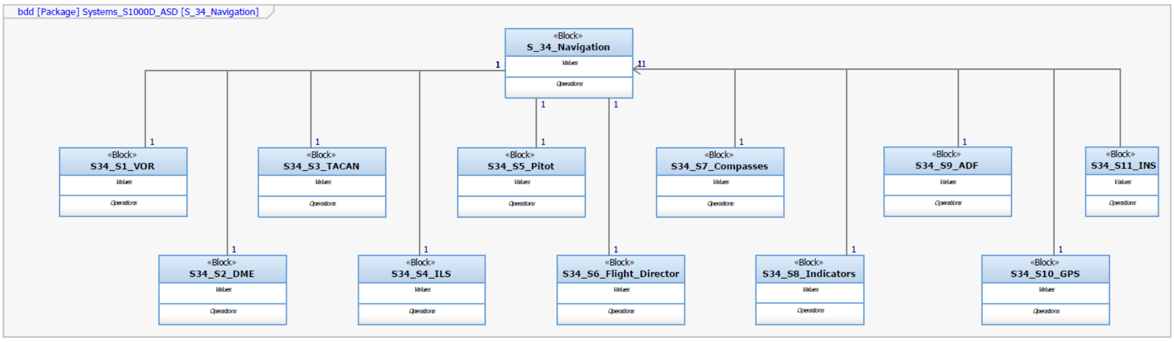


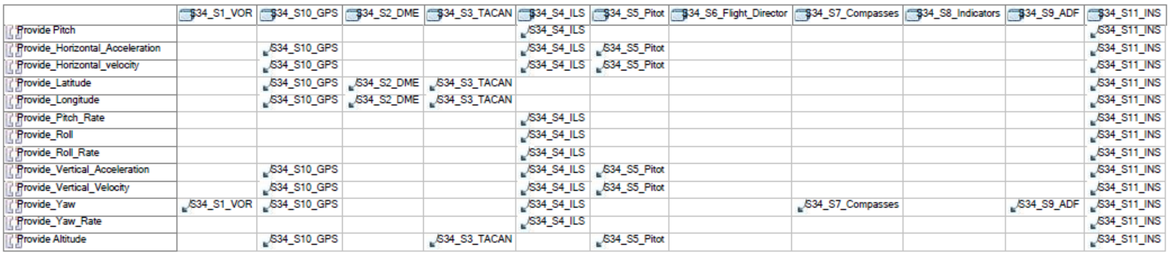
Figure 1.5: Navigation System

Once again in the previous picture is shown only a decomposition in terms of "father-child" relations. It's utility us to identify each system on which sub-level can be allocated, and thus with which other system is concurrent to fulfill a function or requirement, and on which other is related in a different way.

1.4.4 Allocation

An important phase in the developing process is the allocation of functional requirements to systems in order to define the desired behavior of system and subsystem. With the top-level requirements defined as in *1.4.1 Requirements* it is necessary to identify the specific requirements for critical items of equipment. It must pointed out that these allocation are mandatory to trace the decomposition of the high level requirements. With the partitioning increase the cross-linkage and therefor the complexity of the model. Therefore any change in the design must be checked trough the allocated requirements to understand which impact it can have.

In figure1.6 is shown the first level of navigational subsystems and their allocated functional requirements. Only the function concerning position, velocities, rate and trim are shown, thus there are subsystems with no allocated function. This does not mean that they are useless, but only that from this view point they are not involved.



	S34_S1_VOR	S34_S10_GPS	S34_S2_DME	S34_S3_TACAN	S34_S4_ILS	S34_S5_Pitot	S34_S6_Flight_Director	S34_S7_Compasses	S34_S8_Indicators	S34_S9_ADF	S34_S11_INS
Provide Pitch					S34_S4_ILS						S34_S11_INS
Provide_Horizontal_Acceleration		S34_S10_GPS			S34_S4_ILS	S34_S5_Pitot					S34_S11_INS
Provide_Horizontal_velocity		S34_S10_GPS			S34_S4_ILS	S34_S5_Pitot					S34_S11_INS
Provide_Latitude		S34_S10_GPS	S34_S2_DME	S34_S3_TACAN							S34_S11_INS
Provide_Longitude		S34_S10_GPS	S34_S2_DME	S34_S3_TACAN							S34_S11_INS
Provide_Pitch_Rate					S34_S4_ILS						S34_S11_INS
Provide_Roll					S34_S4_ILS						S34_S11_INS
Provide_Roll_Rate					S34_S4_ILS						S34_S11_INS
Provide_Vertical_Acceleration		S34_S10_GPS			S34_S4_ILS	S34_S5_Pitot					S34_S11_INS
Provide_Vertical_Velocity		S34_S10_GPS			S34_S4_ILS	S34_S5_Pitot					S34_S11_INS
Provide_Yaw	S34_S1_VOR	S34_S10_GPS			S34_S4_ILS			S34_S7_Compasses		S34_S9_ADF	S34_S11_INS
Provide_Yaw_Rate					S34_S4_ILS						S34_S11_INS
Provide Altitude		S34_S10_GPS		S34_S3_TACAN		S34_S5_Pitot					S34_S11_INS

Figure 1.6: Allocation Matrix

This allocation combined with decomposition is a top-down distribution process, iterative initially and often evolving from trade-offs. The objective is to be able to identify specific qualitative and quantitative design requirements for each element of the system. There may be times when a given requirements is too stringent, and so it will changed in a less restrictive one. but this implies a tightening of a requirement for one or more of the other units. Thus it is not always a top-down process, but can also be horizontal and it is definitively iterative. [1]

When the selected system design meet the stakeholder needs the team, trough the allcation process, baseline the products. Developing complex system, it is difficult to design a portion of the whole if the system design is constantly changing. Baselining a single design solution allows the technical team to focus on only one alternative. It is important to not baseline in the early stage of the development, in fact the early exploration of different design solution should be free and open to a wide range of options. Baselining in the early stages crystallize the project on a solution without the creative exploration of all the possibilities, thus the one selected may not be the best one. [22] Must be specified once again that the main focus of this work is not to baseline a technical solution, but to provide a functional model that works as a guideline for the developing process.

This process is also very important for the technology assessment. In fact there must be a constant interaction between the technology development and the design identification process to ensure that the best possibilities are achieved. Often the technologies are chosen immature and should be fully developed. It is not possible to develop them all, but must understand the gap between the desired technology and it's maturity to pursue only the most promising technologies. The technology assessment plays a crucial role during the preliminary design, if done incorrectly then the project is at risk. Development, but also modification, of technology plays a greater role in the life cycle of a project. Because of the high impact that technology development may have on the success or failure of a project, its assessment must play a role throughout the design process.

Chapter 2

Design optimization and system analysis

In this chapter will be discussed the strategies of system analysis and the possible design optimization processes.

Once defined the high level requirements and allocated to the high level system, the first step of the process is completed. The configuration choose is still not the final one, it can still be modified if needed, but is the basis for the next phase of development, in other words: the functional basis for the physical development.

For a good engineering process the developing proceed with a deep analysis of the system in order to understand without uncertainty the tasks and the behavior that it must have and, in order to identify the criticality and to manage them. The most common analysis are shortly explained.

- Sequence diagram: describe the sequence of events and identifies the behavior of the system to off-nominal condition.
- Failure Modes and Effect Analyses (FMEAs): describes a systematic group of activities and is intended to identify the potential failure of an item or process and the effect on the overall system and to identify the actions that can eliminate or mitigate the potential failure occurrence.[23]
- Functional Hazard Analysis (FHA): identifies the failure modes and the overall impact on the system combining with the evaluation of the severity and likelihood of the event.
- Qualitative top-down logic models: identifies the possible combination of failure and they're effect on the overall system.

- Quantitative logic models: also called Probabilistic risk assessment, complements the qualitative models introducing the likelihood of failure. This models are based on statistical techniques and failure criteria.
- Reliability block diagrams: evaluate the reliability of a system.
- Preliminary Hazard Analysis (PHA): implemented in the early stage identify the hazards responding at the question ”what if”. it evaluate potential hazards suggesting potential correction in order to eliminate the hazard or, if it can not be eliminate, to control it. [24]
- Hazard Analysis: implemented on the completed design is equivalent to the PHA.
- Human Reliability analysis: is used to identify how human interaction can lead to system failures ant evaluate the probability of this occurrence.
- Probabilistic structural analysis: used to evaluate the uncertainties in materials and load in structural elements.
- Logistics models: used to analyze the interactions of systems in time.

All these analysis are performed in a iterative process of trial and error until the desired performance is reached.

2.1 FHA

The Fault or Functional Hazard Analysis can be viewed as an expansion of the FMEA, in fact FMEA's output data can be used as input for a FHA. Although it can be performed on the final design, is more useful if it is performed in the early stages, in order to help identify any criticality in the design before time and money are spent developing it. The FHA should identify every possible failure of the system, it will be used as basis for a reliable design development. It is thus a key process for the safety and security of the aircraft. The FHA must[25]:

- consider all function.
- consider all functional failure modes.
- consider all operational phases.
- consider all operational interfaces.
- derive all operational condition and classify its severity.
- be systematic and accurate.

In order to understand the importance in a multi-platform system of this analysis it has been conducted the functional hazards of the navigation system, a mandatory system for any nowadays airplane. It has been conducted a FHA on a set of high level function:

- Provide Position information (NED coordinates).
- Provide Orientation information (Euler angles)
- Provide Velocity information (linear and angular)
- Provide Acceleration information (linear and angular rates)

All these functions have been considered failed with the awareness of the crew and without, this distinction is important because often the pilot or the control tower controller are not capable to understand if the data form the navigation system are corrupted or not.

The FHA, once identified the function of a system or a subsystem, will attempt to understand the possible failure modes of a component, and the consequences that the failure may have on the general system. To classify the hazard have been used the levels exposed in the table 2.1:

Classification	Effect
No safety effect	An event that, if it occurred, would have no effect on the mission
Minor	An event that, if it occurred,would cause minor mission degradation, minor increment in crew workload, minor reduction of safety margins, no injury, no illness, general discomfort and no system damage
Major	An event that, if it occurred,would cause major mission degradation, significant crew workload, significant reduction in safety margins, minor occupational illness, minor injury or minor system damage
Hazardous	An event that, if it occurred,would cause large reduction in safety margins, physical distress or a workload such that the operators cannot perform their tasks accurately or completely, severe injury, occupational illness or major system damage
Catastrophic	An event that, if it occurred, would cause complete mission failure, multiple death, or complete loss of the system

Table 2.1: Hazards Classification

The flight phases and flight condition are also important to correctly identify the situation, the pilot's situation awareness, the hazard classification and the consequences that these failure can have. Two flight condition have been considered:

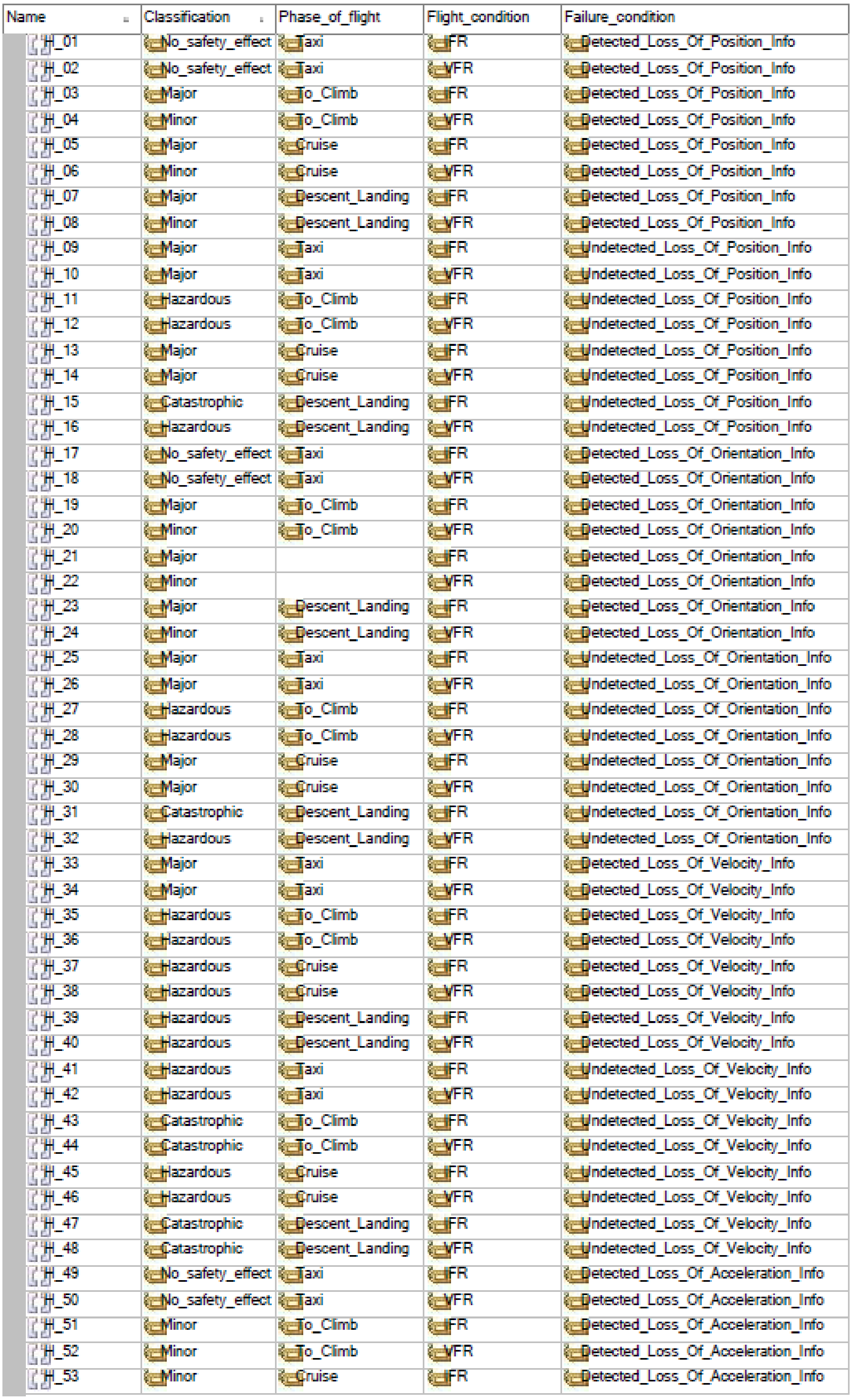
- Visual Flight Rules (VFR): the rules that govern the operation of aircraft in Visual Meteorological Conditions (VMC). In this condition the pilot have external references that can help him to interpret and evaluate the situation.
- Instrumental Flight Rules (IFR): the rules that govern the operation of aircraft in Instrumental Meteorological Conditions (IMC).In this condition the pilot have none or to few external references in order to evaluate correctly the situation.

The flight phases considered are the classic:

- Taxi: from the parking spot to the runway holding position. It involves low speed maneuver and the navigation's data required in this phase is not very relevant.
- Take-off and Climb Out: form the runway holding position to 1000 ft above runway elevation or the VFR pattern, whichever comes first. It involves high accelerations and loads. This phase is really important to the check of some navigational instrumentation. It can end in an aborted takeoff in case of a failure is detected.
- Cruise: from the previous condition to the start of descent to the destination. It involves high speed maneuver with low loads, it is the phase is which the NAVAIDs are most used.
- Descent and Landing: from the beginning of the descent trough touchdown, braking, to the exit of the runway. It involves high deceleration and high loads, the approach is a critic phase the landing the most strict in terms of precision of the data (if used).

