Preliminary Reliability and Safety Assessment Methodology for Trans-Atmospheric Transportation Systems

Abstract

Purpose – The paper aims at proposing a methodology for a Safety and Reliability Assessment for the conceptual and preliminary design of very complex and disrupting-innovative systems like trans-atmospheric vehicles are. The proposed methodology differs from existing ones because does not rely on statistical data at aircraft-level but it exploits the statistical population at components-level only. For the sake of clarity, the paper provides some preliminary results of the application of the methodology at system-level. The example deals with the safety and reliability assessment of a very complex propulsion system aimed at guaranteeing Vertical Take-Off and Landing capabilities of a suborbital vehicle.

Design/methodology/approach – The proposed methodology is strongly based on a Systems Engineering approach. It exploits safety and reliability assessment analyses which have already been developed in both aeronautical and space engineering domains, but it combines them in an innovative way to overcome the lack of statistics at aircraft level. The methodology consists of two different steps: a qualitative top-down process, allowing a functional and physical decomposition of the transportation system and a following quantitative bottom-up approach, which provides the estimation of System-level reliability and safety characteristics starting from the statistical estimation of the components' characteristics.

Findings – The paper presents a new methodology for the preliminary reliability and safety assessment of innovative transportation systems, like hypersonic ones, since the conceptual design phase, overcoming the big problem of lack of statistical data.

Research limitations/implications – The paper shows the application of the articulated methodology to a limited case-study. A complete example of application of the methodology to estimate safety and reliability characteristics at vehicle level will be provided in feature works.

Practical implications – The methodology has been proposed to be exploited in international research activities in the field of hypersonic transportation systems. Furthermore, a massive application of this approach would allow to create a database for the generation and the update of semi-empirical models focused on high-level estimations of Reliability, Availability, Maintainability and Safety (RAMS) characteristics. Moreover, the proposed safety assessment has been conceived to be fully integrated within a typical conceptual design process.

Originality/value – The existing literature about safety and reliability assessment at the early design stages proposes pure statistical approaches which are usually not applicable to highly innovative products, where the statistical population is not existing, like, for example, in the case of trans-atmospheric vehicles. This paper describes how to overcome this problem, through the exploitation of statistical data at components-level only through the combination of these data to estimate RAMS characteristics at aircraft-level thanks to functional analysis, concept of operations and typical safety assessment tools, like Functional Hazard Analysis, Failure Mode and Effect Analysis, Reliability Block Diagram and Fault Tree Analysis.

Keywords Safety assessment, suborbital parabolic flights, hypersonic transportation systems, Vertical Take-Off and Landing.

Paper type Conceptual paper

Introduction

Hypersonic transportation systems are becoming the joining ring between space and aeronautical domains from both the industrial and the research activities perspectives (Tauri Group, 2012). Lot of efforts are currently employed by different research centres and agencies and also from academia.

From the one hand, the possibility of proofing structures and materials able to survive very extreme environmental conditions like the ones experienced in a hypersonic flight is of absolute interest for space industries. These capabilities can be exploited in several missions implying a re-entry manoeuvre on Earth but also on other planets or celestial bodies. From the other hand, looking at the problem from aeronautical perspective, the capability of reaching hypersonic speeds is fascinating designers, companies and also passengers, especially because of the envisaged drastic reduction in flight duration due to the maximum achievable speed.

In the last decade, not only national or governmental agencies showed their interest in these topics but also several private stakeholders are trying to develop their own transportation system. In particular, many of these visionaries are not only focusing on long-haul missions but also to provide touristic flight services to allow passengers experiencing microgravity and an amazing view of the Earth curvature as well as the possibility, for the scientific community, to exploit this service to perform microgravity tests.

From the technical point of view, suborbital parabolic flights are characterized by a lower level of complexity with respect to the hypersonic missions and, for this reason, the related vehicles are considered as test-bed for different kind of enabling technologies (Santoro et al., 2014). Moreover, ad-hoc vehicles designed for parabolic suborbital flights can be considered themselves the short-term goal of a technology development roadmap (Cresto et. al, 2016) aimed at the reaching the routine operations of a hypersonic crew transportation system.

In any of these enterprises, considering the fact that they are dealing with really disrupting technologies, special focus should be devoted to ensure a reasonable level of safety to the crew, the flight participants, the on-ground personnel and to all non-involved people. It is mainly for this reason that it is very important to take safety into account since the very beginning of the design process. In both aeronautics and space tradition, the very first rough estimations of the vehicle failure rates and the allocation of this value on the systems is mainly based on historical data. However, in case of spaceplanes, these approaches cannot be anymore exploited due to the lack of useful statistical population. This paper tries to overcome this problem, proposing a two-steps methodology consisting in a sequence of qualitative and quantitative evaluations that can enable to perform a safety assessment at conceptual design level.

In addition, the paper provides an example of the application of the approach to the design of a complex propulsion system aimed at guaranteeing the fulfilment of vertical take-off and landing requirements and powering a spaceplane up to a target altitude of 100 km.

Section *Safety Assessment Methodology* aims at describing the methodology with a step-by step approach, pointing out possible ways to integrate these analyses within the currently exploited conceptual and preliminary design methodologies. Then, before starting with the application of this process to the evaluation of the safety levels of a peculiar propulsion system for VTOL spaceplane, the Section *Vertical Take Off and Landing Strategy* provides a brief description of the reference mission and vehicle highlighting the different strategies to ensure Vertical Take-Off and Landing (VTOL) capabilities, justifying the selected architecture and pointing out the main reasons why this one is so deeply affected by safety considerations. Then, Section *Integrated Methodology* shows the way in which this approach has been followed for the definition of the above-mentioned propulsion system architecture, providing also some preliminary quantitative results. Eventually, the integration of the methodology within a proper Model Based Systems Engineering tool-chain is proposed as future development of this study.

Safety Assessment Methodology

Considering (NASA, 2014), Safety can be defined as: *freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment*. In any given application, the specific scope of safety must be clearly defined by the stakeholders in terms of the entities to which it applies and the consequences against which it is assessed. For example, for non-reusable and/or non-recoverable systems, damage to or loss of equipment may be meaningful only insofar as it translates into degradation or loss of mission objectives.

It is not possible to deal with vehicles of mission 100% safe but in the real world it is necessary to accept a certain degree of risk. From this consideration, the principle of being As Safe As Reasonably Practicable (ASARP) has also been derived. Always referring to (NASA, 2014), a determination that a system is ASARP entails weighing its safety performance against the sacrifice needed to further improve it.

In this context, System Reliability and Safety techniques have been developed.

Before entering in the detail of the integrated methodology, the following subsections aim at describing the main tools. It is worth to notice that it consists of very well-known tools currently used in both aeronautical and space domains (Chiesa, 2010), (Chiesa et al., 2013), (Viscio et al. 2014), (Viscio et al. 2015).

Considering the typical aeronautical approach, safety assessment methodologies provide engineers with proper knowledge and tools to carry out a-posteriori checks in order to verify the compliance of the already completed design to the high level safety requirements (from regulations or from stakeholders). In the last decades, this approach has been abandoned and a-priori evaluations have been preferred. For this reason, several methodologies suitable to design reliable and safety systems allowing RAMS estimations since the beginning of the design process, have been proposed.

On the other hand, safety design has ever been considered a crucial topic in space transportation (Musgrave, 2009), (Stamatelatos et. al, 2011) and especially for the mission including humans on-board. New Probabilistic Risk Assessment methodologies have been developed since the Space Shuttle era and are currently in-depth evaluated with the aim of increasing the public consensus on reusable space transportation systems and on space commercialization.

The proposed methodology is based on the exploitation of the tools developed and used in both aeronautical and space domains but arranged within a dual process that would allow at first, to use these tools to formalize the structure of the system (from reliability standpoint) and then, to derive the characteristic value of the system, starting from assumptions on the basic elements of the tree.