In the following figures 2.1; 2.2; 2.3; 2.4 is reported the FHA for the case study. It has been implemented in Rhapsody considering each combination of failure, phase if flight and flight condition as a single requirement. With the definition of a stereotype named "Hazard" these requirements are distinguished from the other ones. In this stereotype were defined five different tags corresponding to each data considered:

- Classification
- Phase of flight
- Flight condition
- Failure condition
- Effect

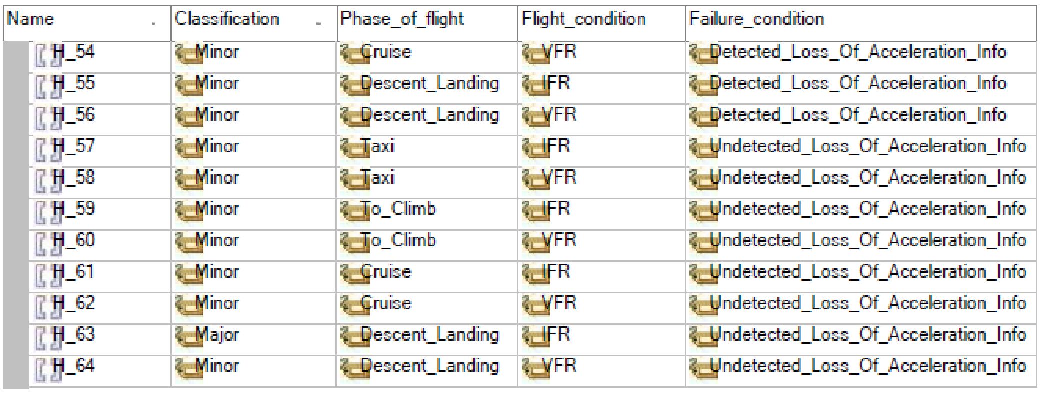


Name	Classification	Phase_of_flight	Flight_condition	Failure_condition
H_01	No_safety_effect	Taxi	IFR	Detected_Loss_Of_Position_Info
H_02	No_safety_effect	Taxi	VFR	Detected_Loss_Of_Position_Info
H_03	Major	To_Climb	IFR	Detected_Loss_Of_Position_Info
H_04	Minor	To_Climb	VFR	Detected_Loss_Of_Position_Info
H_05	Major	Cruise	IFR	Detected_Loss_Of_Position_Info
H_06	Minor	Cruise	VFR	Detected_Loss_Of_Position_Info
H_07	Major	Descent_Landing	IFR	Detected_Loss_Of_Position_Info
H_08	Minor	Descent_Landing	VFR	Detected_Loss_Of_Position_Info
H_09	Major	Taxi	IFR	Undetected_Loss_Of_Position_Info
H_10	Major	Taxi	VFR	Undetected_Loss_Of_Position_Info
H_11	Hazardous	To_Climb	IFR	Undetected_Loss_Of_Position_Info
H_12	Hazardous	To_Climb	VFR	Undetected_Loss_Of_Position_Info
H_13	Major	Cruise	IFR	Undetected_Loss_Of_Position_Info
H_14	Major	Cruise	VFR	Undetected_Loss_Of_Position_Info
H_15	Catastrophic	Descent_Landing	IFR	Undetected_Loss_Of_Position_Info
H_16	Hazardous	Descent_Landing	VFR	Undetected_Loss_Of_Position_Info
H_17	No_safety_effect	Taxi	IFR	Detected_Loss_Of_Orientation_Info
H_18	No_safety_effect	Taxi	VFR	Detected_Loss_Of_Orientation_Info
H_19	Major	To_Climb	IFR	Detected_Loss_Of_Orientation_Info
H_20	Minor	To_Climb	VFR	Detected_Loss_Of_Orientation_Info
H_21	Major		IFR	Detected_Loss_Of_Orientation_Info
H_22	Minor		VFR	Detected_Loss_Of_Orientation_Info
H_23	Major	Descent_Landing	IFR	Detected_Loss_Of_Orientation_Info
H_24	Minor	Descent_Landing	VFR	Detected_Loss_Of_Orientation_Info
H_25	Major	Taxi	IFR	Undetected_Loss_Of_Orientation_Info
H_26	Major	Taxi	VFR	Undetected_Loss_Of_Orientation_Info
H_27	Hazardous	To_Climb	IFR	Undetected_Loss_Of_Orientation_Info
H_28	Hazardous	To_Climb	VFR	Undetected_Loss_Of_Orientation_Info
H_29	Major	Cruise	IFR	Undetected_Loss_Of_Orientation_Info
H_30	Major	Cruise	VFR	Undetected_Loss_Of_Orientation_Info
H_31	Catastrophic	Descent_Landing	IFR	Undetected_Loss_Of_Orientation_Info
H_32	Hazardous	Descent_Landing	VFR	Undetected_Loss_Of_Orientation_Info
H_33	Major	Taxi	IFR	Detected_Loss_Of_Velocity_Info
H_34	Major	Taxi	VFR	Detected_Loss_Of_Velocity_Info
H_35	Hazardous	To_Climb	IFR	Detected_Loss_Of_Velocity_Info
H_36	Hazardous	To_Climb	VFR	Detected_Loss_Of_Velocity_Info
H_37	Hazardous	Cruise	IFR	Detected_Loss_Of_Velocity_Info
H_38	Hazardous	Cruise	VFR	Detected_Loss_Of_Velocity_Info
H_39	Hazardous	Descent_Landing	IFR	Detected_Loss_Of_Velocity_Info
H_40	Hazardous	Descent_Landing	VFR	Detected_Loss_Of_Velocity_Info
H_41	Hazardous	Taxi	IFR	Undetected_Loss_Of_Velocity_Info
H_42	Hazardous	Taxi	VFR	Undetected_Loss_Of_Velocity_Info
H_43	Catastrophic	To_Climb	IFR	Undetected_Loss_Of_Velocity_Info
H_44	Catastrophic	To_Climb	VFR	Undetected_Loss_Of_Velocity_Info
H_45	Hazardous	Cruise	IFR	Undetected_Loss_Of_Velocity_Info
H_46	Hazardous	Cruise	VFR	Undetected_Loss_Of_Velocity_Info
H_47	Catastrophic	Descent_Landing	IFR	Undetected_Loss_Of_Velocity_Info
H_48	Catastrophic	Descent_Landing	VFR	Undetected_Loss_Of_Velocity_Info
H_49	No_safety_effect	Taxi	IFR	Detected_Loss_Of_Acceleration_Info
H_50	No_safety_effect	Taxi	VFR	Detected_Loss_Of_Acceleration_Info
H_51	Minor	To_Climb	IFR	Detected_Loss_Of_Acceleration_Info
H_52	Minor	To_Climb	VFR	Detected_Loss_Of_Acceleration_Info
H_53	Minor	Cruise	IFR	Detected_Loss_Of_Acceleration_Info

Figure 2.1: Fault Hazard Analysis: pg.1

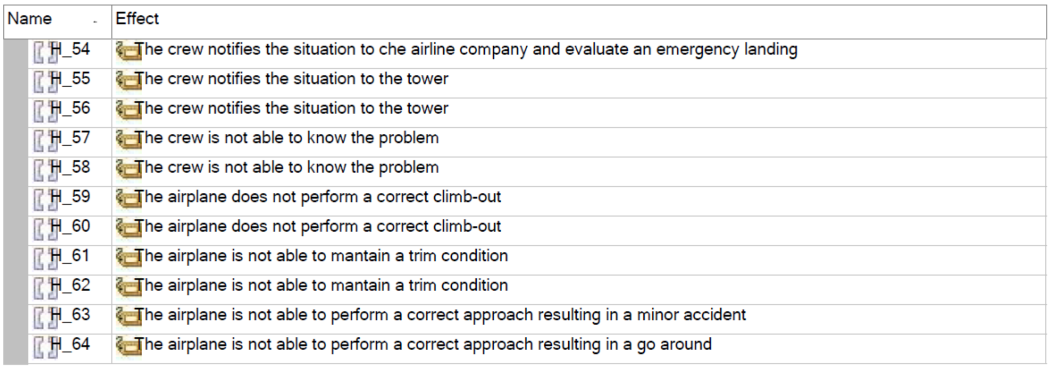
Name	Effect
H_01	Crew return the aircraft to the parking
H_02	Crew return the aircraft to the parking
H_03	Crew will return to the departure airport and notifies emergency
H_04	Crew will return to the departure airport and notifies emergency
H_05	Crew asks for ATC support, notifies emergency
H_06	Crew Asks fot ATC support, notifies emergency
H_07	Crew asks for ATC support, notifies emergency
H_08	crew asks for atc support, notifies emergency
H_09	The crew is not able to identify the position of the plane, results in a nortmal take off
H_10	The crew is not able to identify the position of the plane, results in a nortmal take off
H_11	The crew is not able to identify the position of the plane, results in a nortmal take off
H_12	The crew is not able to identify the position of the plane, results in a nortmal take off
H_13	The crew is not able to identify the position of the plane, results in a deviation of the flight path
H_14	The crew is not able to identify the position of the plane, results in a deviation of the flight path
H_15	The Crew is not able to identify the position of the plane, resulting in a wrong approach and a landing out of the runway
H_16	The Crew is not able to identify the position of the plane, resulting in a missed landing
H_17	Crew return the aircraft to the parking
H_18	Crew return the aircraft to the parking
H_19	Crew will return to the departure airport notifies emergency
H_20	Crew will return to the departure airport notifies emergency
H_21	Crew asks for ATC support, notifies Emergency
H_22	Crew asks for ATC support, notifies Emergency
H_23	Crew asks for ATC support, notifies Emergency
H_24	Crew asks for ATC support, notifies Emergency
H_25	The Crew is not able to identify the orientation of the plane, resulst in a normal take-off
H_26	The Crew is not able to identify the orientation of the plane, resulst in a normal take-off
H_27	The Crew is not able to identify the orientation of the plane, resulst in a normal take-off
H_28	The Crew is not able to identify the orientation of the plane, resulst in a normal take-off
H_29	The Crew is not able to identify the orientation of the plane, resulst in a deviation of the flight path
H_30	The Crew is not able to identify the orientation of the plane, resulst in a deviation of the flight path
H_31	The Crew is not able to identify the orientation of the plane, resulting in a wrong approach and a landing out of the runway
H_32	The Crew is not able to identify the orientation of the plane, resulting in a missed landing
H_33	The crew is not able to stop the aircraft properly, resulting in resulting in low speed contact with terminal, aircraft, or
H_34	The crew is not able to stop the aircraft properly, resulting in resulting in low speed contact with terminal, aircraft, or
H_35	Crew call emergency and return to the departure airport
H_36	Crew call emergency and return to the departure airport
H_37	Crew call emergency and perform an emergency landing
H_38	Crew call emergency and perform an emergency landing
H_39	Crew call emergency, selects a more suitable runway, and prepare occupants for runway overrun
H_40	Crew call emergency, selects a more suitable runway, and prepare occupants for runway overrun
H_41	The crew is not able to stop the aircraft properly, results in a runway incursion
H_42	The crew is not able to stop the aircraft properly, results in a runway incursion
H_43	Aircraft stalls at too low altitude for recover resulting in a fatal accident
H_44	Aircraft stalls at too low altitude for recover resulting in a fatal accident
H_45	Aircraft stalls and crew call emergency resulting in a emergency landing
H_46	Aircraft stalls and crew call emergency resulting in a emergency landing
H_47	Aircraft stalls at too low altitude for recover resulting in a major accident
H_48	Aircraft stalls at too low altitude for recover resulting in a major accident
H_49	The airplane returns to the gate for investigation.
H_50	
H_51	The airplane returns to the departure airport for investigation.
H_52	The airplane returns to the departure airport for investigation.
H_53	The crew notifies the situation to che airline company and evaluate an emergency landing

Figure 2.2: Fault Hazard Analysis: pg.2



Name	Classification	Phase_of_flight	Flight_condition	Failure_condition
H_54	Minor	Cruise	VFR	Detected_Loss_Of_Acceleration_Info
H_55	Minor	Descent_Landing	IFR	Detected_Loss_Of_Acceleration_Info
H_56	Minor	Descent_Landing	VFR	Detected_Loss_Of_Acceleration_Info
H_57	Minor	Taxi	IFR	Undetected_Loss_Of_Acceleration_Info
H_58	Minor	Taxi	VFR	Undetected_Loss_Of_Acceleration_Info
H_59	Minor	To_Climb	IFR	Undetected_Loss_Of_Acceleration_Info
H_60	Minor	To_Climb	VFR	Undetected_Loss_Of_Acceleration_Info
H_61	Minor	Cruise	IFR	Undetected_Loss_Of_Acceleration_Info
H_62	Minor	Cruise	VFR	Undetected_Loss_Of_Acceleration_Info
H_63	Major	Descent_Landing	IFR	Undetected_Loss_Of_Acceleration_Info
H_64	Minor	Descent_Landing	VFR	Undetected_Loss_Of_Acceleration_Info

Figure 2.3: Fault Hazard Analysis: pg.3



Name	Effect
H_54	The crew notifies the situation to che airline company and evaluate an emergency landing
H_55	The crew notifies the situation to the tower
H_56	The crew notifies the situation to the tower
H_57	The crew is not able to know the problem
H_58	The crew is not able to know the problem
H_59	The airplane does not perform a correct climb-out
H_60	The airplane does not perform a correct climb-out
H_61	The airplane is not able to mantain a trim condition
H_62	The airplane is not able to mantain a trim condition
H_63	The airplane is not able to perform a correct approach resulting in a minor accident
H_64	The airplane is not able to perform a correct approach resulting in a go around

Figure 2.4: Fault Hazard Analysis: pg.4

As can be seen in the FHA is important to notice that the same failure can have different hazard classification and effect for different phase of flight and flight condition. All the possibilities must be considered during the analysis to understand properly all the eventualities. Generally can be viewed that an undetected failure, all other conditions equal, has a worst classification than a detected failure. Thanks to this kind of analysis it is possible to define the reliability of a specific function, a key point in the physical development of the system.

2.2 System Structure

To investigate the system structure and analyse the connections between the subsystems has been used the Integrated DEFinition Method 0 (IDEF0) as representation method in the Internal Block Diagrams (IBD). The IDEF0 is a method used to model the actions and activities of a system. It helps to promote a good communication between the analyst and the customer, because of it's easy readability, and enhances domain expert involvement and consensus decision-making through simplified graphical devices. A Simple representation of the IDEF0 is shown in figure 2.5

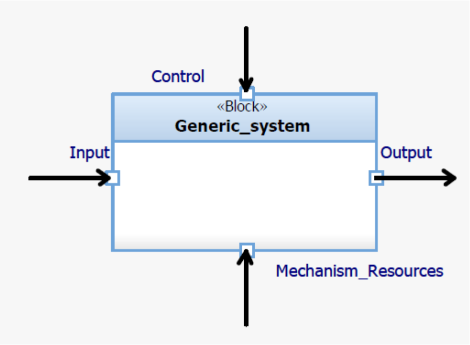


Figure 2.5: IDEF0 representation

In figure 2.6 is shown the system behavior in terms of connections between the different elements and typologies of information exchanged through them self and with other systems. The gray boundary represent the navigation system in his wholeness, instead, the smaller white box represents the most common subsystems, once again this boundaries are not fixed and does not imply that all the components of these subsystem are not used in other systems. And also the subsystem design represented is not a physical design, it is just a preliminary hypothesis of a possible configuration. This design does not consider any reliability aspect, it serves just to understand how will each subsystem works in a system view. All the links represented in the figure does not constitute a physical configuration but only a functional view of the interfaces. The components are, instead, connected to data-busses with protocols like ARINC 429[26] that defines Physical packaging and mounting of avionics equipment, data communications standards and high level computer languages. In other words the ARINC standards define how the system will communicate through itself and with other systems.

All the linkage between parts are exposed in the figures 2.7, 2.8, 2.9, 2.10. Which shows for every connections, the two elements connected, the ports trough which the connection is guaranteed and the type of message that flows through that connection. The message type, expressed as ”Port interface” are managed in a general view, and grouped for similarity, that does not mean that all the subsystems that have the same port interface receive or send the same data. I.E. the DME and the Pitot have both the port ”D” with the port interface ”Distance” but the DME measures a distance from a ground station equipment and the Pitot system, through the air pressure, measures the distance from a selected reference altitude as QFE[1], QNH[2], ecc .

---

[1] Pressure measured at Field

[2] Pressure measured in hPa at sea level

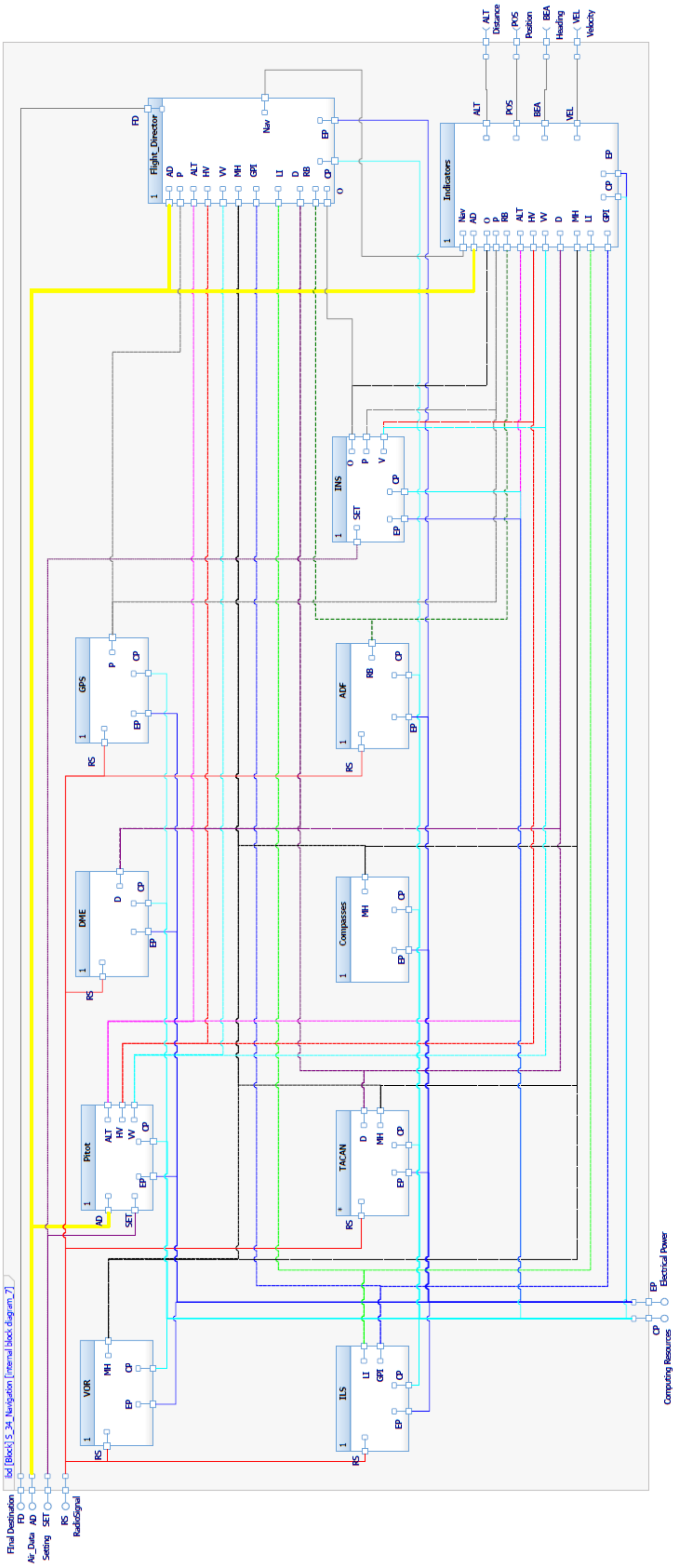
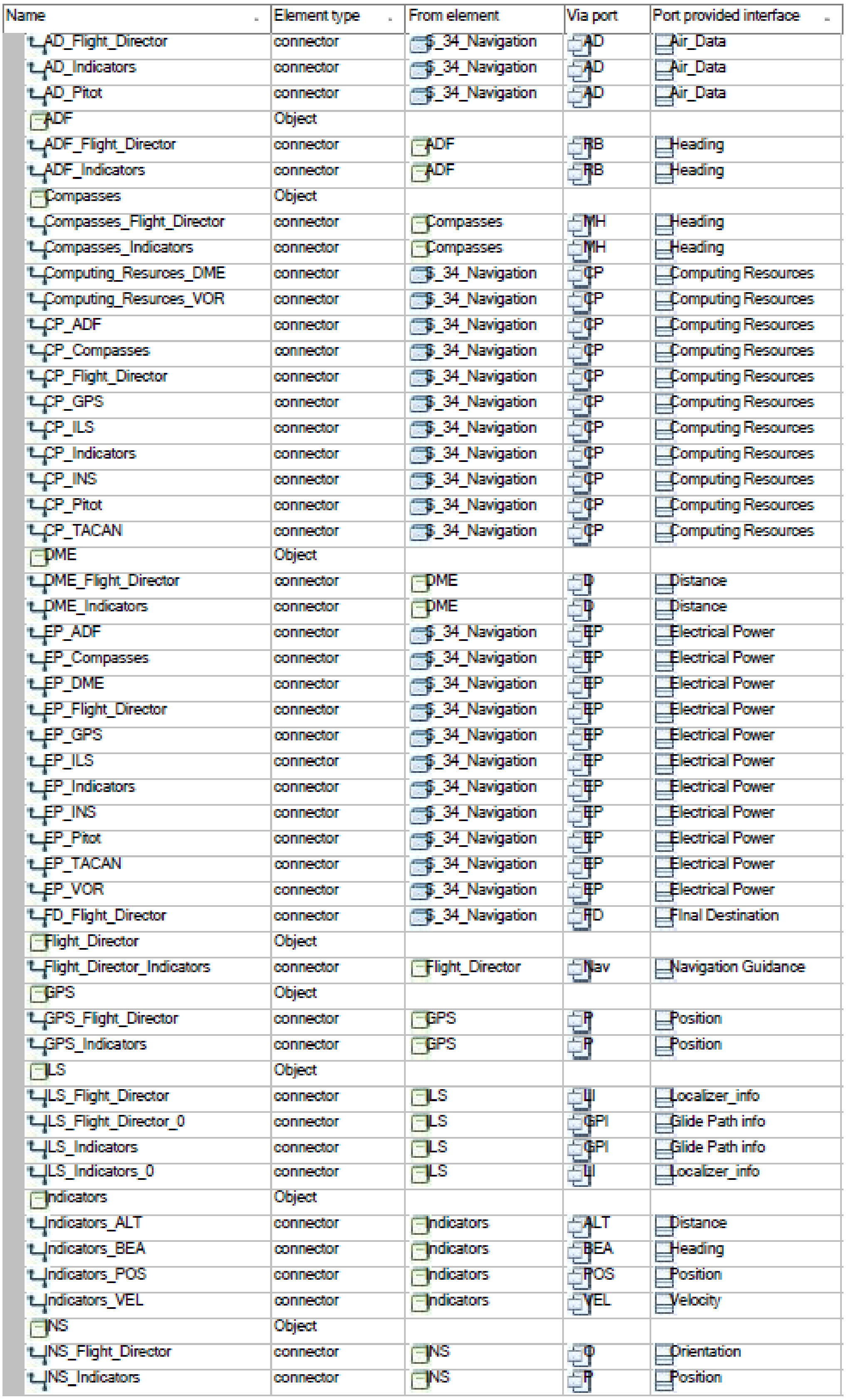
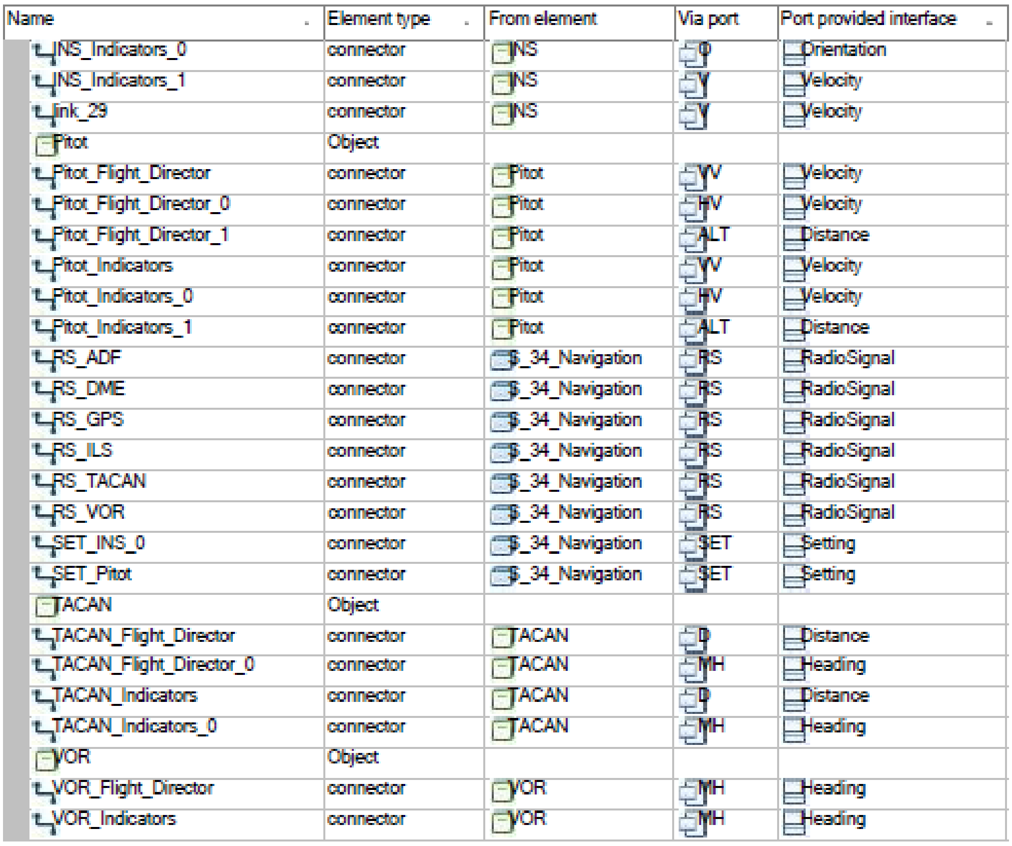


Figure 2.6: Internal Block Diagram Navigation System



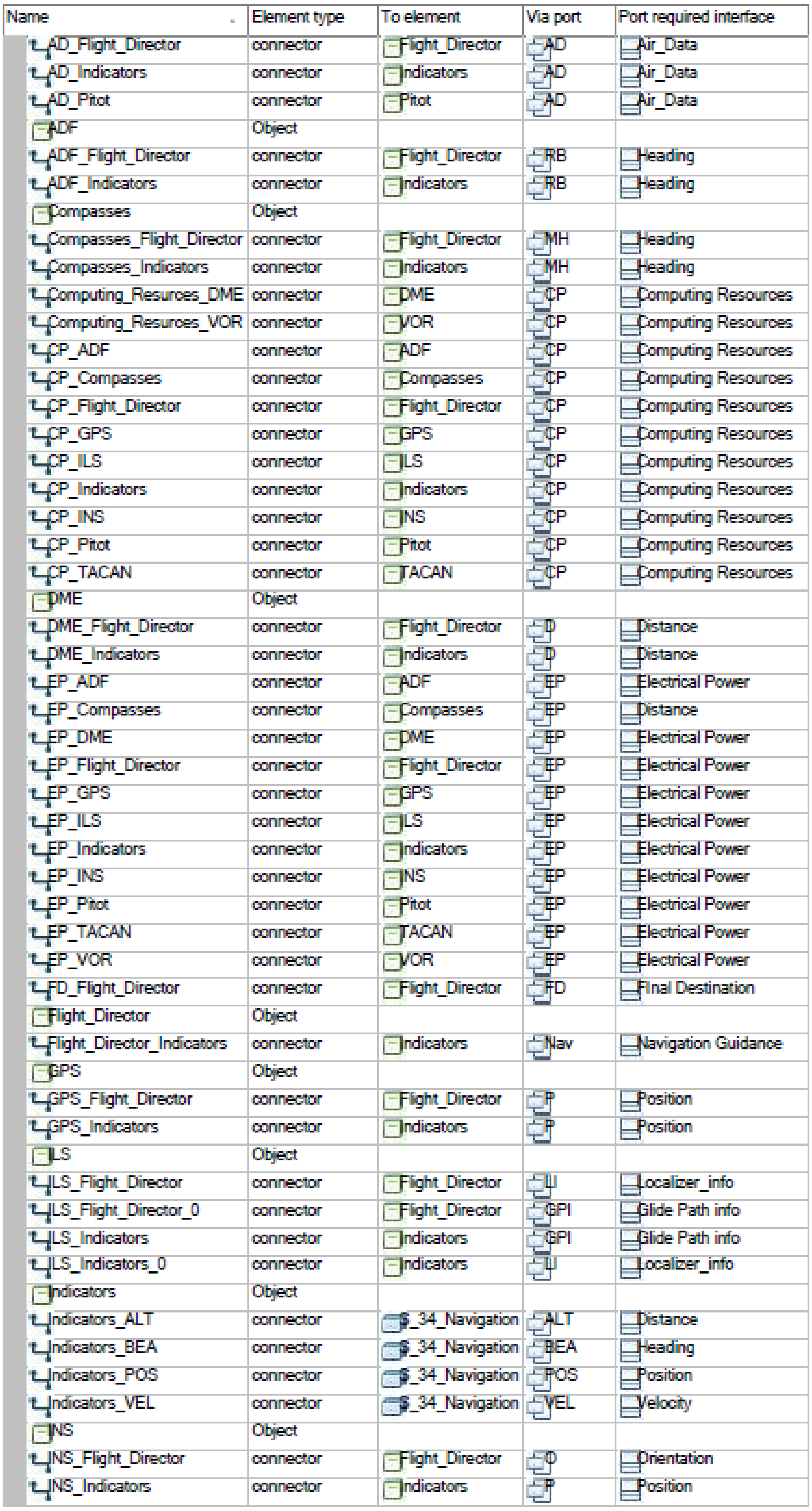
Name	Element type	From element	Via port	Port provided interface
AD_Flight_Director	connector	S_34_Navigation	AD	Air_Data
AD_Indicators	connector	S_34_Navigation	AD	Air_Data
AD_Pitot	connector	S_34_Navigation	AD	Air_Data
ADF	Object			
ADF_Flight_Director	connector	ADF	RB	Heading
ADF_Indicators	connector	ADF	RB	Heading
Compasses	Object			
Compasses_Flight_Director	connector	Compasses	MH	Heading
Compasses_Indicators	connector	Compasses	MH	Heading
Computing_Resurces_DME	connector	S_34_Navigation	CP	Computing Resources
Computing_Resurces_VOR	connector	S_34_Navigation	CP	Computing Resources
CP_ADF	connector	S_34_Navigation	CP	Computing Resources
CP_Compasses	connector	S_34_Navigation	CP	Computing Resources
CP_Flight_Director	connector	S_34_Navigation	CP	Computing Resources
CP_GPS	connector	S_34_Navigation	CP	Computing Resources
CP_ILS	connector	S_34_Navigation	CP	Computing Resources
CP_Indicators	connector	S_34_Navigation	CP	Computing Resources
CP_INS	connector	S_34_Navigation	CP	Computing Resources
CP_Pitot	connector	S_34_Navigation	CP	Computing Resources
CP_TACAN	connector	S_34_Navigation	CP	Computing Resources
DME	Object			
DME_Flight_Director	connector	DME	D	Distance
DME_Indicators	connector	DME	D	Distance
EP_ADF	connector	S_34_Navigation	EP	Electrical Power
EP_Compasses	connector	S_34_Navigation	EP	Electrical Power
EP_DME	connector	S_34_Navigation	EP	Electrical Power
EP_Flight_Director	connector	S_34_Navigation	EP	Electrical Power
EP_GPS	connector	S_34_Navigation	EP	Electrical Power
EP_ILS	connector	S_34_Navigation	EP	Electrical Power
EP_Indicators	connector	S_34_Navigation	EP	Electrical Power
EP_INS	connector	S_34_Navigation	EP	Electrical Power
EP_Pitot	connector	S_34_Navigation	EP	Electrical Power
EP_TACAN	connector	S_34_Navigation	EP	Electrical Power
EP_VOR	connector	S_34_Navigation	EP	Electrical Power
FD_Flight_Director	connector	S_34_Navigation	FD	Final Destination
Flight_Director	Object			
Flight_Director_Indicators	connector	Flight_Director	Nav	Navigation Guidance
GPS	Object			
GPS_Flight_Director	connector	GPS	P	Position
GPS_Indicators	connector	GPS	P	Position
ILS	Object			
ILS_Flight_Director	connector	ILS	LI	Localizer_info
ILS_Flight_Director_0	connector	ILS	GPI	Glide Path info
ILS_Indicators	connector	ILS	GPI	Glide Path info
ILS_Indicators_0	connector	ILS	LI	Localizer_info
Indicators	Object			
Indicators_ALT	connector	Indicators	ALT	Distance
Indicators_BEA	connector	Indicators	BEA	Heading
Indicators_POS	connector	Indicators	POS	Position
Indicators_VEL	connector	Indicators	VEL	Velocity
INS	Object			
INS_Flight_Director	connector	INS	O	Orientation
INS_Indicators	connector	INS	P	Position

Figure 2.7: Connections navigational system: pg.1



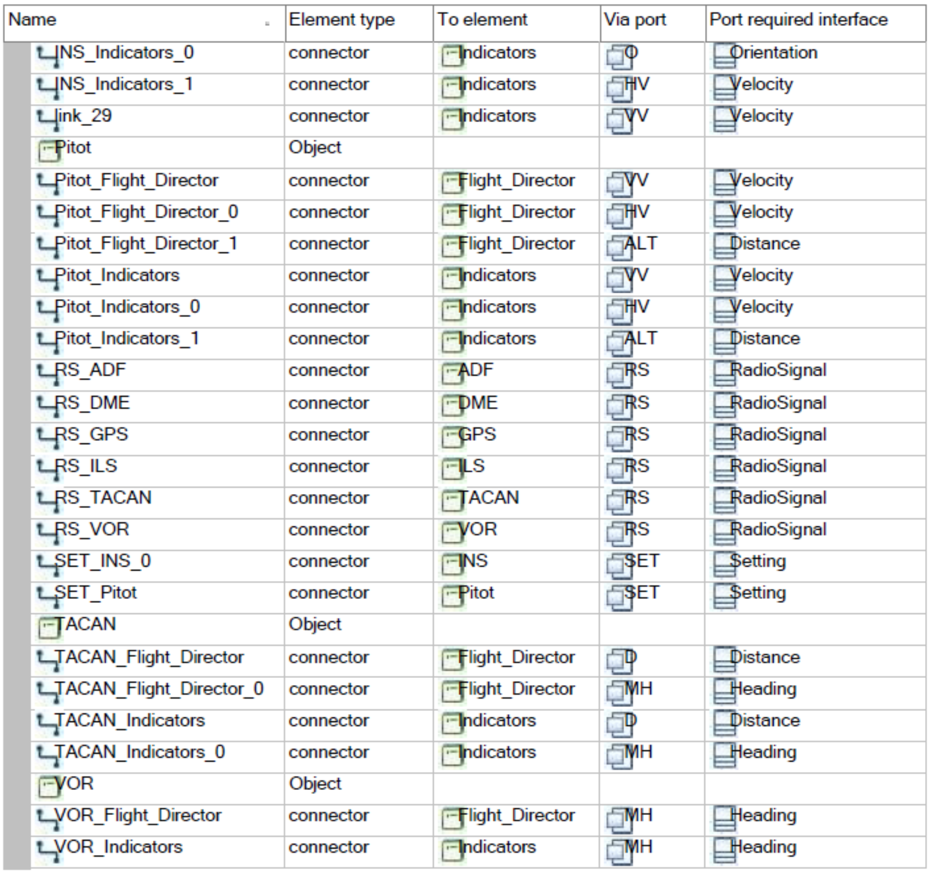
Name	Element type	From element	Via port	Port provided interface
INS_Indicators_0	connector	INS	O	Orientation
INS_Indicators_1	connector	INS	V	Velocity
link_29	connector	INS	V	Velocity
Pitot	Object			
Pitot_Flight_Director	connector	Pitot	VV	Velocity
Pitot_Flight_Director_0	connector	Pitot	HV	Velocity
Pitot_Flight_Director_1	connector	Pitot	ALT	Distance
Pitot_Indicators	connector	Pitot	VV	Velocity
Pitot_Indicators_0	connector	Pitot	HV	Velocity
Pitot_Indicators_1	connector	Pitot	ALT	Distance
RS_ADF	connector	S_34_Navigation	RS	RadioSignal
RS_DME	connector	S_34_Navigation	RS	RadioSignal
RS_GPS	connector	S_34_Navigation	RS	RadioSignal
RS_ILS	connector	S_34_Navigation	RS	RadioSignal
RS_TACAN	connector	S_34_Navigation	RS	RadioSignal
RS_VOR	connector	S_34_Navigation	RS	RadioSignal
SET_INS_0	connector	S_34_Navigation	SET	Setting
SET_Pitot	connector	S_34_Navigation	SET	Setting
TACAN	Object			
TACAN_Flight_Director	connector	TACAN	D	Distance
TACAN_Flight_Director_0	connector	TACAN	MH	Heading
TACAN_Indicators	connector	TACAN	D	Distance
TACAN_Indicators_0	connector	TACAN	MH	Heading
VOR	Object			
VOR_Flight_Director	connector	VOR	MH	Heading
VOR_Indicators	connector	VOR	MH	Heading