System safety is considered a proper discipline (NASA, 2014), directly derived by the application of systems engineering approach and management principles, criteria, and techniques to optimize safety within the constraints of operational effectiveness, time, and cost throughout all phases of the system life cycle. For this reason, in this paper, the author proposes an integrated methodology that allows to take safety into account since the beginning of the design process and in a harmonized way with the rest of the usual design activities. Thus, the suggested tools are typically those typically used to perform a high-level safety assessment in conceptual design. However, this paper suggests an innovative way to connect all these tools within a well-defined and structured conceptual design methodology. As it will be discussed later, this is the first step to reach the complete automation of this process, since the aim of translating it in a Model Based Systems Engineering (MBSE) Methodology is envisaged. In particular, the selection of tools (not only software but also diagram etc…) and the proper sequence by which they are used, i.e. the tool chain, can be the most relevant difference between the ARP 4761 and the methodology proposed in this paper.

An Integrated Safety Design Methodology

As it was announced above, the here proposed methodology consists of two major parts:

1. A Qualitative Analysis where, starting from the top-level design activities, a safety assessment is performed following a top-down approach, from the mission level to the equipment level. This process does not imply any quantitative evaluations.
2. A Quantitative Analysis where, starting from the results of the Qualitative Analysis, exploiting available statistics at equipment level and following a bottom-up approach, it is possible to retrace the way to derive the probability of the top-event related to the mission or to the system.

The following subsections aim at describing into details the two parts of the methodologies, highlighting its intrinsic feature of being fully integrated within a modern conceptual design activity based on a Systems Engineering approach.

Qualitative Process

This subsection aims at providing a detailed description of the sequence of actions summarized in Fig. 3. This first part of the methodology aims at deriving the basic elements composing the high-level system, starting from the identification of all the possible people and public or private entities interested in the design of the innovative aerospace product and in all the possible advantages coming out from its exploitation.

It should be noticed that the very first step, i.e. the Stakeholder analysis, coincides with the usual starting activity of each conceptual design of innovative products, consisting in looking for all possible interested private or public entities and trying to evaluate their needs. At the same time, as soon as the product category has been defined, it is important to deeply investigate the market, in order to understand where to sell the product and also to evaluate if the technologies that should be developed for this application can be interesting in different fields. Moreover, a review of the national and international regulations related to the development but also to the operations of the vehicle should be considered and a first draft list of constraint can arise.

From this preliminary analysis, a mission statement and consequently a first list of objectives and requirements can be derived. At this point it is possible to concretely starts the safety assessment creating a simple Functional Tree (Chiesa, 2010). Within the conceptual design phase, with a Systems Engineering approach, Functional Trees are used to look at the system from a broader functional perspective, allowing to derive all the functionalities or capabilities the System should guarantee to fulfil the main objectives. While these functions are on one side associated to subsystems, equipment and components able to perform these functions, they can also on the other side be exploited as inputs to carry out the Functional Hazard Assessment (FHA) at aircraft level.

Functional Hazard Assessment is a logical examination of functions to identify and classify failure conditions related to those functions according to their severity (SAE, 1996). The objective of the FHA is to consider functions at the most appropriate level and to identify failure conditions and the associated classifications while considering both loss of functionalities and malfunctions. It is important to notice that the FHA, especially if carried out at system or at lower levels, should identify the failure conditions for each phase of flight when the failure effects and classifications vary from one flight phase to another. The FHA also allows to derive safety requirements needed to limit the function failure effects which affect the failure condition classification. Once the high level requirements have been identified, they may be used to generate lower level requirements. As well as for all the other categories of requirements, this process shall continue iteratively, until the design process is complete. The most common and useful way to perform a FHA is to create a table view where this data can be organized, as part of the Preliminary System Safety Assessment process for the systems or items.

It is worth to notice that in Figure 3, where the overall process is shown, there are two levels of FHA, the Aircraft level FHA and the System-Subsystem level FHA. Indeed, the FHA will be carried out at different levels of the design process but exploiting the same principles.

Coming back to aircraft level, once the functional tree and FHA have been derived, each failure condition identified by the FHA should become the top-event of a Fault Tree.

Fault Tree Analysis is a deductive, failure-based approach that starts with an undesired event (called top event) and then logically determines (deduces) its causes using a systematic, top-down approach. In determining the causes, a Fault Tree (FT) (Figure 1) is constructed as a logical illustration of the events and their relationships that are necessary and sufficient to result in the top event. To carry out FTA, a real tree consisting in boxes and connectors should be built. In particular, the types of boxes used identify the different kind of events, while the different connectors stand for the Boolean algebraic symbols (“AND” and “OR”) should be used to specify the relationships among the several events.

The FT is a qualitative model but provides extremely useful information on the causes of the undesired event. The FT can also be quantified to provide useful information on the probability of the top event occurring and the importance of all the causes and events modelled in the FT.

In this way, a FTA can be carried out taking into account that each basic event of all the FTs will become the new failure condition for a specific function of a lower level FHA. Moreover, following the procedure explained for the aircraft-level FHA, this lower-level FHA should also receive inputs from Functional Tree carried out for the relative design level.

Then, to continue in the analysis, it is necessary to move from a strict functional view of the system to a more product-based stand point. This is usually performed within the design procedure based on SE approach, linking the results of product trees (Chiesa, 2010) with the possible way of working of the system itself or its behavior during its operative life, creating the so called Concept of Operations. The Concept of Operations allows describing how the system will be operated during its entire life cycle, in order to achieve the mission objectives. Typical analyses contained in ConOps include evaluations of mission phases, operation timelines, operational scenarios, end-to-end communications strategy, command and data architecture, operational facilities, integrated logistic support and critical events.

Carefully evaluating the results of the Concept of Operations analysis and taking into account the results of the functional analysis, the Reliability Block Diagrams (RBDs) can be derived. Reliability Block Diagrams are graphical representation used to reproduce the way of working of a certain system or subsystem in a well-defined mission phase and operative mode. Indeed, depending on the operative modes, the system could be schematically represented through different layouts. Exploiting existing reliability theories, it is possible to translate the scheme in an algebraic equation in which the known values are the failure rates of the different components and the unknown parameter is the system or subsystem Reliability.

Figure 1 Example of Fault Tree (left) and Reliability Block Diagram (right)

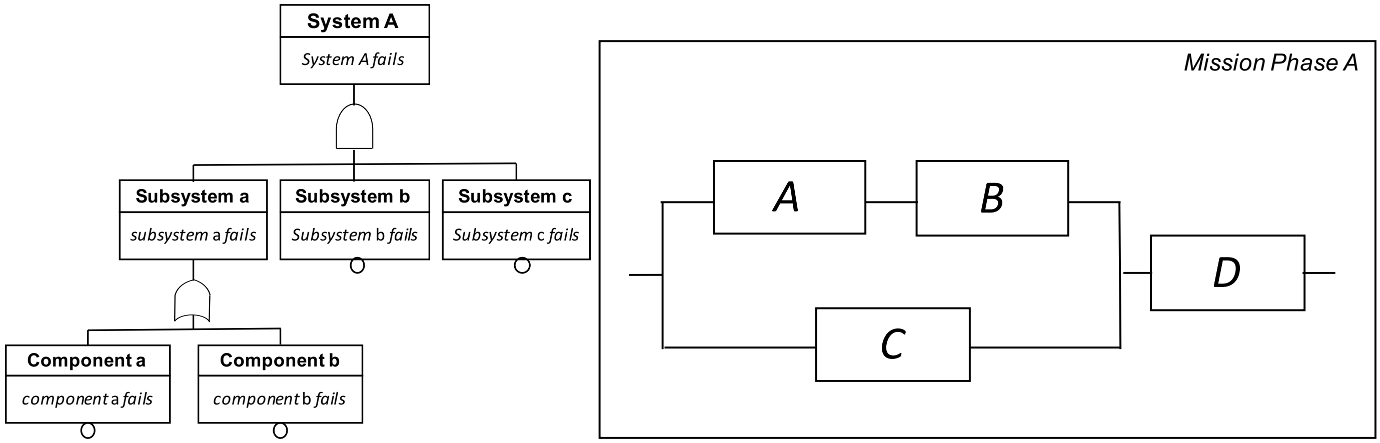


Figure 2 Example of FHA (left) and FMEA (right)

Function	Phase	Failure Condition	Failure Effect	Risk

Component	Failure Mode	Failure Effect	Failure Causes

Then, on the one hand, each component of the RBD can be in depth evaluated from the safety stand point exploiting the Failure Modes and Effects Analysis (FMEA), while on the other hand, the way in which the different components are mutually interfaced will define the logic operators of the related Fault Tree.