Figure 2.8: Connections navigational system: pg.2



Name	Element type	To element	Via port	Port required interface
AD_Flight_Director	connector	Flight_Director	AD	Air_Data
AD_Indicators	connector	Indicators	AD	Air_Data
AD_Pitot	connector	Pitot	AD	Air_Data
ADF	Object			
ADF_Flight_Director	connector	Flight_Director	RB	Heading
ADF_Indicators	connector	Indicators	RB	Heading
Compasses	Object			
Compasses_Flight_Director	connector	Flight_Director	MH	Heading
Compasses_Indicators	connector	Indicators	MH	Heading
Computing_Resurces_DME	connector	DME	CP	Computing Resources
Computing_Resurces_VOR	connector	VOR	CP	Computing Resources
CP_ADF	connector	ADF	CP	Computing Resources
CP_Compasses	connector	Compasses	CP	Computing Resources
CP_Flight_Director	connector	Flight_Director	CP	Computing Resources
CP_GPS	connector	GPS	CP	Computing Resources
CP_ILS	connector	ILS	CP	Computing Resources
CP_Indicators	connector	Indicators	CP	Computing Resources
CP_INS	connector	INS	CP	Computing Resources
CP_Pitot	connector	Pitot	CP	Computing Resources
CP_TACAN	connector	TACAN	CP	Computing Resources
DME	Object			
DME_Flight_Director	connector	Flight_Director	D	Distance
DME_Indicators	connector	Indicators	D	Distance
EP_ADF	connector	ADF	EP	Electrical Power
EP_Compasses	connector	Compasses	EP	Distance
EP_DME	connector	DME	EP	Electrical Power
EP_Flight_Director	connector	Flight_Director	EP	Electrical Power
EP_GPS	connector	GPS	EP	Electrical Power
EP_ILS	connector	ILS	EP	Electrical Power
EP_Indicators	connector	Indicators	EP	Electrical Power
EP_INS	connector	INS	EP	Electrical Power
EP_Pitot	connector	Pitot	EP	Electrical Power
EP_TACAN	connector	TACAN	EP	Electrical Power
EP_VOR	connector	VOR	EP	Electrical Power
FD_Flight_Director	connector	Flight_Director	FD	Final Destination
Flight_Director	Object			
Flight_Director_Indicators	connector	Indicators	Nav	Navigation Guidance
GPS	Object			
GPS_Flight_Director	connector	Flight_Director	P	Position
GPS_Indicators	connector	Indicators	P	Position
ILS	Object			
ILS_Flight_Director	connector	Flight_Director	LI	Localizer_info
ILS_Flight_Director_0	connector	Flight_Director	GPI	Glide Path info
ILS_Indicators	connector	Indicators	GPI	Glide Path info
ILS_Indicators_0	connector	Indicators	LI	Localizer_info
Indicators	Object			
Indicators_ALT	connector	S_34_Navigation	ALT	Distance
Indicators_BEA	connector	S_34_Navigation	BEA	Heading
Indicators_POS	connector	S_34_Navigation	POS	Position
Indicators_VEL	connector	S_34_Navigation	VEL	Velocity
INS	Object			
INS_Flight_Director	connector	Flight_Director	O	Orientation
INS_Indicators	connector	Indicators	P	Position

Figure 2.9: Connections navigational system: pg.3



Name	Element type	To element	Via port	Port required interface
INS_Indicators_0	connector	Indicators	D	Orientation
INS_Indicators_1	connector	Indicators	HV	Velocity
link_29	connector	Indicators	VV	Velocity
Pitot	Object			
Pitot_Flight_Director	connector	Flight_Director	VV	Velocity
Pitot_Flight_Director_0	connector	Flight_Director	HV	Velocity
Pitot_Flight_Director_1	connector	Flight_Director	ALT	Distance
Pitot_Indicators	connector	Indicators	VV	Velocity
Pitot_Indicators_0	connector	Indicators	HV	Velocity
Pitot_Indicators_1	connector	Indicators	ALT	Distance
RS_ADF	connector	ADF	RS	RadioSignal
RS_DME	connector	DME	RS	RadioSignal
RS_GPS	connector	GPS	RS	RadioSignal
RS_ILS	connector	ILS	RS	RadioSignal
RS_TACAN	connector	TACAN	RS	RadioSignal
RS_VOR	connector	VOR	RS	RadioSignal
SET_INS_0	connector	INS	SET	Setting
SET_Pitot	connector	Pitot	SET	Setting
TACAN	Object			
TACAN_Flight_Director	connector	Flight_Director	D	Distance
TACAN_Flight_Director_0	connector	Flight_Director	MH	Heading
TACAN_Indicators	connector	Indicators	D	Distance
TACAN_Indicators_0	connector	Indicators	MH	Heading
VOR	Object			
VOR_Flight_Director	connector	Flight_Director	MH	Heading
VOR_Indicators	connector	Indicators	MH	Heading

Figure 2.10: Connections navigational system: pg.4

In this phase is clearly expressed the behavior of each subsystem, it enable the developer to make a first evaluation, with the FHA, of the reliability need of the system in terms of corrective measure and number of redundancy, if needed, for each component. The easy readability and the interconnection trough the diagrams are a success key in the MBSE approach, that make really effective the behavioral analysis. The creation of the connection matrix is automatic, with no request from the developer. Thus the human error in this process is greatly reduced compared to the one of the document based system engineering. The figures just seen express all functional aspects of sub-systems and interface, they are all treated as black box in order to just understand what kind of information are exchanged, but leaving all the allocations to physical components and design choices to a different phase of the work, not seen in this paper.

Once the behavior of each subsystem is analysed, the developing process will proceed with the configuration definition through an iterative process of design and analysis to define the best design possible. The principal aspects of the analysis are:

- The understanding of the behavior of the system in any possible rainy day[3].
- The decomposition of the risk of the system, through fault tree analysis, from the general system to the single component of the system. This process is deeply correlated to the FHA and is performed to guarantee that the Catastrophic and Hazardous events defined in the FHA will have a acceptable probability of occurrence.
- Effectiveness analysis and requirements verification of the design developed and possible improvement identification.

Through all these phases the developer must evaluate if there is a technological solution, already developed, that is compliant to the requirements and if this solution is the best one implementable in terms of effectiveness and cost. This process can be viewed in two different phases, the first purely behavioral that involves only the deep understanding of the system tasks and behavior, and the second phase that involves the effective design development and validation, still in non physical terms, the choice of the components is the last phase at all.

2.3 System Activity

The activities of a system are not always correlated to the design, in fact the physical configuration must with some behavioral configuration guarantee the compliance to the AW and client's requirements, but it is a not binding in the choose of the activity design, that often is more than one (i.e the TACAN, a single system, have up to four working modes: Mode A, Mode C, Mode S and Ident) and, for many systems, more advanced compared to what the normative prescribes. I.e the efficiency of the plane: is a company goal to reduce the operational costs and make the aircraft more desirable for the client. Thus, defined the structure and the functions of the system and subsystem and performed the first analysis, the activities must be defined and deeply studied to choose the best strategy or to identify the design issues and be capable to fix it. To perform this design phase are useful the Activity Diagrams of the SysMl, in which through action message it is possible to define a behavioral flow and to easily represent complex activities. The Activity Diagrams works with the use of token that from a start point to a end point through all the actions and the logical component such as:

- Fork Node: split the token in many as many are the flows outgoing from it.
- Join Node: combines all the tokens from the incoming flows in a single one, once

---

[3] refers to a future time of need or trouble, suggesting that one should save resources for such a day[27]

they are all arrived in the joint node.

- Decision Node: choose a path in which the token will flow through a decision.
- Merge Node: combines two or more flows, the first token that arrives form any of the incoming flows pass through the merge node.

As shown in the FHA section 2.1 the knowledge of the system status is the first improvement that can be made to increase the safety, and thus, one of the main requirement will be to check always the corruption of the data obtained from the subsystem, in order to avoid incident like the Lion Air 610 (Boeing 737 max 8).Although the action strategy may be used to support the process of certification of a physical design, this improvement is independent from it and is purely an actions management strategy. In fact for the certification process the pilot can be inserted in a system as part of it to guarantee the safety of that systems that are not compliant or whose compliance is to difficult to prove. Although the system activity is deeply correlated to the physical design of the system, it can also be performed as a "configuration analysis" in order to define the final one.

In figure 2.11 is represented the first set of actions that may be performed for the navigation system. All these actions are traceable to the requirements exposed in figure 1.3 showing how the requirements, in this case, are translated in actions. This operations guarantee, due the correct data analysis, the knowledge of the status of the information, allowing the developer to be capable to demonstrate it in a easy way, supporting so the certification procedure. This is a key process in the information transmission process.

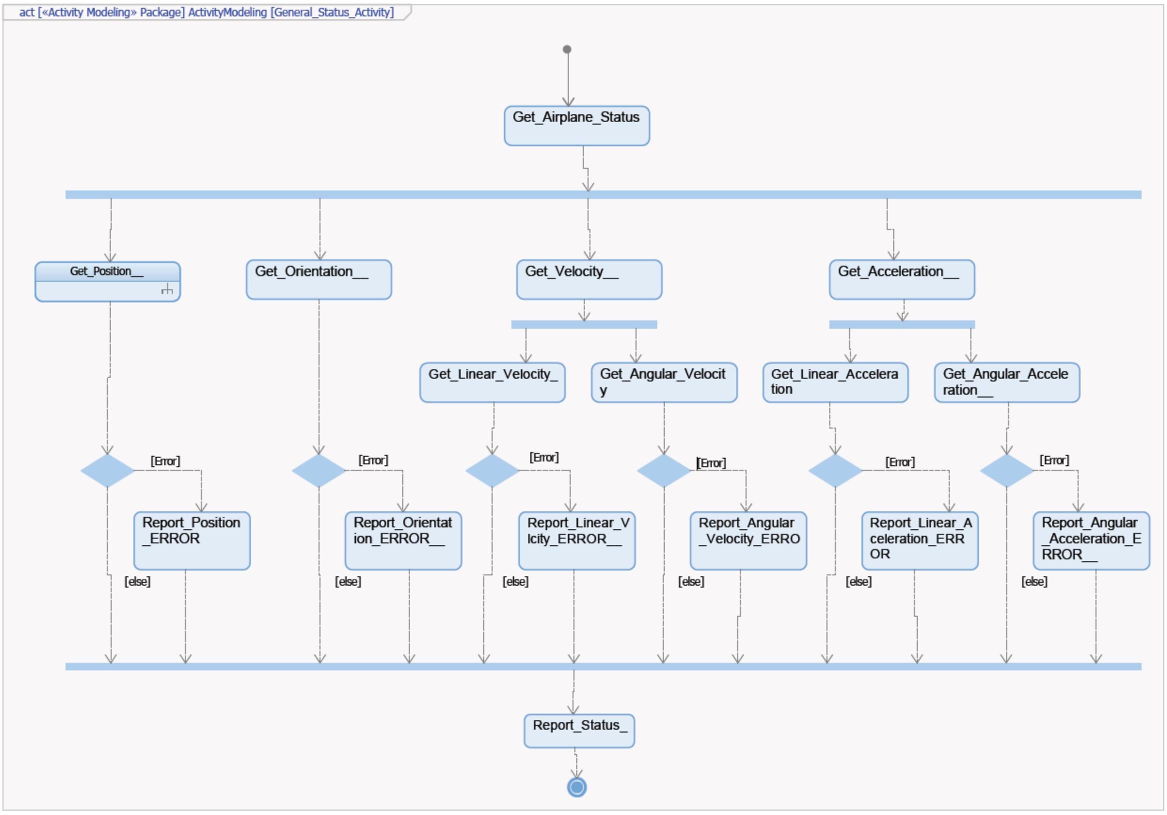


Figure 2.11: Status acquisition activity

The SysML allows, like the matryoshka doll, to enclose different diagrams one in one other from different levels of decomposition and detail. By clicking, in IBM Rhapsody, on the "Get_Position__" action the diagram 2.12 will open, showing a higher level of detail of the system's behavior. This kind of feature of the SysML is fundamental to guarantee that the model can be used as basis for future development.

In this figure are shown all the action that can be performed in different workflows to get the position information (NED). All the actions are allocated to a specific subsystem through the swim lanes[4] in which are set. The figure shows the data acquisition process highlighting the different approaches that will be applied in different situations, such as the disregard of the Instrumental Landing System in all the flight phases except for the landing.

These actions can define further requirements or strategies, I.E. the ILS inactivity during the great part of the flight can lead to different possibilities:

- the common use of components for the ILS and systems with low level of utility in the landing phase.

---

[4] Graphical instrument used in the Activity diagram to relate a function (action) to a structure

- the switching off of the ILS during all the other flight phases.

- other.

From this level of decomposition are available many deeper level, fist of all the interrogation process of any subsystem must be defined. In fact the components working specifics may are various, such as in broadcast mode[5], or in interrogation and response mode[6], or with other modes. This difference between the communication protocols influence deeply the logical configuration and the physical one, in fact the sizing of the data-busses depends also from the data amount that must pass through them.

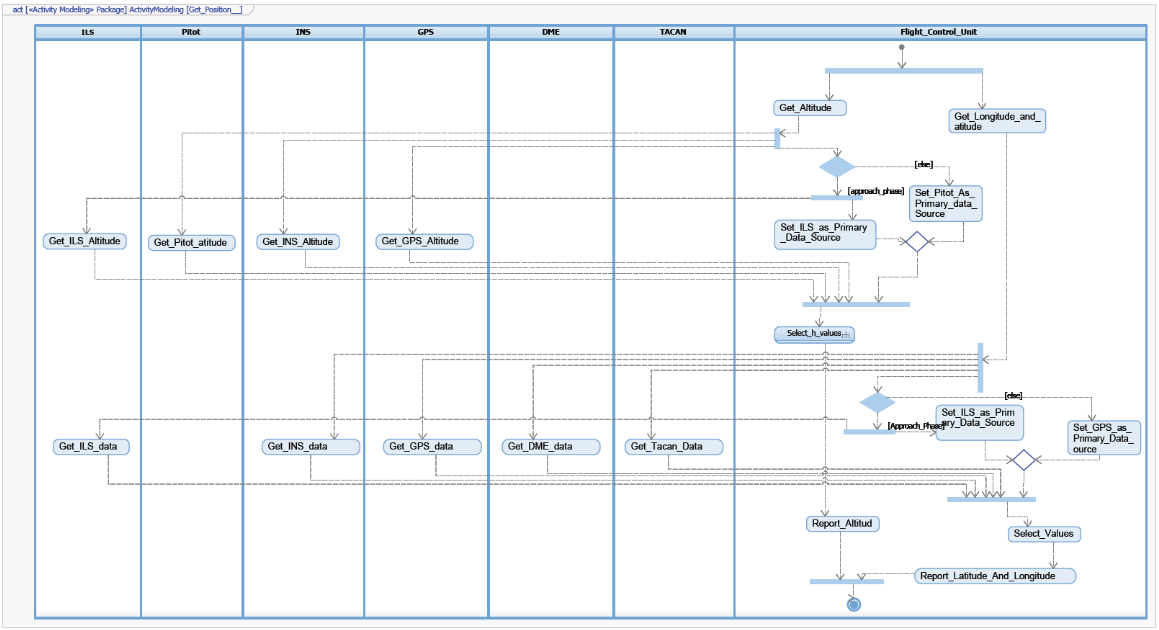


Figure 2.12: Get Position

Another level is reached through the action "Select_h_values", opening the figure 2.13, that shows a possible strategy to identify and select automatically the best altitude value during each flight phase considering any possible system failure.