The Failure Modes and Effects Analysis is a systematic analysis of the way in which each subsystem or components can be affected by malfunctions, thus behaving differently if compared to what it was expected in nominal mode. For each type of failure, this analysis allows to induce the effect related to this failure that could be experienced by the system. Then, starting from the failure modes and from the possible causes of these mishaps, the failure effects and its seriousness can be estimated. Similar to what has been presented in the previous subsections, also in this case, it is possible to exploit this tool in an iterative way in order to obtain at each step, a new set of more detailed information.

At the lowest level of decomposition (equipment level) the failure effects of the FMEA are the basic events of the FTA.

Eventually, this first part of the methodology will be used to derive the functional and behavioural structure of the system, reaching a decomposition sufficiently low level such that it is possible to assign numerical values of failure rates to each basic component. This will be the first activity of the quantitative methodology (bottom-up approach), in-depth analysed in subsection “Quantitative process” that would lead to the estimation of an aircraft level failure rate to be compared with existing regulation and/or high level constraints.

Quantitative Process

Once the activities described in the previous section have been completed, the quantitative analysis can start. The process is summarized in Figure 4 where the process followed should be read from bottom to the upper part. At the beginning, it is necessary to consider the lowest event that could occur (i.e. the event related to a malfunctioning of one of the lowest-level identified component) and the smallest identified components of the system and associate the probability of occurrences to each of them. It is important to notice that at the beginning of this process, a deep analysis and research of available statistics shall be conducted. Then, it is reasonable to proceed with a bottom-up approach aimed at solving the aforementioned probability equations, reaching the top-level event as graphically summarized in Figure 4. In particular, the quantitative process exploits all the Fault Trees previously derived in the qualitative process, starting from the lowest level until reaching the aircraft-level Fault Tree.

Exploiting a similar approach, in addition to the Top Event Probability, estimations of Mission Reliability can also be carried out, solving the Reliability Block Diagrams derived for each mission phase.

Figure 3 Scheme of the Methodology, the qualitative approach

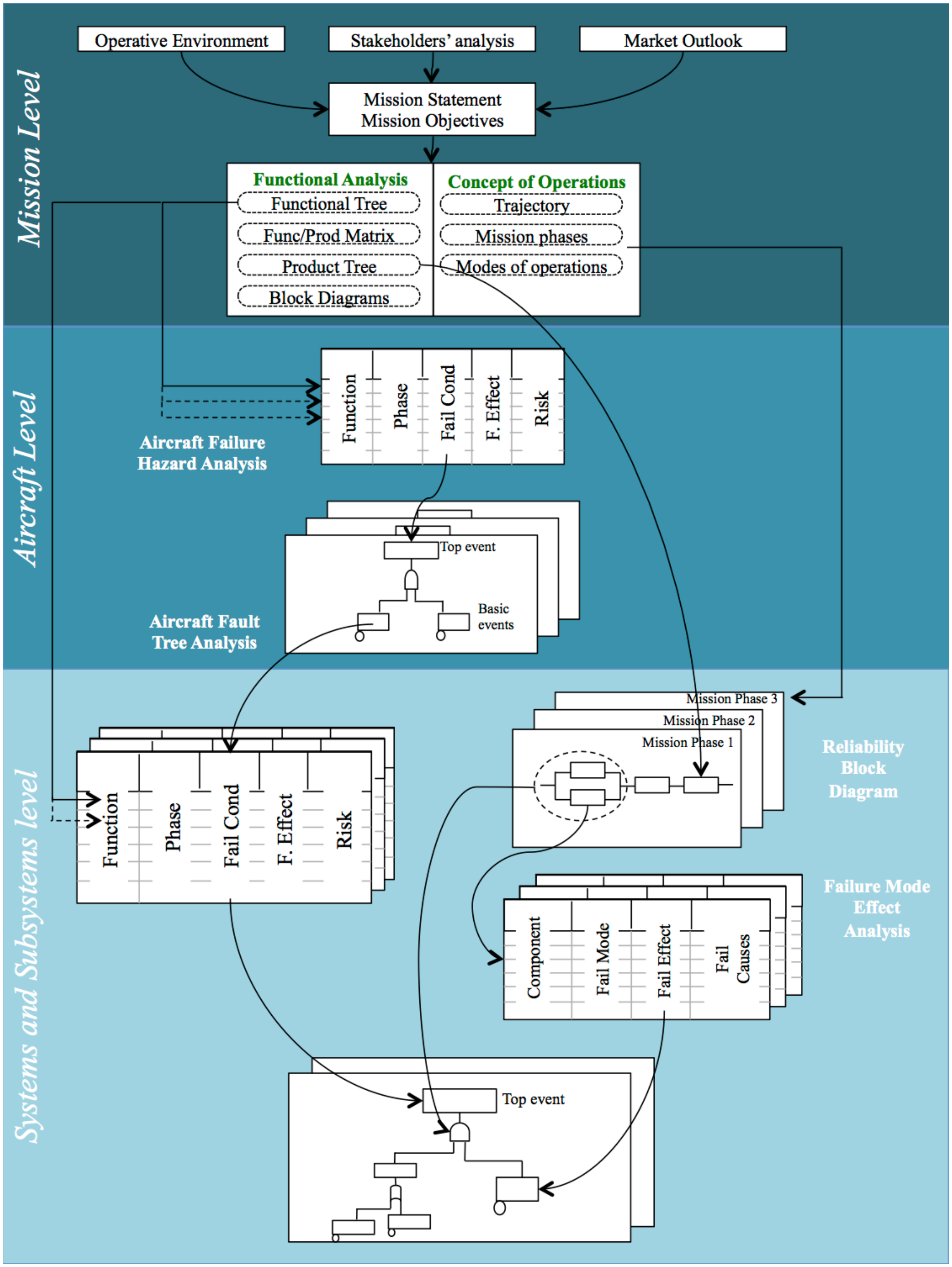
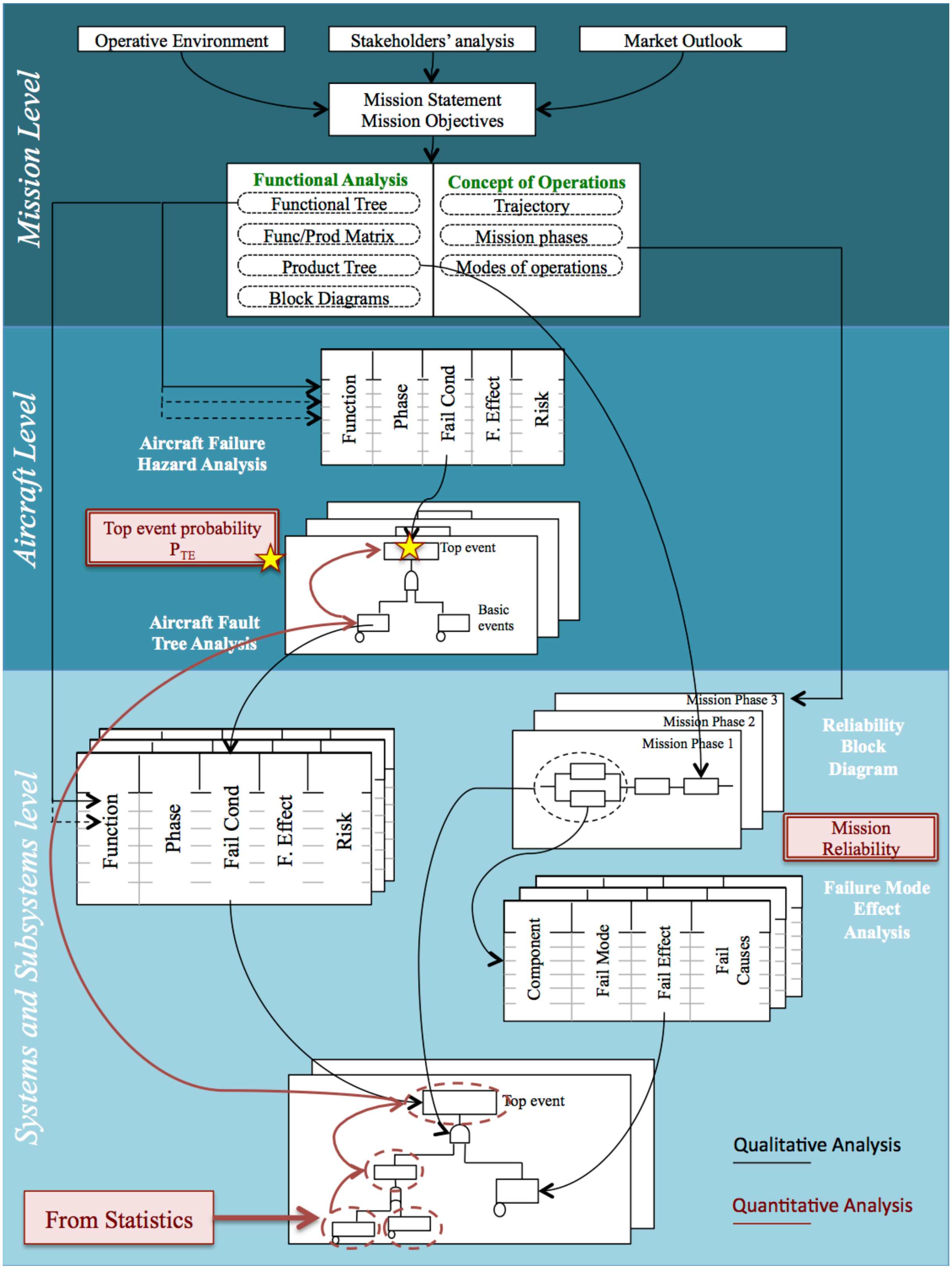


Figure 4 Scheme of the Methodology, the quantitative approach



Case Study: estimation of the reliability characteristics of a complex propulsion system aimed at supporting VTOL capabilities

Reference mission and vehicle description

The paper suggests a methodology for a preliminary safety assessment with a special focus on the analysis of a crucial propulsion system. In order to contextualize the peculiar type of application selected, the mission statement is here reported.

"*The mission shall allow regular flight services to enable 4 flight participants at a time to reach 100 km to experience a period of microgravity and an amazing view of the Earth. The spacecraft shall perform a vertical take-off from a sea-based or land-based platform and a vertical landing on the same site. Moreover, the additional capability to perform an un-crewed mission shall be considered*".

This mission statement refers to a pre-feasibility study granted to an Italian small enterprise (ALTEC S.p.A) and carried out involving Politecnico di Torino, which the author belongs to, and Thales Alenia Space Italy (in particular a team of experts of the Turin site) by a private Malaysian Stakeholder. The results of mission analysis and prefeasibility study have been already presented in (Viola et al., 2015) and (Fusaro et al., 2016), where further details can be found.

Among the primary objectives, it is crystal clear that the stakeholders' expectations of having a suborbital vehicle able to vertically take-off and landing will severely affect the vehicle layout and on-board systems integration, as well as the location and the layout of the spaceport (Santoro et al., 2015) and (De Vita et al., 2015) (Figure 5).

The mission statement clearly identifies VTOL capability as one on the major stakeholders needs. Moreover, considering the high impact of this requirement on the vehicle layout and mission strategy, it is important to take it into account since the beginning of the design process but also to properly select the propulsion system strategy and architecture. In addition, in order to comply with Malaysian regulations, the mission shall not envisage a rocket powered lift-off but only conventional air-breathing engines could be exploited up to a certain altitude.

The very preliminary trade-off studies have been carried out and both the processes, selection criteria and results related to this reference case study are reported in (Fusaro et al., 2016). Among hundreds of alternatives, a winged body configuration has been selected (Figure 6) as the most suitable to carry non-trained passengers guaranteeing a proper level of comfort and safety during the entire flight envelope. Indeed, this configuration is the most suitable for a single stage-to-orbit, enabling passengers to free-float during microgravity experience and to integrate a detachable cabin escape system.