---

[5] The subsystem it is always in sending mode, also if none is receiving

[6] The subsystem sends his message only in some other component expressly requires it

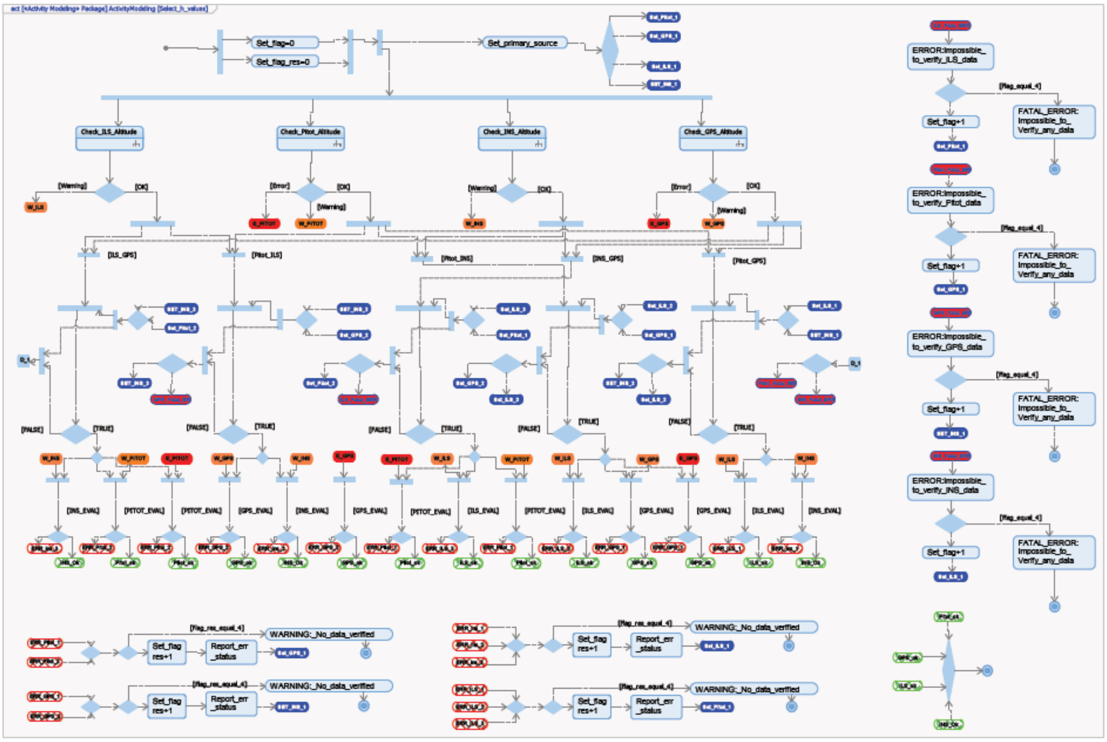


Figure 2.13: Select h value

In order to avoid flight accident due to false reading of the position information and in general, flight condition information, as the flight Alitalia 404, or the most recent Lion Air 610, has been hypothesized a more complex data management that include different levels of cross-check with different systems data and internal data evaluation of every system. It is also represented a hierarchy of the subsystem, as in table2.2, in terms of reliability and precision of the data in the different situation. The knowledge of the subsystem that are implemented is mandatory to correctly implement its functions and to manage its weakness. In fact the use of new technologies on airplane is always a process that requires long times due to test and certification process.

Flight Phase	Approach	Other
Pitot System	$2nd$	$1st$
GPS	$3rd$	$2nd$
ILS	$1st$	$4th$
INS	$4th$	$3rd$

Table 2.2: Priority classification

In figure 2.14, 2.15 and 2.16 are represented the tree section of the figure 2.13.

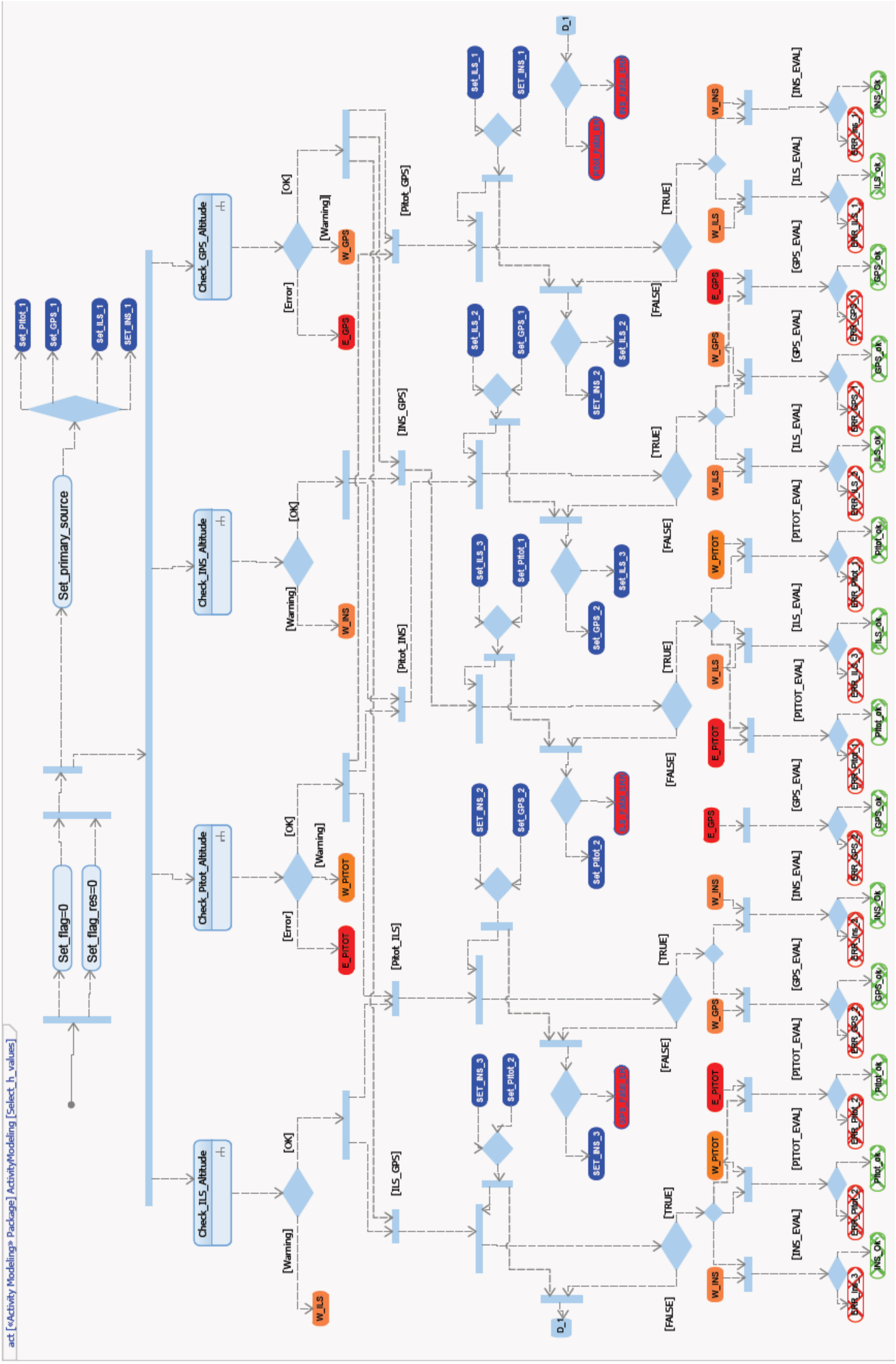


Figure 2.14: Main section select h value

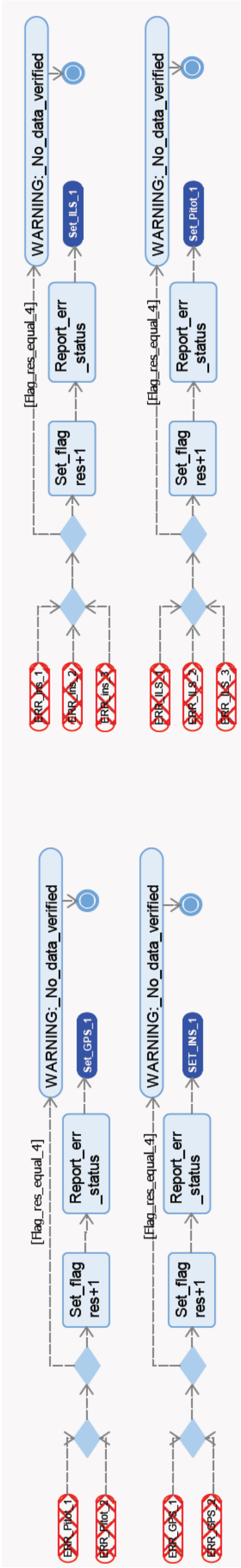


Figure 2.15: Error results select h value

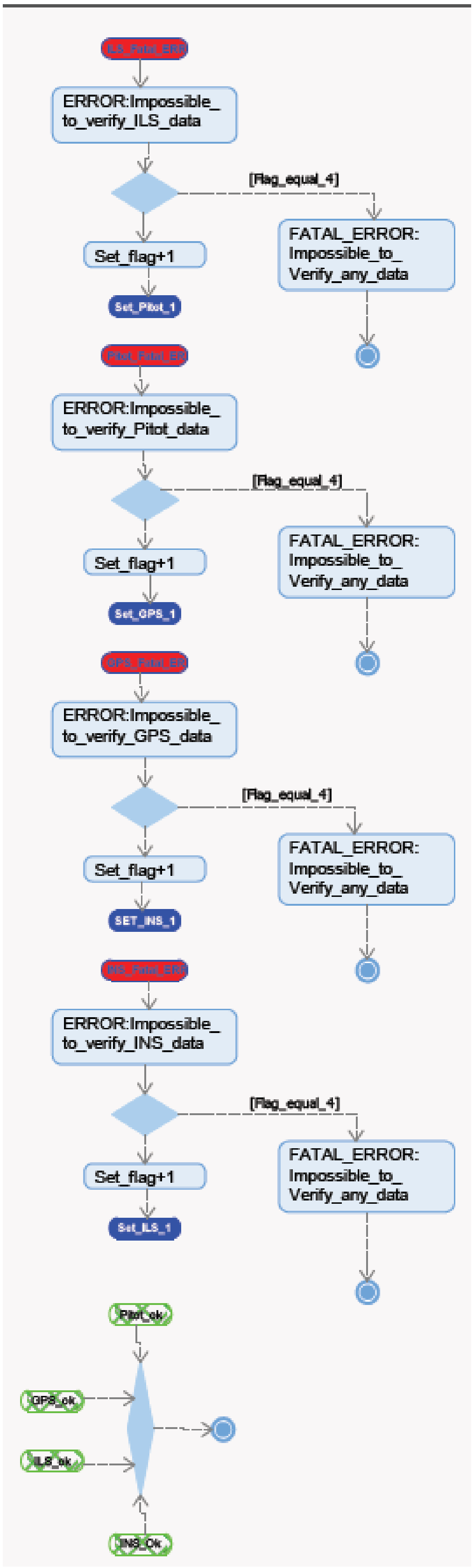


Figure 2.16: Error Process select h value

The first phase is to apply the hierarchical classification in the choose of the primary source of information. Once done the system will check automatically all the different data out-coming from the different systems separately. The Pitot system and the GPS are considered with tree redundancies, thus it is possible to identify tree different working scenarios:

- All the tree redundancies provide the same data, the system works correctly.
- One of the tree provide a different data, this one is excluded from the general system and the malfunction is reported to the pilot in form of warning.
- All the tree redundancies provide different data, the system is not able to identify if and which one is correct, the malfunction is reported in form of error.

For the other systems are hypothesized only two redundancies, because of the lower level of importance for the overall system. In this case the subsystem check can only compare two values, thus or they are equal, or the system can not define if or which one is correct.

The following step is to check if the data of two different sources are comparable, this two sources are set from the choose of the primary source and so on from eventual errors find in the systems. All these checks allows the computer to identify with a high level of certainly if a system is giving some wrong data.

By clicking on the "Check_Pitot_Data" Action in the precious diagram, IBM Rhapsody will open a new level of detail in a new diagram. In figure 2.17 is represented the work flow of the internal check of the pitot system through the comparison of the different values, and the different scenarios that may occur.

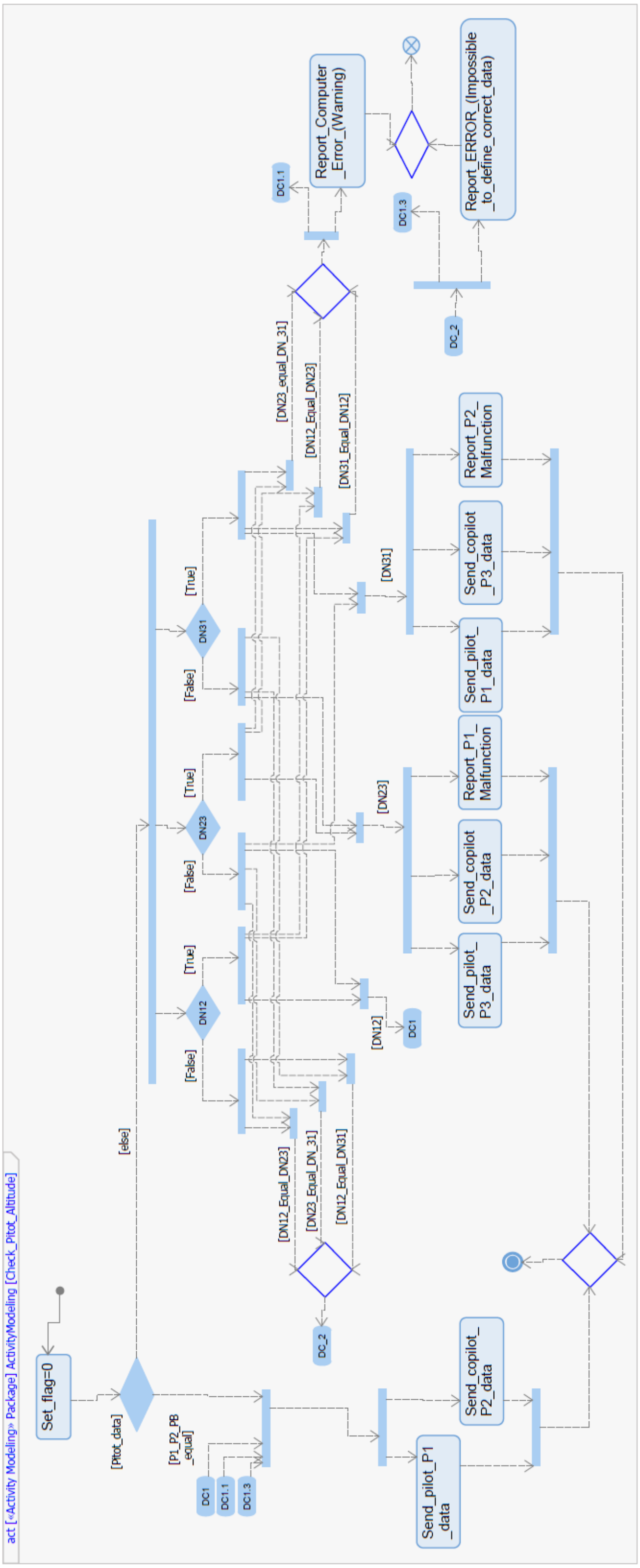


Figure 2.17: Check Pitot Altitude

Nowadays most of the behaviors expressed in these action diagrams are performed by computers and thus does not represent a physical components or design solutions as was until the seventies, but still provides many physical information.

Chapter 3

Work analysis and Conclusion

The goal of this work was not to develop a new configuration for the navigation system of an aircraft, neither to prove the effectiveness of an existing one: Was, instead, to analyse the overall development process, and to explore the advantages of the MBSE approach to developing a base model of an aircraft system that can be the baseline for future projects. This chapter will analyse the effectiveness of the results.

3.1 Work Analysis

3.1.1 The Model

In order to analyse the effectiveness of a single model as basis for multiple projects it has built a simplified model for the first steps of the development process. The software IBM Rhapsody that has been used has many possibilities of usage, in fact the SysML impose some formal rules, but allows many usage of the same "artifact". It has many useful capabilities, but also some issues: The requirements management capabilities of the software are really complex to be effective in a complex system like an aircraft. The System reproduction proposed is a limited static picture of a constantly evolving development model. The SysML diagrams offers more information than what can be seen just from the picture. This has allowed the binding of different parts and blocks through different connections and the definition of proprieties given to specific families of parts. The usage of SysML in a high level model like a airplanes one involves the effort of many specialists from different engineering fields supporting an easy communication between different aspects.

3.1.2 The Process

The process of model building, as already expressed, is an iterative procedure of definition, evaluation, analysis and verification. The Build of the analysed model has followed the phases of the classic developing, as expressed in the ISO/IEC/IEEE 42010 [15], the "System Engineering Handbook [22]. All the work has been conducted through one software: IBM Rhapsody, without involving any others, although, often many tools like IBM Engineering Requirements Management DOORS (DOORS) are used.