Figure 5 Reference Mission Trajectory

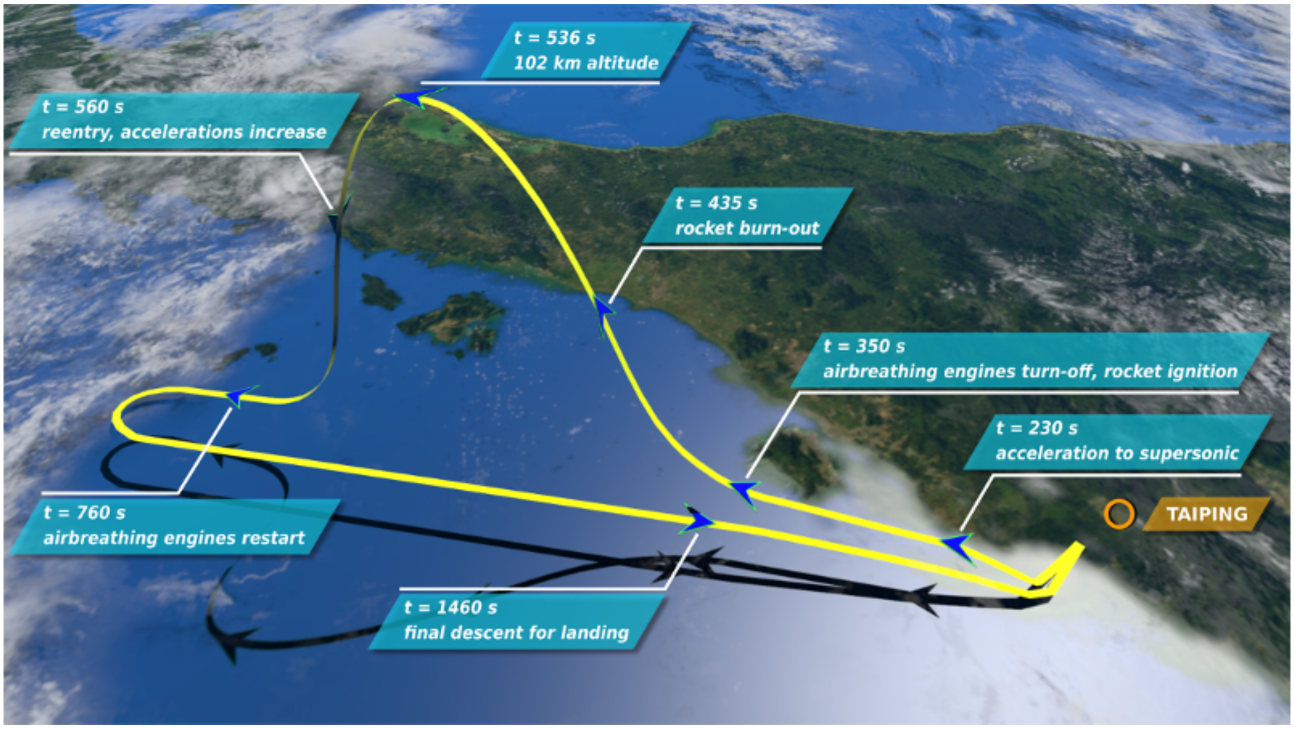
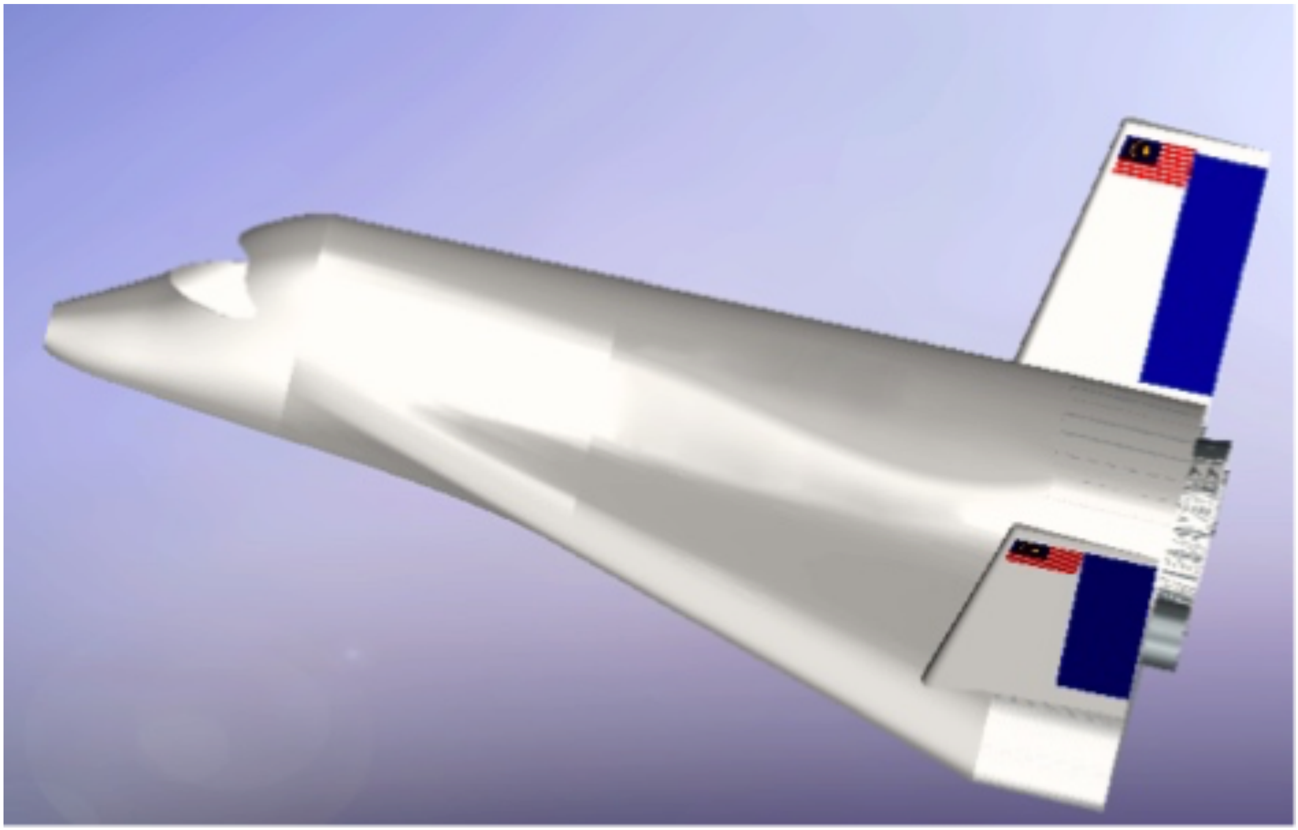

t = 536 s
102 km altitude
t = 560 s
reentry, accelerations increase
t = 435 s
rocket burn-out
t = 350 s
airbreathing engines turn-off, rocket ignition
t = 230 s
acceleration to supersonic
TAIPING
t = 760 s
airbreathing engines restart
t = 1460 s
final descent for landing

Figure 6 Reference vehicle layout



Trade-off among possible propulsion systems architectures for assisting VTOL

The need for a vehicle able to comply with VTOL requirements is strictly related to economic feasibility studies. On the one hand, the VTOL capability guarantees several advantages, as, for example, the low impact on the on-ground infrastructures. Indeed, in order to make such a spaceplane operative, long runways are not required anymore and a smaller confined area could be sufficient. In particular, this advantage is optimized in the case of a non-tail-sitting take-off since a simple pad or clear area could be sufficient to perform a take-off and no launch tower should be required. Consequently, a higher number of locations would be theoretically able to host the vehicle. Unfortunately, this is not completely applicable to this kind of vehicles, especially if they use rocket technology that implies to store also dangerous explosive propellant on-board. The infrastructure location should be properly selected depending on environmental, population and logistic constraints.

In opposition to the higher flexibility guaranteed by VTOL vehicles, a very high level of complexity, postponed time-to-market and additional costs should be properly taken into account.

In the following subsection, different ways to ensure VTOL capabilities are reported and two major alternatives are in-depth analysed. It is worth noting that the research group of Politecnico di Torino, which the authors belong to, had already dealt with VTOL capabilities, also for different kind of innovative vehicles (Chiesa et al., 2014)

Non-Tail-Sitting Strategy

As it has been mentioned in the previous subsection, the VTOL strategy has always been considered to be the most desirable feature from operational standpoints, but due to the high level of complexity of the solution, the need of containing weight to be competitive and of maintaining the level of performances of the Horizontal Take Off and Landing (HOTOL) vehicles, this traduces in a real nightmare for the designers.

In particular, in the next subsection two different propulsion systems architectures have been analysed in order to show three main existing strategies that could be adopted for the proposed case study. The examples are taken from the military field where the need of taking off and landing in unprepared and narrow areas is frequently considered to be the added value of the vehicle. It is worth to notice that these descriptions do not pretend to be propulsion system technical dissertation, being instead conceived to explain the reader which components they comprehend, which are the main topic related to their integration with the other aircraft subsystems and how the overall system works. Due to the aim of this paper, the feasibility of these options for a hypersonic spaceplane is also discussed.

Steerable nozzles and lift engines (Yak 38–like architecture)

The first propulsion system architecture here proposed is the one exploited by the Russian Yakovlev Yak 38, which is based on two separate subsystems. Indeed, the main engine, entirely contained within the fuselage, has two steerable nozzles able to direct downward the hot gasses during the take-off and landing phases. As it possible to notice in Figure 7, due to the distance of the nozzles from the Centre of Gravity (CG) of the overall configuration at take-off, at least an additional thrust point should be added in the forepart of the fuselage. To solve this problem two secondary engines, called lift-engines, were added in order to be exploited only during take-off and landing phases. Considering the studies performed by Raymer (2006) the so-called "lift plus lift/cruise" (L+L/C) approach may be the best in class for supersonic VTOL aircraft. Indeed, this solution proposes to use the lift of the main engine plus the extra lift of the lift engines, deleting the need for a compromise with the "normal" mission, because the main engine is always the same (apart from the steerable nozzles). As it is clearly sketched in Figure 7, these engines receive air from the inlets placed in the upper part of the fuselage and they directly discharge the hot gasses downward. Please notice that four small doors have been designed to cover both inlets and outlets in order to avoid the structural discontinuities and the undesired air-flow in the intakes during the other mission phases. Moreover, the presence of these two lift engines implies the creation of two split lateral intakes to feed the main engine. In addition to the main thrust produced by hot gasses, a proper distribution system has been envisaged to enhance the stability of the configuration. It is worth to notice that this L+L/C configuration has a safety related issue: in case a lift engine should fail during vertical flight or in transition, the aircraft may lose its stability immediately, with a fast pitch down movement. This is the reason why the Yak 38 had been designed with an ejection system to be exploited also at take-off. To increase the stability of this configuration, rearward vectoring should be hypothesized also for the two lift engines: in this case, they could also be used to assist a return base mission if a cruise engine would fail.

It is clear that this kind of solution avoids the duplication of the main propulsion system to fulfil the take-off requirement in terms of thrust, allowing mass and fuel savings and maintaining a compact configuration. However, the presence of the two lift engines creates a non-negligible interruption of the airframe and this could be hardly accepted for spaceplanes due to their very high speed and critical operative environment. On the other hand, the exploitation of steerable nozzles and devices for enhancing stability will be taken into account for the case study.

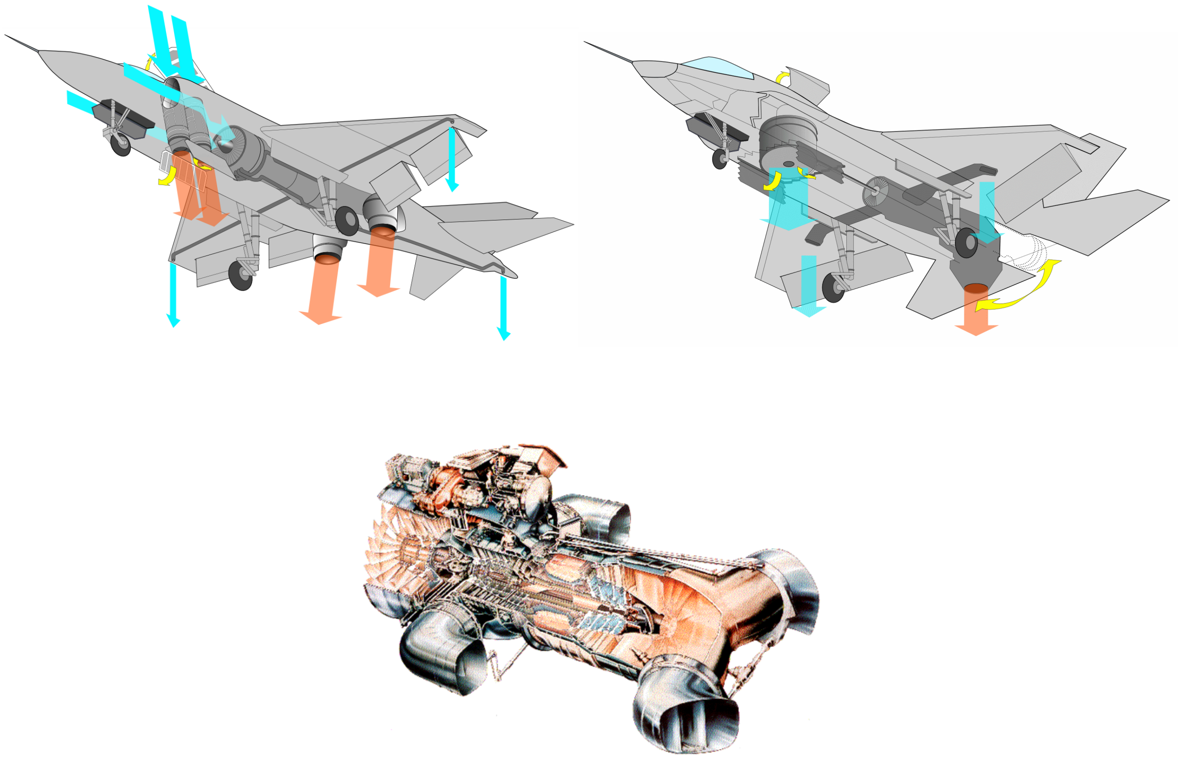
Lift fan and steerable nozzle (F-35–like architecture)

The second analysed solution is the one adopted on-board the F-35B and it is known as "Shaft-Driven Lift Fan" (SDLF). From the balance of forces standpoint, also this configuration can be basically considered as a L+L/C, but the lift-engines are here replaced by a fan directly connected to main engine shaft. The overall configuration consists of a jet engine compressor mechanically spun by a driveshaft that is spun by an extra turbine. Of course, during cruise, a clutch shall allow to disconnect the fan from the main engine, allowing the unloaded turbine to spin freely. When the fan is engaged, the mechanical power is extracted from the engine exhaust and it is applied to a larger amount of air allowing a thrust augmentation factor that can reach 1.4 times (Raymer, 2006). With respect to the configuration proposed in the previous subsection, SDLF inherits the main benefits avoiding the higher temperatures of separated lift engines and the related maintenance activities. On the other side, an increase in complexity should be taken into account considering the additional components of the architecture, such as shaft, clutch, gearbox and an extra-turbine.

Harrier-like

Dealing with VTOL, it is not possible to forget the AV-8 Harrier aircraft. It uses the high-bypass ratio engine called Pegasus in which the fan air and the core air are separately vectored through "elbow" nozzles. It is clear that such a solution simplifies transition and enhance the manoeuvrability of the aircraft, especially during low speed manoeuvres. The most important drawback of this system is the fact that there is a single engine that should be able to generate the required lift in each single mission phases. This is the so-called "matching problem". For stability reasons, the engine should be placed pretty closed to the CG and this can imply an increase of the cross-sectional area in coincidence with the wing fuselage connection, increasing the supersonic wave drag.

Figure 7 VTOL major configurations (Yak-38 and F35 B) and Pegasus, the Harrier AV-8 Engine



Case Study: Reference System Architecture

The present case study refers to the Mission Statement proposed in the previous section. As it is clearly sketched in Figure 6, the need of fulfilling the very peculiar mission objectives and the constrains about the minimum altitude required for the rockets ignition forced the designers to conceive a very complex propulsion system consisting of two air-breathing engines and related subsystems and a liquid rocket engine. For the sake of clarity, Figure 5 and Table 1 have been added in the previous section in order to synthetize the mission main phases and the way in which the propulsion system has been envisage to work in the different phases. Figure 8 summarizes the main components of two main subsystems. As far as the air-breathing is concerned, the system is composed of two main engines, each of which should be able to guarantee the thrust required to overcome the Maximum Take-Off Weight (MTOW) enabling the VTOL capability. Due to the shape of the vehicle in which they should be accommodated and the presence of the other subsystems, the two engines were placed on the two sides of the rocket motor. They are equipped with two main steerable nozzles but there is also the possibility of conveying the hot gasses in a distribution system to feed the four secondary steerable and retractable nozzles installed in the lower flat surface of the vehicle. Two main fuel tank located in the wing available room, can feed both the two engines through a cross-feed valve. At the same time, for safety reasons, another cross-valve is required in the hot gasses distribution lines in order to allow the left-hand engine to provide hot-gasses to the right-hand nozzles and vice versa, in case of One Engine Inoperative (OEI) condition. In addition, component like pumps or valves should be obviously taken into account for the safety assessment.

The approach proposed above has been applied to identify the top-event probability of the so complex propulsion system able to guarantee VTOL capabilities. Some example of the RBD and FT are reported in Figure 9 and Figure 10 respectively.