3.2 Conclusion

The following conclusion have been evaluated compared to the processes expressed in the ISO 15288:

- Knowledge management process: Due to the freedom of the SysML the development of a method with strict procedures, defined internally by the company, is mandatory for a positive outcome of the project, and to allow different developer to collaborate and to communicate effectively.
- Information management process: The great advantage of the MBSE approach is to group the information and the information sources into a unique model readable in different ways, to avoid the loss of information traceability due to any change and to avoid the information error during any communication through different developers.
- System architecture definition process: One of the objective of the system architecture definition process in common with one of the MBSE's: the purpose of generation of system architecture alternatives. The high effort of any choose through the developing process in the MBSE approach emphasize the effectiveness of the method in order to fulfill properly the requirements.
- Verification process: The MBSE through the SysML is not capable to manage all the different typologies of analysis needed in any phases of the developing, but allows the implementation of the results through a single unified Language. The SysML allows external links to any other file or resource to simplify the management process.
- Transition process: The MBSE allows, thought the traceability of any configurational decision and the different analysis conducted, to simplify the updating or changing of any system by starting from a advanced development phase.

The definition of a clear method of application of the SysML is mandatory to manage properly the developing process through many different companies, internal division, and developer, is also necessary to support the production of any type of documents for costumers, through the developing team to the certification agency.

A great attention must be posed on the correct integration of different information sources and typologies.

The overall goal of a single model that works as a basis for multiple projects is indeed a useful tool for the future, must be pointed out that it requires a great effort for be fully developed. The choose of SysML for the purpose is surely correct, but nowadays the use of this kind of tools is not as intense as it should be to build the entire model of the airplane.

3.3 Future development

3.3.1 Digital Twin

One of the future application of these kind of model is the evolution to digital twin. Considering that, to these days, the digital twin in the literature focuses only on the behavioral simulation of one or a limited number of scenarios. Currently the development of complex digital twin as multi-scale, multi-scenario and multidimensional applicable is not easy. Wenjie et al. affirms that some scholars are trying to develop a standardized method for complex system modelling, in order to predict and optimize behavior in any possible context[28]. The evolution of the MBSE model could, in the future, get to a point where the deep faithfulness to the real system allows the usage of the model to manage the maintenance in a better way. It could extend the components life cycle, in a safe life philosophy, by monitoring and simulating the operative life of the part through the model, and forecasting the failures modes and times. Humans might implement small deficiencies with tacit information, the machines not. It must, because of that, implement in a ”machine point of view” all the diagrams.[29]. The implementation of this kind of model can lead also to a great data acquisition during the operative life of the physical airplane increasing the reliability of the components, decreasing the inspections and simplifying the accident investigations.

3.3.2 Certification Process

The future development could, once again, create models so faithful to reality that the type certification process will be conducted mostly through these models. The advantage of this evolution is that it has a lower cost compared to physical tests, in fact the development of the model is already a main phase of the overall process. It will be only converted in a form in which it can be used to obtain the means of compliance. The implementation of all the risk analysis in the model allows the monitoring of the safety aspects through the developing process and could one day be a key process of the system life cycle processes. The implementation of the model could also be a important phase in new digital simulators development, in order to use reliable data to permit faithful analysis to the physical behavior of the future aircrafts.

Bibliography

Cited resources

[1] Benjamin S. Blanchard and John E. Blyle. *System Engineering Managemen.* John Wiley & Sons, Incorporated, 2016.

[2] Wang Haoqi et al. "System Engineering Method Based On Axiomatic Design And MBSE Modelling Framework". In: *Proceedings of the ASME 2016 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference IDETC/CIE 2016.* Aug. 2016.

[3] Moir, Ian, and al. *Civil Avionic Systems.* John Wiley & Sons, Incorporated, 2013.

[4] Ludvig Knöös Franzen et al. "Breackdown of System of Syestems Needs Using Architecture Frameworks, Ontologies and Description Logic Reasoning". In: *Aerospace* 8 (2021), p. 118. DOI: `https://doi.org/10.3390/aerospace8040118`.

[5] BSI, ed. *ISO/IEC/IEEE 15288. Systems and software engineering-System life cycle process.* 2023.

[6] P. W. G. Morris. "Interface management—an organization theory approach to project management". In: *Project Management Quarterly* 10 (1979), pp. 27–37.

[7] Ing. Ralf Lossack and H. Grabowsk. "The Axiomatic Approach In The Universal Design Theory". In: *Proceedings of ICAD2000 First International Conference on Axiomatic Design.* June 2000.

[8] Giulia Lucia Sicuso. "Definizione e Modellazione di funzioni cooperative e non per un Loyal Wingman come componente di System of Systems all'interno di uno scenario operativo". Politecnico di Torino, 2020.

[9] INCOSE. 2024. DOI: `https://www.incose.org/about-systems-engineering/system-and-se-definitions/systems-engineering-definition`.

[10] H Eisner. *Essentials of project and syste engineering management.* John Wiley & Sons, Incorporated, 2008.

[11] FAA. *System Engineering Manual. Version 3.1.* FAA, 2006.

[12] Sanford Fiedenthal, Alan Moore, and Rick Steiner. *A Pratical Guide To SysML.* Elsevier Inc, 2015.

[13] Tim Weilkiens. *Systems Engineering mit sysML/UML-Modellierung,, Analyse, Design.* Morgan Kaufmann, 2007.

[14] Yübo Wanga et al. "Integration of model based system engineering into the digital twin concep". In: *31st CIRP Design Conference 2021.* aTU Darmstadt Datenverarbeitung in der Konstruktion, Otto-Berndt-Str.2, Darmstadt 64287, Germany, 2021.

[15] BSI, ed. *ISO/IEC/IEEE 42010.* 2022.

[16] Franceso Antonio D'Amico. "Multi-Level Type Certification Approach in a multi-DOA context". Politecnico di Torino, 2023.

[17] Access 5 Systems Engineering and Integration Team. *Functional Requirements Document For HALE UAS Operations in the NAS Step 1.* Access Five, Nasa, UAV national industry team, 2006.

[18] ASD, ed. *S1000D.* 2012.

[19] *Performance-Based navigation manual Volume I: Concept and Implementation Guidance and Volume II: Implementing RNAV and RNP Operations.* ICAO.

[20] Alexander V. Nebylov and Joseph Watson. *Aerospace Navigation System.* John Wiley & Sons, Incorporated, 2016.

[21] EASA, ed. *CS-MMEL. Easy Access Rules for Master Minimum Equipment List.* 2014.

[22] NASA, ed. *Systems Engineering Handbook.* 2016.

[23] Ilias Maragakis et al. "Safety Management System and Safety Culture Working Group (SMS WG) [GUIDANCE ON HAZARDS IDENTIFICATION]". In: *ECAST* (2009).

[24] Sam Mannan. *Less'Loss Prevention in the Process Industries.* Elsevier Inc, 2012.

[25] jeffrey W. Vincoli. *Basic guide to System Safety. Third Edition.* John Wiley & Sons, Incorporated, 2014.

[26] AIM, ed. *ARNC429.* 2019.

[27] U.S.Dictionary. Apr. 24, 2024. DOI: `https://usdictionary.com/idioms/a-rainy-day/`.

[28] Wenjie Jia, Wei Wang, and Zhenzu Zhan. "From simple digital twin to complex digital twin Part I: A novel modeling method for multi-scale and multi-scenario digital twin." In: *Advanced Engineering Informatics* 53 (2022).

[29] Fabian Wilking et al. "SysML 4 Digital Twins – Utilization of System Models for the Design and Operation of Digital Twins". In: *Proceedings of the Design Society.* May 2022. DOI: `10.1017/pds.2022.184`.

[36] Eurocontrol, ed. *European GNSS Contingency/Reversion Handbook for PBN Operations, Scenarios and Options. PBN HANDBOOK No. 6, Draft v0.3.*

[68] SysMl.org. Apr. 5, 2024. DOI: `https://sysml.org/tutorials/sysml-diagram-tutorial/`.

Supplementary resources

[30] Prajwal Shiva Praksha et al. "Aircraft architecture and fleet assessment framework for urban air mobility using a system of systems approach". In: *Aerospace Science and Technology* 125 (2022).

[31] Sergei Gerasenko et al. "Beacon Signals: What, Why, How and Where?" In: *Computer* 34 (2001), pp. 108–110. DOI: `10.1109/2.955103`.

[32] Gustavo Esdras and Susan Liscouet-Hanke. "Development of Core Functions for Aircraft Conceptual Design: Methodology and Results". In: *Canadian Aeronautics and Space Institute AERO 2015 Conference.* Montreal, Canada, May 2015.

[33] Guruprasad Kulkarni and Sebastian Price. “MBSE Model On Gas Turbine Tip Clearance Control”. In: *Proceedings of the ASME 2019 Gas Turbine India Conference GTINDIA2019*. Dec. 2019.

[34] I. S. Dimov. *Global aeronautical communications, navigation, and surveillance (cns): Applications*. American Institute of Aeronautics and Astronautics (AIAA), 2013.

[35] Saurabh Mittal and Josè L. Risco Martìn. *Netcentric System of Systems Engineering with DEVS Unified Process*. Taylor & Francis Group, 2013.

[37] Laurent Moss et al. *An ESL Methodology for Rapid Creation of Embedded Aerospace Systems using Hardware-Software Co-Design on Virtual Platforms*. Ed. by SAE International. 2012.

[38] SAE International, ed. *Arp4761. Guidelines and Methods for conducting the safety assesment process on civil airborne systems and equipment*. 1996.

[39] SAE International, ed. *AIR6110. Contiguous Aircraft/System Development Process Example*. 2011.

[40] SAE International, ed. *ARP4754. Guidelines for Development of Civil Aircraft and Systems*. 2010.

[41] BSI, ed. *EN 9100. Quality Management Systems - Requirements for Aviation, Space and Defence Organizations*. 2018.

[42] Flight Assurance Procedure (FAP), ed. *Standard fot performing a failure mode and effects analysis (FMEA) and establishing a critical items list (CIL).*

[43] FAA, ed. *System design and analysis*. 1988.

[44] FAA, ed. *Airworthiness approval of attitude heading reference system (AHRS) Equipment. 20-181*. 2014.

[45] Department of Defense, ed. *MIL-HDBK-516C. Airwothiness certification criteria*. 2014.

[46] Department of Defense, ed. *MIL-STD-188-200. System design and engineering standards for tactical communications*. 1983.

[47] Department of Defense, ed. *MIL-STD-188-212. Subsystem design and engineering standards for tactical digital information link (TADIL) B*. 1992.

[48] Department of Defense, ed. *MIL-STD-188C. Military communication system Technical Standards*. 1964.

[49] Department of Defense, ed. *MIL-STD-291C. Standard Tactical Air Navigation (TACAN) Signal*. 2019.

[50] Department of Defense, ed. *MIL-STD-1553C. Digital Time Division Command/Response Multiplex Data Bus*. 2018.

[51] ICAO, ed. *Aeronautical Telecommunications. Annex 10. Volume I: Radio Navigation Aids*. 2006.

[52] ICAO, ed. *Aeronautical Telecommunications. Annex 10. Volume II: Communication Procedures including those with PANS status*. 2001.

[53] ICAO, ed. *Aeronautical Telecommunications. Annex 10. Volume IV: Survelliance and Collision Avoidance Systems*. 2007.

[54] ICAO4, ed. *Aeronautical Telecommunications. Annex 10. Volume V: Aeronautical Radio Frequency Spectrum Utilization*. 2006.

[55] Inc RTCA, ed. *DO-196. Minimum Operational Performance Standards (MOPS) for Airborne VOR Receiving Equipment Operating Whitin the Radio Frequency Range of 108-117.95 MHz*. 1986.

[56] Inc RTCA, ed. *DO-197A. Minimum Operational Performance Standards (MOPS) for an Active Traffic Alert and Collision Avoidance System I (Active TCAS I)*. 1997.

[57] EASA, ed. *CS-25 (Amendment 27). Easy Access Rules for Large Aeroplanes*. 2022.

[58] EASA, ed. *CS-ETSO (Initial issue). Easy Access Rules for European Technical Standard Orders*. 2018.

[59] EASA, ed. *CS-ETSO Amendment 17. Certification Specifications for European Technical Standard Orders*. 2022.

[60] EASA, ed. *CS-ETSO Amendment 15. Certification Specifications for European Technical Standard Orders*. 2020.

[61] EASA, ed. *CS-ETSO Annex II. Subpart B- List of ETSOs (Index 1 and Index 2)*. 2018.

[62] ITU, ed. *Radio Regulations. ITU-R Recommendations incorporated by reference*. 2020.

[63] ITU, ed. *Radio Regulations. Appendices*. 2020.

[64] ITU, ed. *Radio Regulations. Articles*. 2020.

[65] IEEE, ed. *Standard for applicartion and management of the Systems Engineering Process*. 2005.

[66] IEEE, ed. *Standard for applicartion and management of the Systems Engineering Process*. 2005.

[67] European Defence Agency, ed. *EMAR 21 Edition 2.0. Certification of military aircraft and related products, parts and appliance, and design and production organisations*. 2021.

List of Figures and Tables

Appendix A

SySML

In the following section will be presented the SysMl diagrams characterization:

The SysML has nine type of diagrams, categorized as shown in figure A.1:

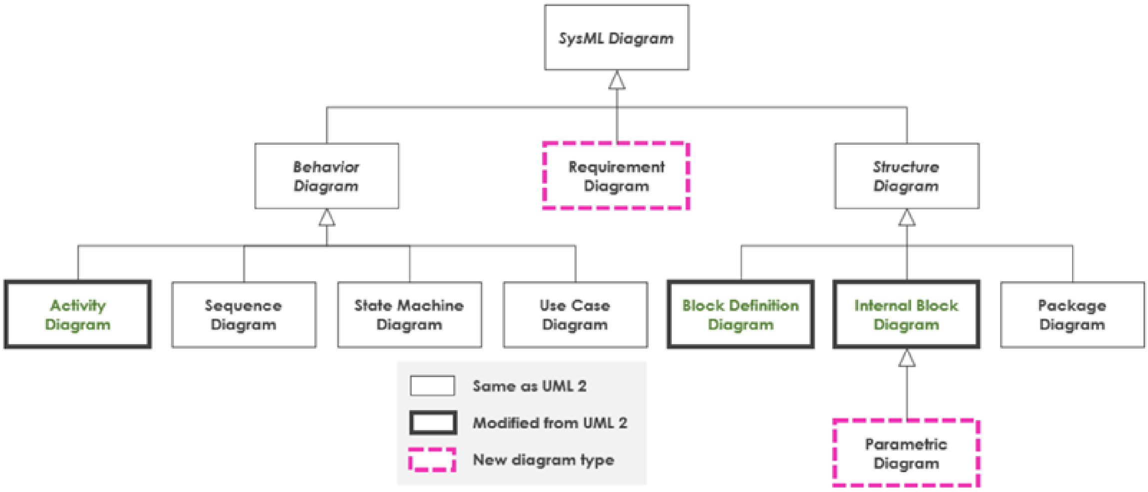


Figure A.1: SysML Diagrams

The different diagram types are used for different purpose[68]:

- Block Definition Diagrams (BDD): used to decompose in blocks the structure of the system and to define the relations between the blocks.
- Internal Definition Diagrams (IBS): used to define the internal structure of a single block of a BDD showing the composing parts between them.
- Requirement Diagrams: used to define the requirements of the system, including functional, performance, interface requirements. This kind of diagram provide a

simply way to trace requirements and to verify they're fulfillment.

- Parametric Diagrams: used to describe the behavior of the system showing how the system respond to different inputs and external conditions. It shows the relation between the system parameters and the correspondent numeric values.
- Sequence Diagrams: used to describe the behavior of the system showing the sequence of messages between the sending and receiving components. This kind of diagram is used to verify the behavior of the system in sunny or rainy day conditions.
- State Machine Diagrams: used to define the behavior of the system showing the state of the system through time.
- Activity Diagrams: used to define the activity flux of a system, shows the step sequence of a process and the relations between the steps.
- Use Case Diagrams: used to model the interaction between a system and its users, it describe behavior in terms of high-level functionality and usage.
- Package Diagrams: used to manage the different elements of the system.

In addition to this diagrams there are allocation table, useful to allocate requirements to specific components to trace it easily.

The following section will report all the diagrams, developed during the project, that has not been exposed in the main section.

Appendix B

Requirements

In the following section are reported all the Requirement diagrams developed during the work. In figure B.1 are represented the high level requirements derived from a Boeing worksheet. Are represented also some hyperlink used during the development to navigate easily in the model (in red the one effectively connected to other diagrams.

In figure B.2, B.3, B.4, B.5 and B.6 are detailed the requirements sons of "Perform Mission"

In figure B.7 is represented the FHA relations between the different requirements, one for each different combination of flight phase, flight condition and fault.