Figure 8 Spaceplane cutaway

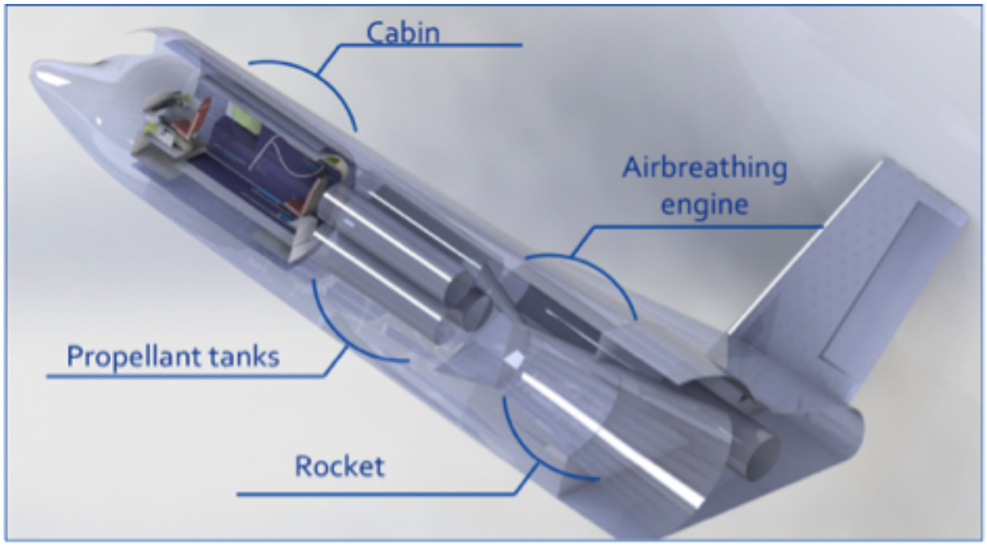


Table 1 Mission phases and propulsion system operative mode

Mission Phases	Operative Mode	Comments
Take-off and transition	Airbreathing engines: ON – VTOL Rocket motor: ON	During take-off and landing the air-breathing engines are exploited in the so called ON-VTOL mode. This means that they are active but the hot gasses are diverted into the downward nozzles (Nozzles 3, 4, 5, 6 of Figure 9). Once that a certain altitude is reached, the nozzles are steered rearward in order to create the required horizontal component of the thrust vector.
Climb 1st segment	Airbreathing engines: ON – NOMINAL Rocket motor: OFF	Once the right attitude is reached, the air-breathing engines can shift to their nominal operative mode in which only Nozzle 1 and 2 of Figure 9 are used. In order to prevent undesired airflows from external, the four steerable nozzles are retracted and four doors cover the holes, avoiding structural discontinuities.
Climb 2nd segment	Airbreathing engines: OFF Rocket motor: ON	At the ceiling altitude (or even below if planned) the air-breathings should be switched off and the rocket motor is ignited.
Parabolic segment	Airbreathing engines: OFF Rocket motor: OFF	After the completion of the liquid propellant, the rocket motor burns out and the aircraft continues its motion performing a typical ballistic parabolic trajectory. This is the phase in which microgravity could be experimented.

Re-entry	Airbreathing engines: OFF Rocket motor: OFF	After the microgravity period, the air-breathing engines cannot be re-started up to reach the ceiling altitude. Up to that altitude, the aircraft should be controlled and manoeuvred exploiting secondary propulsion systems (small thrusters)
Approach and landing	Airbreathing engines: ON - VTOL Rocket motor: OFF	During the approach and final landing phase, the air-breathing engines could be used again, in both nominal and VTOL modes.

Figure 9 Propulsive system architecture (air-breathing subsystem)

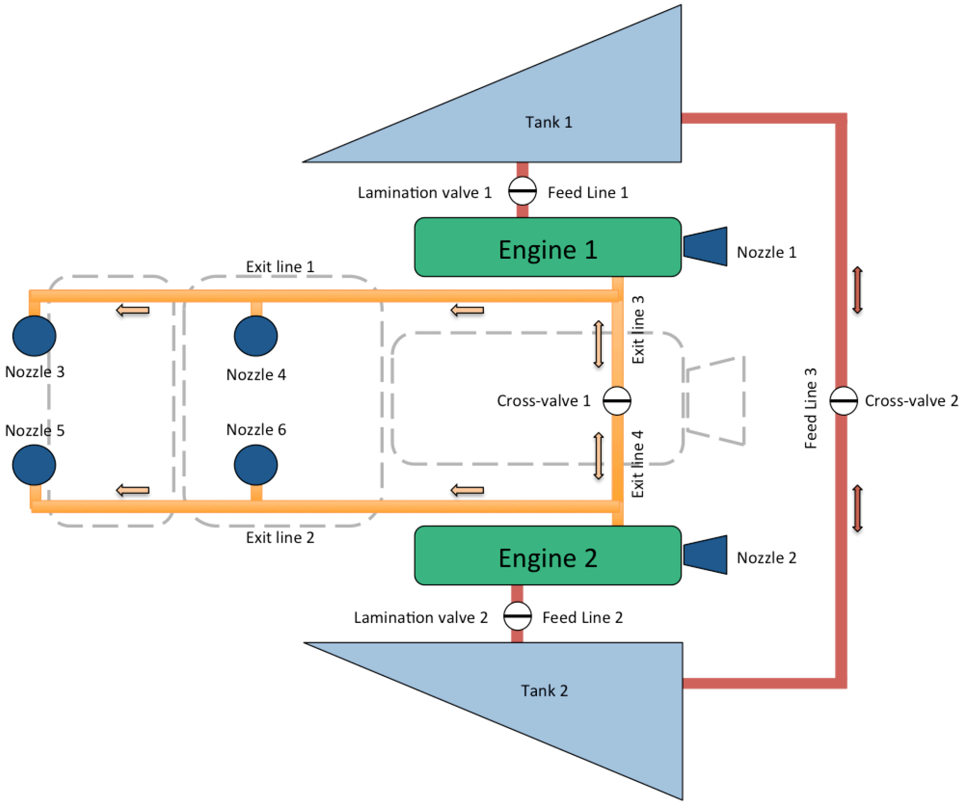


Figure 10 Propulsive system architecture (rocket motor subsystem)

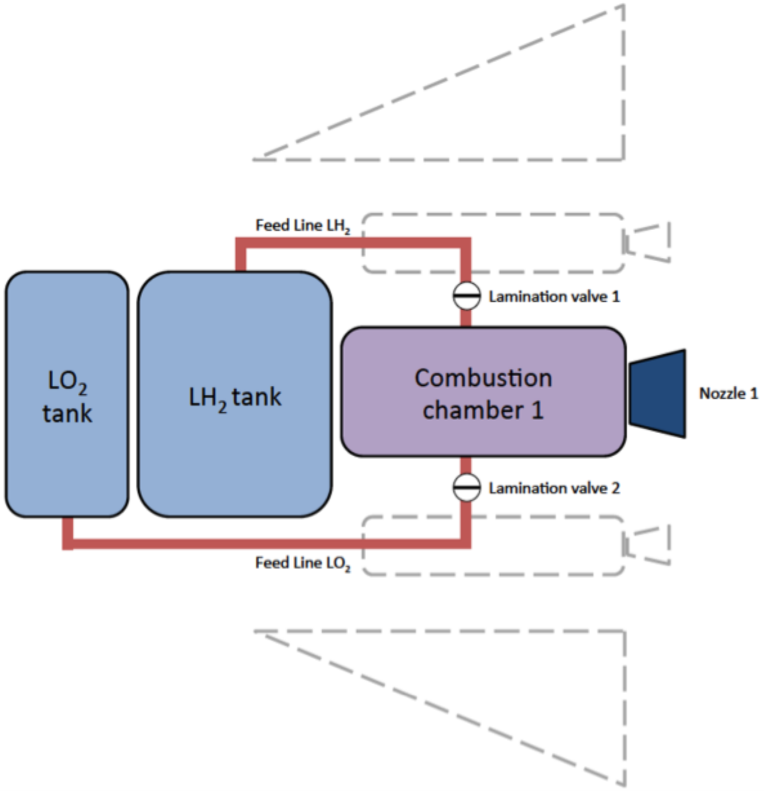


Figure 11 Reliability Block Diagram for the air-breathing engines subsystem in take-off operative mode