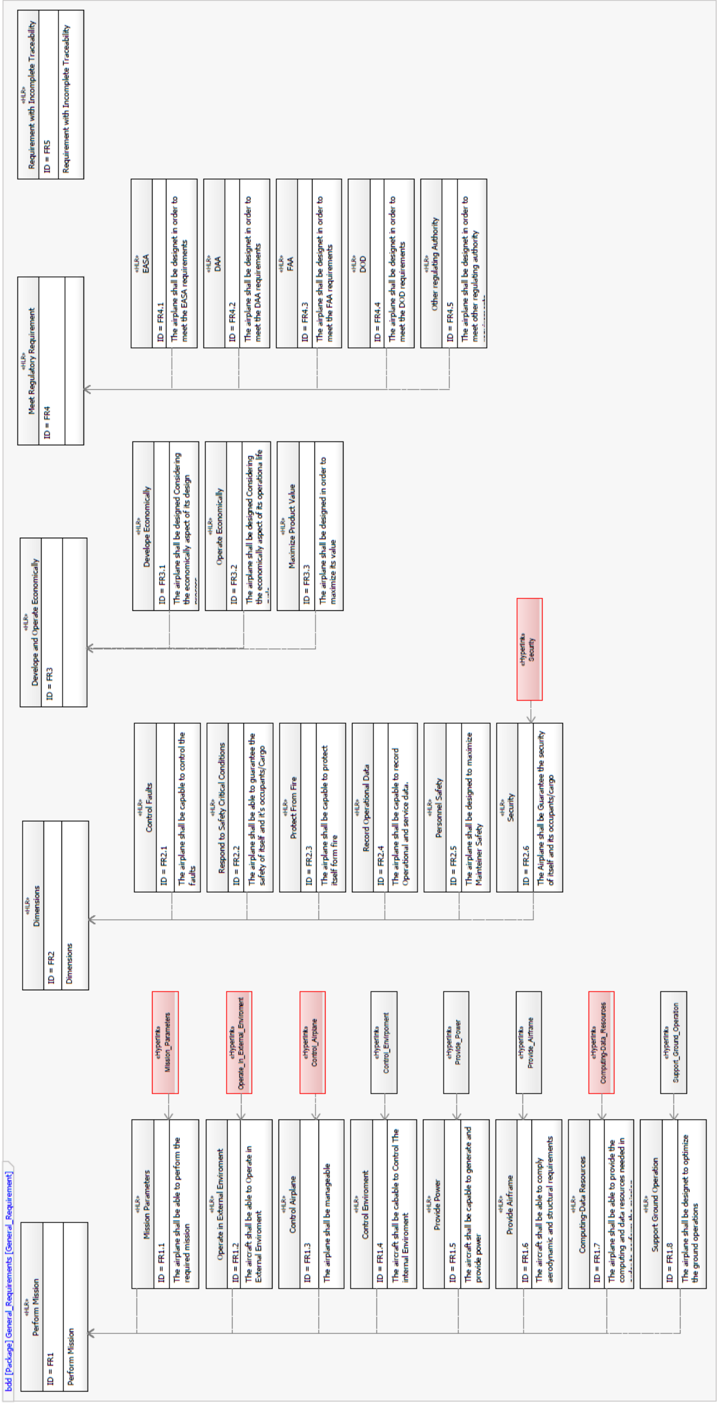


Figure B.1: General requirements

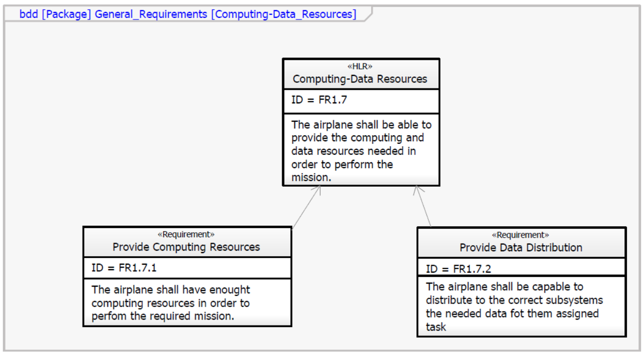


Figure B.2: Computing air data resources

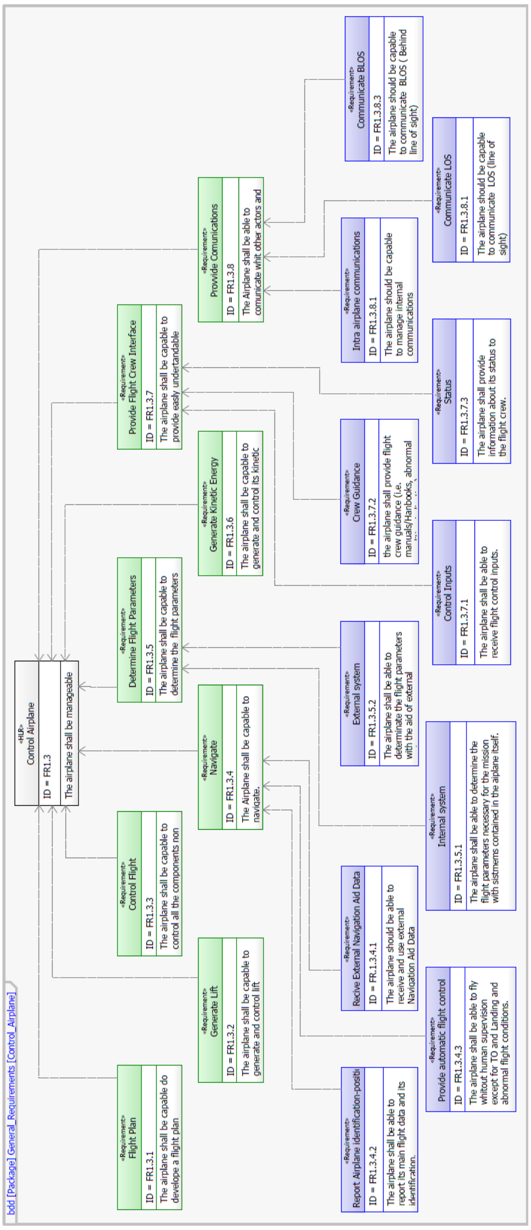


Figure B.3: Control Airplane

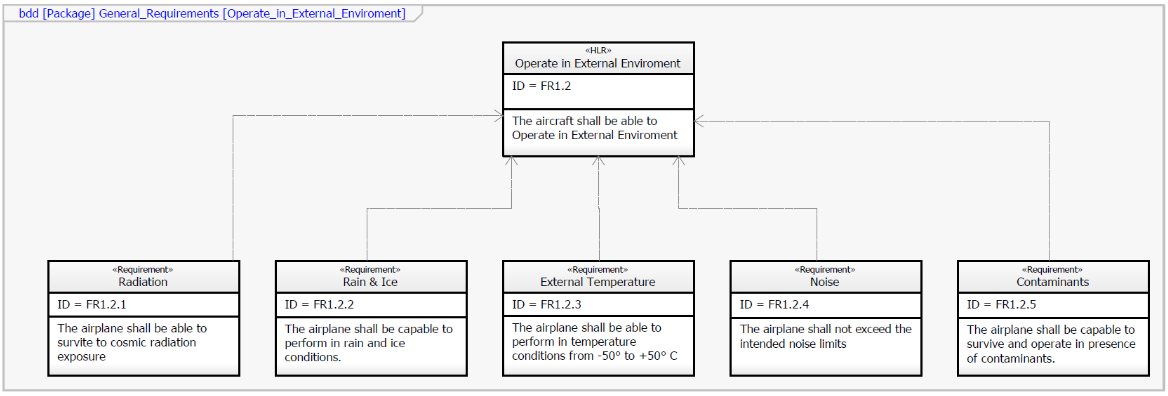


Figure B.4: Operate in external Enviroment

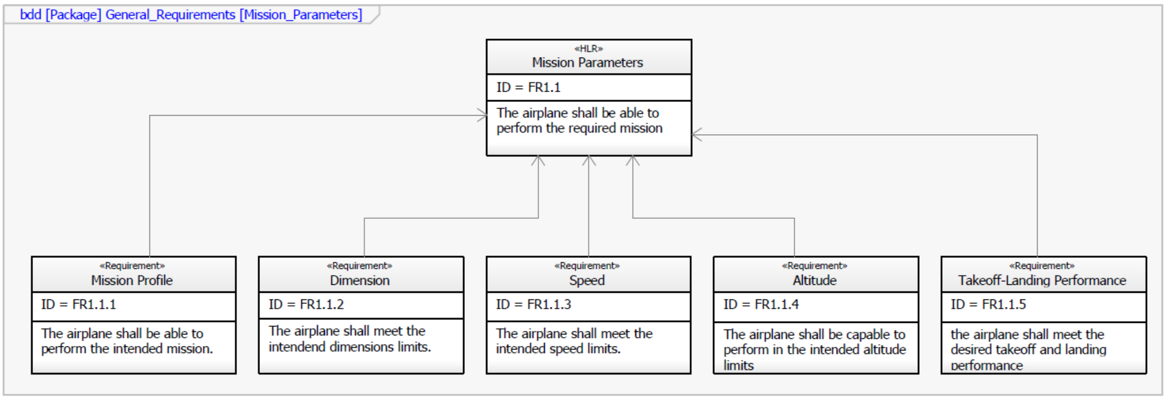


Figure B.5: Mission Parameters

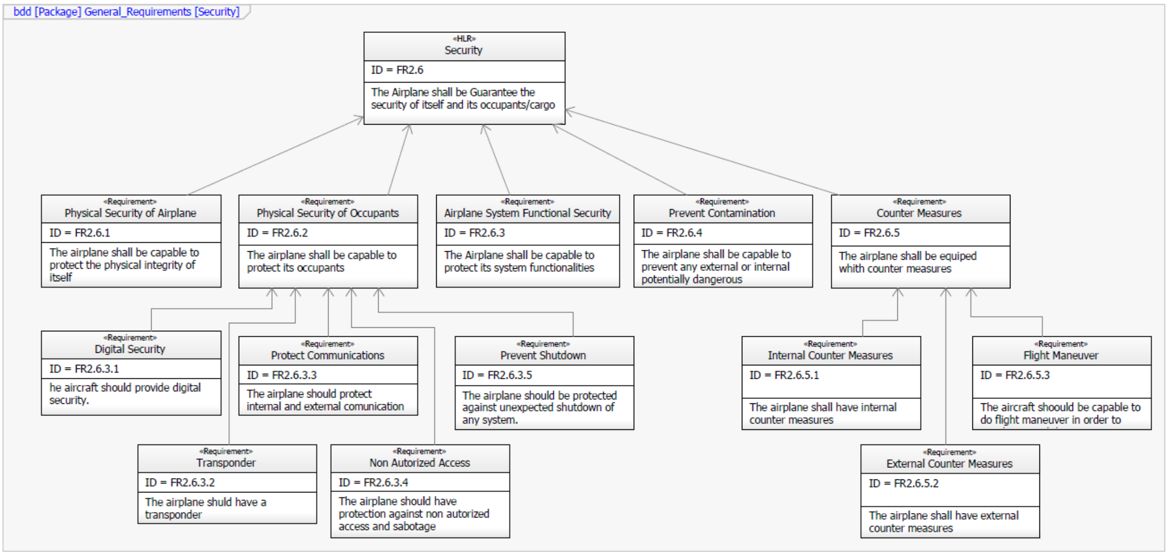


Figure B.6: Security

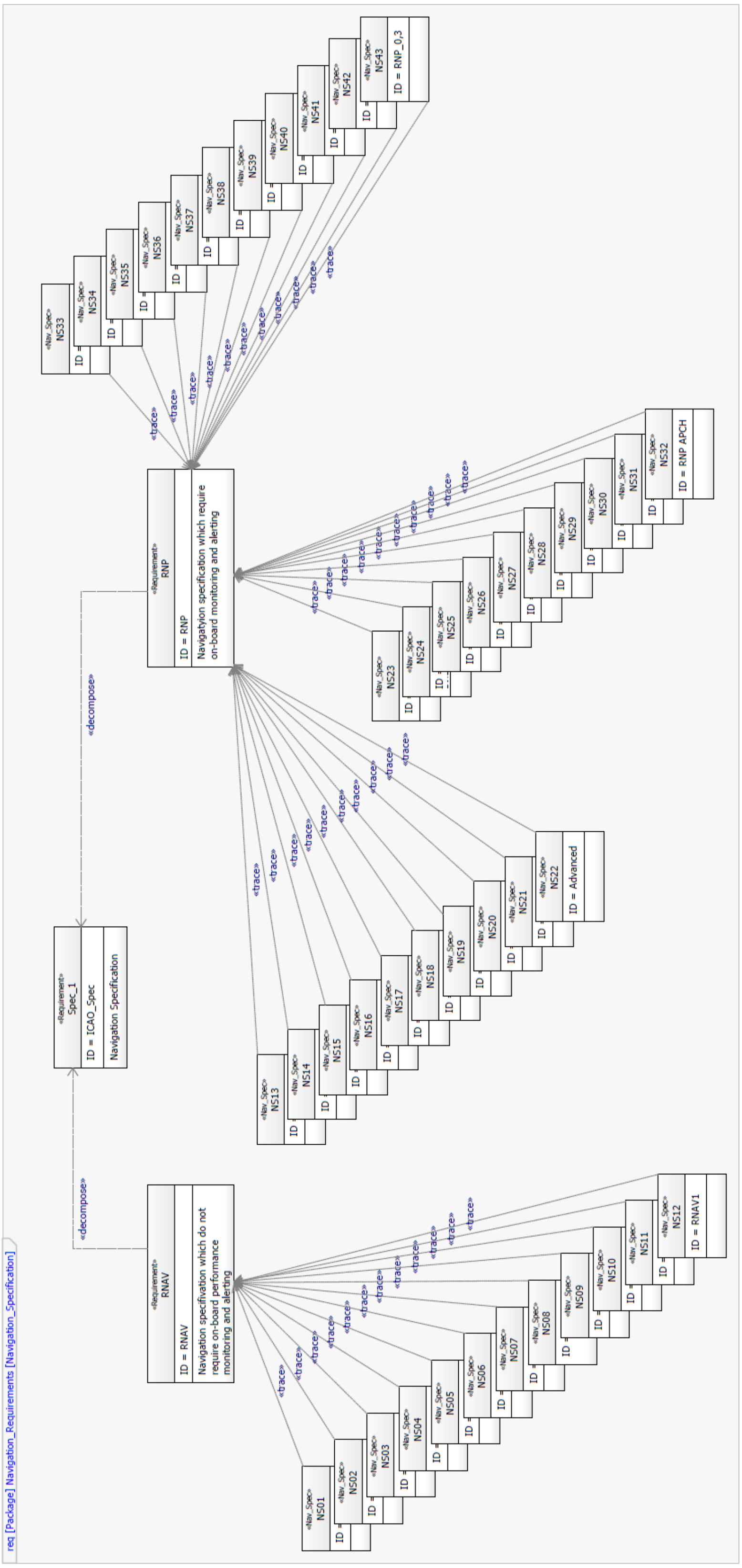


Figure B.7: Specification[36]

Appendix C

BDD

In the following section are reported all the BDD developed during the project. In figure C.1 is represented the decomposition of the Surveillance and Identification system in its easiest way.

In figure C.2 is represented the Communication system, it is easy viewable that it has many interconnections between the different subsystems.

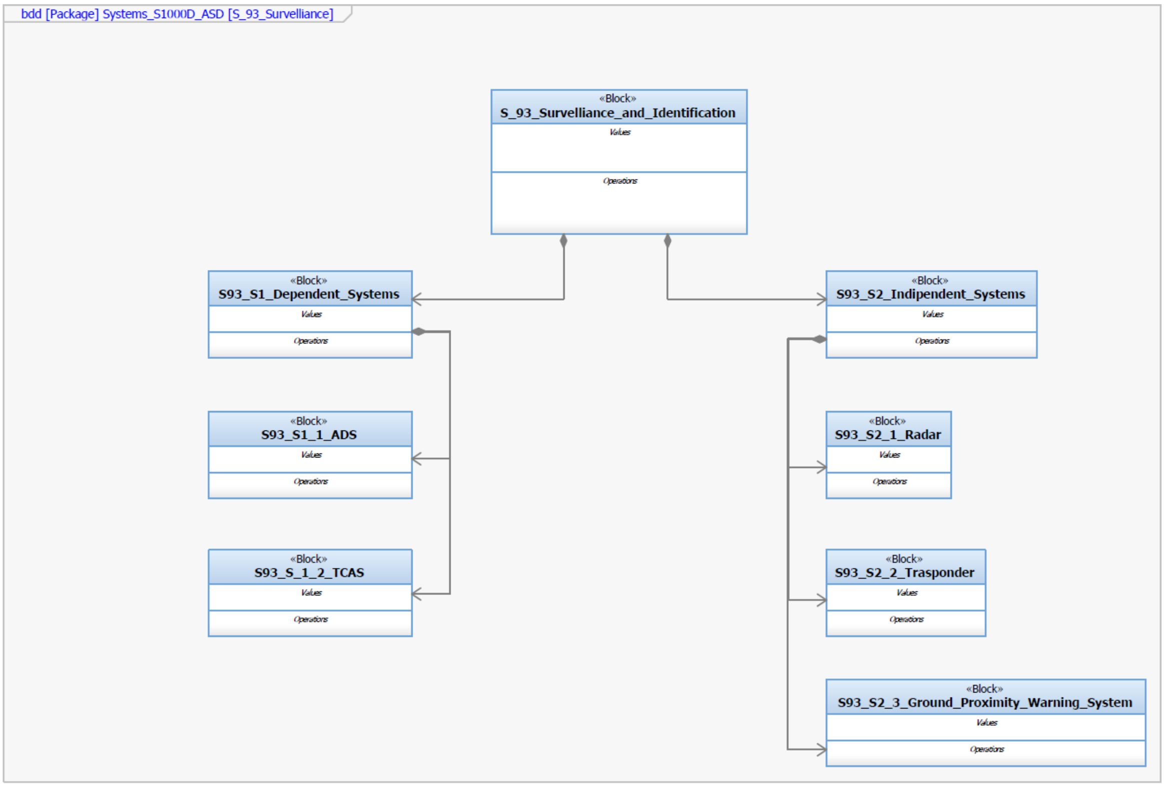


Figure C.1: Surveillance and identification system

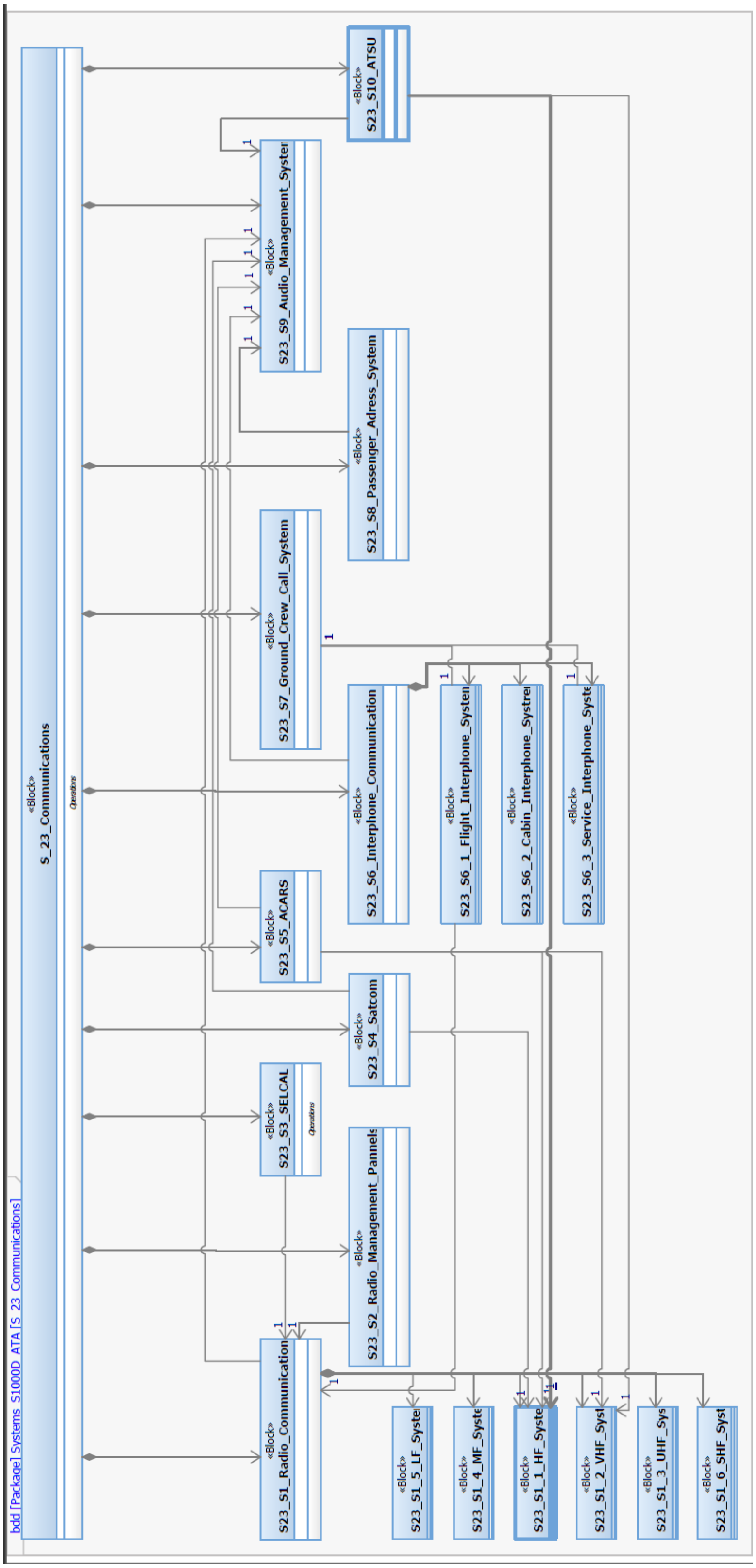


Figure C.2: Communication system

In figure C.3 is represented one of the most powerful instrument of IBM Rhapsody, a diagram created from the program that shows all the relations of the Pitot system. This kind of diagrams are creable in any moment for any different element.

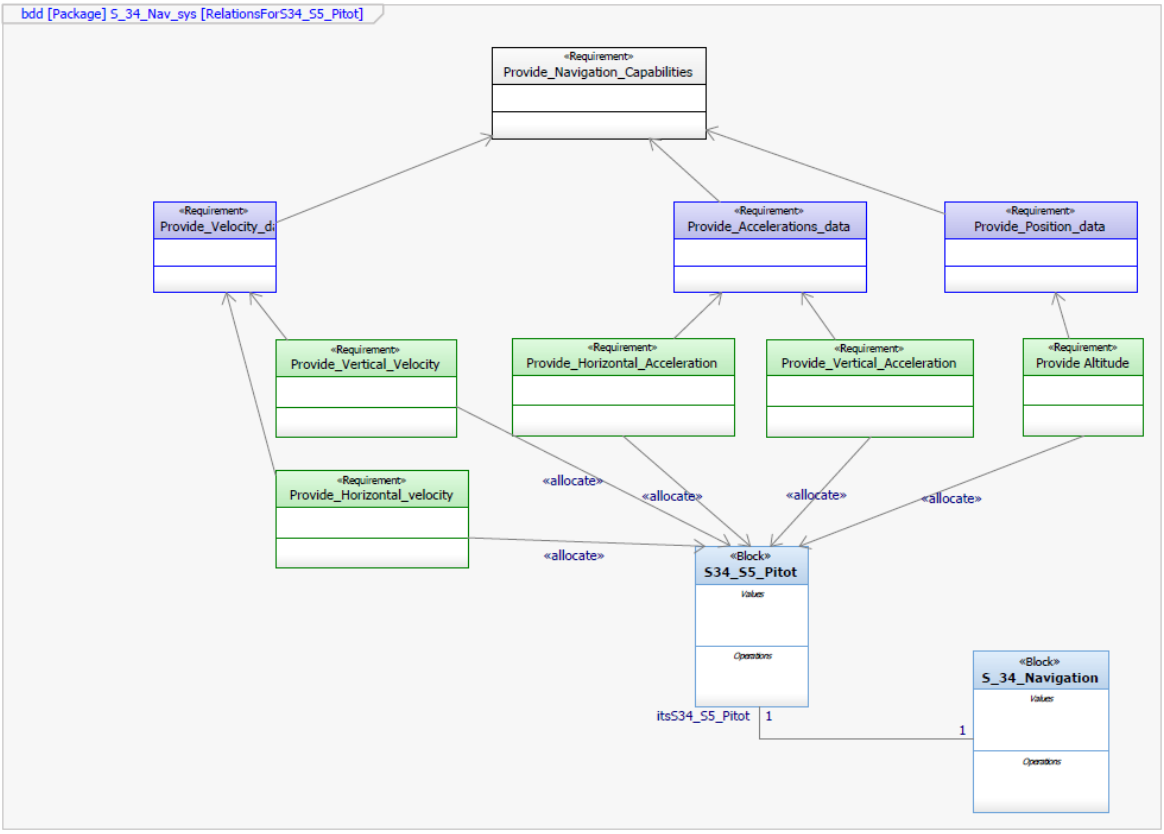


Figure C.3: Pitot tube relations example

Appendix D

IBD

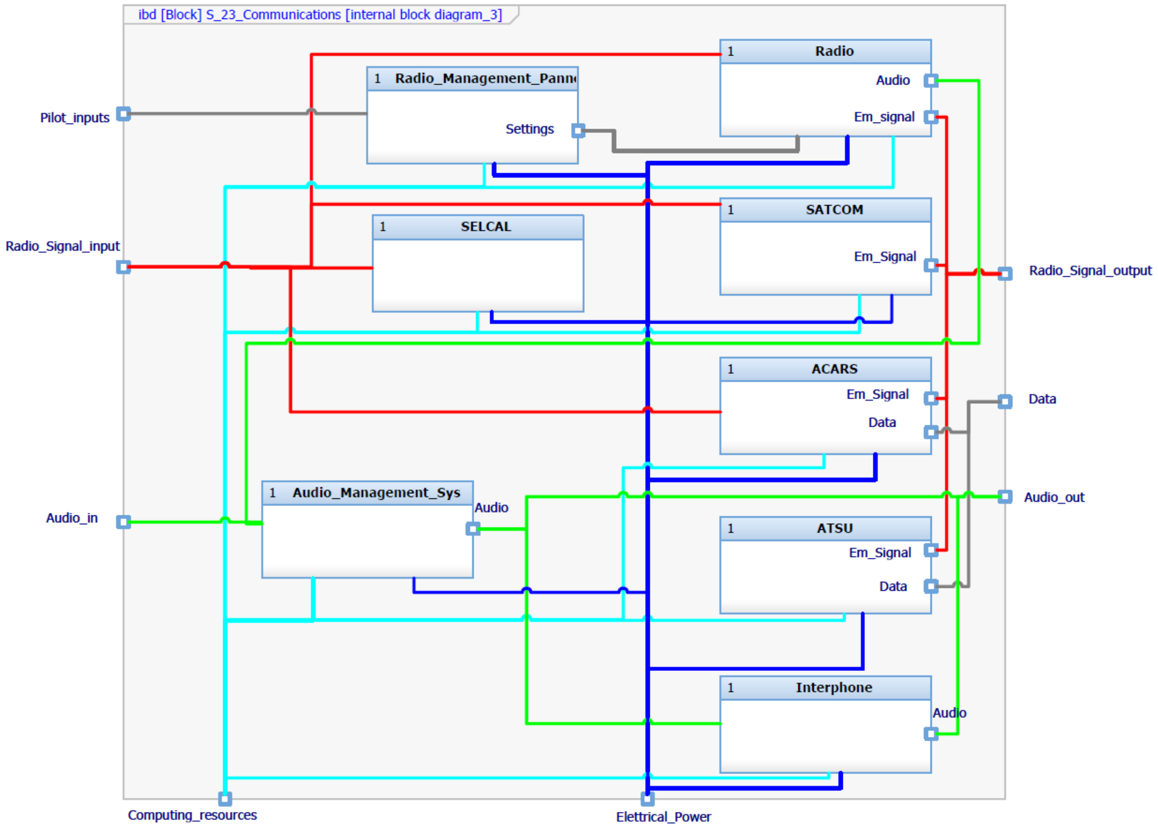


Figure D.1: Communication System

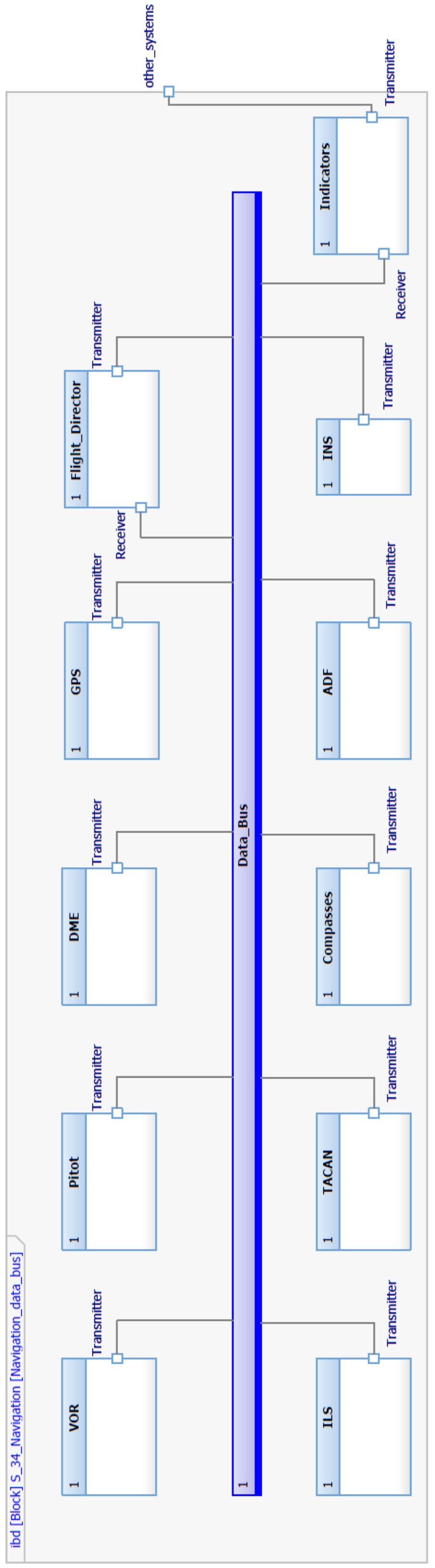


Figure D.2: Navigation system with data-bus

Appendix E

FHA

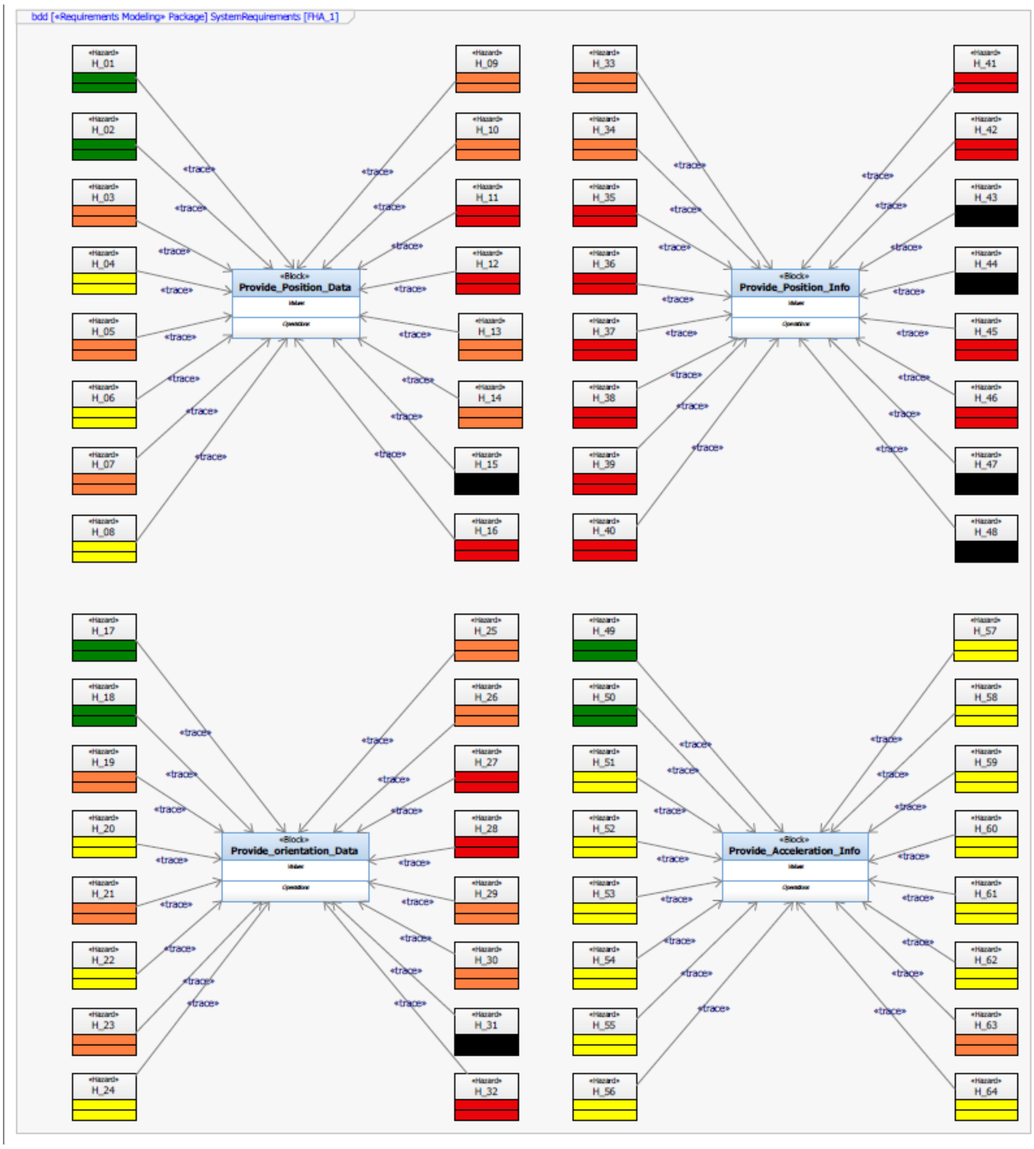


Figure E.1: FHA relations