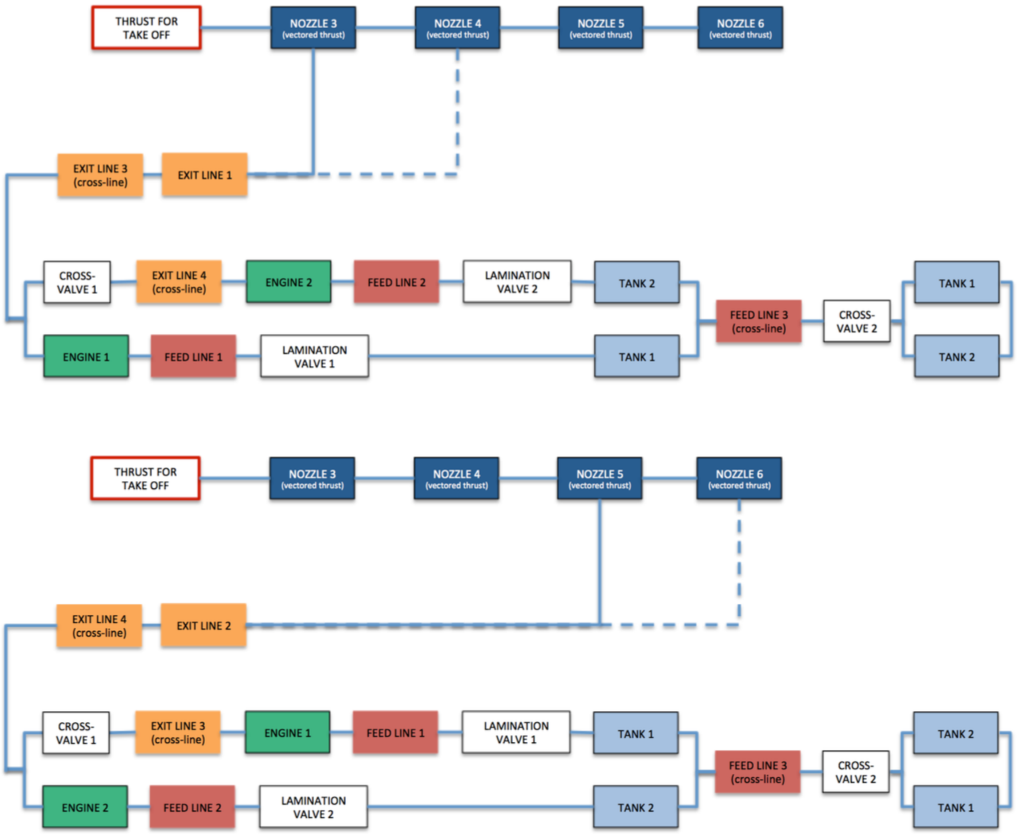
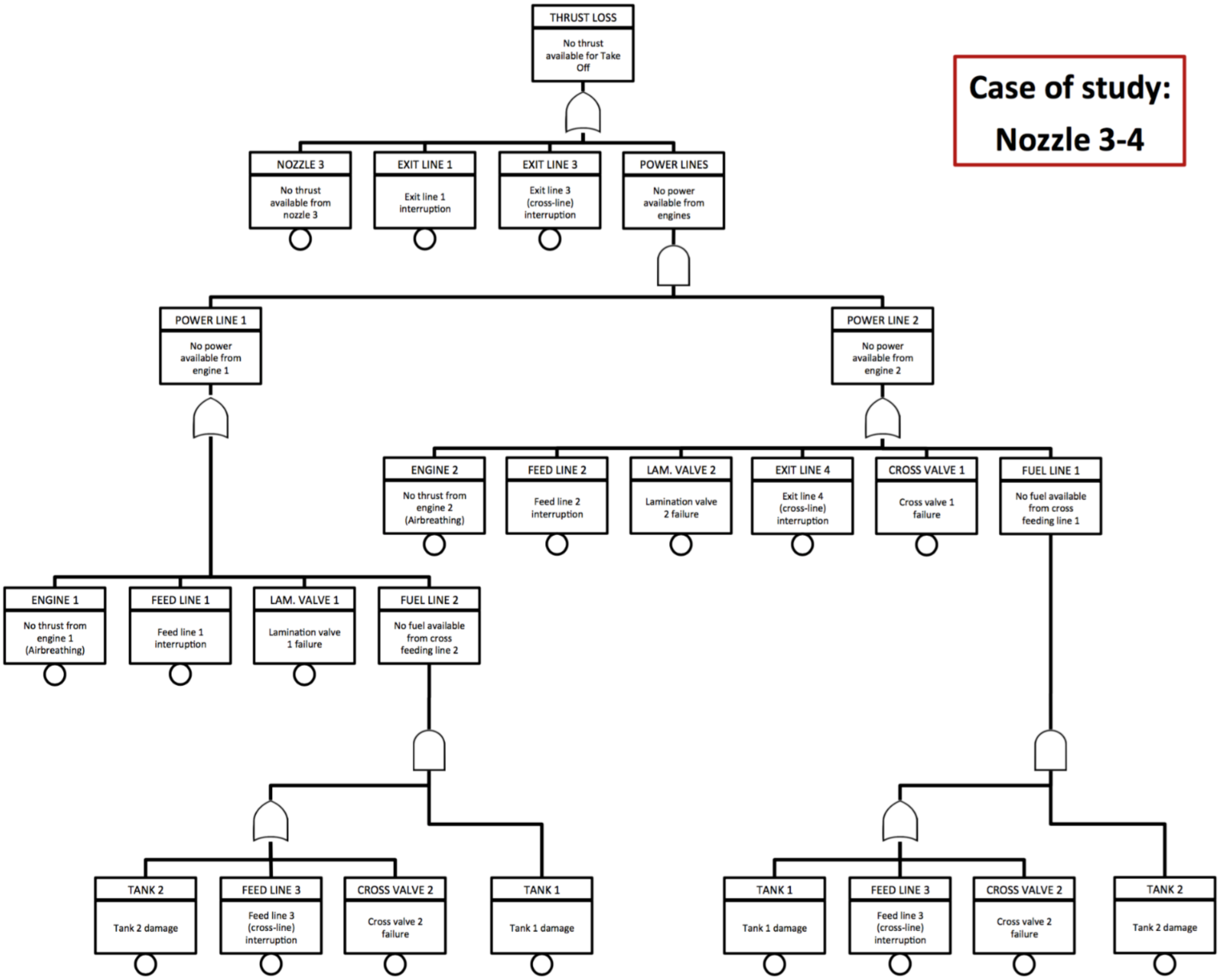


Figure 12 One of the Fault Trees for the air-breathing subsystem


THRUST LOSS
No thrust available for Take Off
Case of study:
Nozzle 3-4
NOZZLE 3
No thrust available from nozzle 3
EXIT LINE 1
Exit line 1 interruption
EXIT LINE 3
Exit line 3 (cross-line) interruption
POWER LINES
No power available from engines
POWER LINE 1
No power available from engine 1
POWER LINE 2
No power available from engine 2
ENGINE 2
No thrust from engine 2 (Airbreathing)
FEED LINE 2
Feed line 2 interruption
LAM. VALVE 2
Lamination valve 2 failure
EXIT LINE 4
Exit line 4 (cross-line) interruption
CROSS VALVE 1
Cross valve 1 failure
FUEL LINE 1
No fuel available from cross feeding line 1
ENGINE 1
No thrust from engine 1 (Airbreathing)
FEED LINE 1
Feed line 1 interruption
LAM. VALVE 1
Lamination valve 1 failure
FUEL LINE 2
No fuel available from cross feeding line 2
TANK 2
Tank 2 damage
FEED LINE 3
Feed line 3 (cross-line) interruption
CROSS VALVE 2
Cross valve 2 failure
TANK 1
Tank 1 damage
TANK 1
Tank 1 damage
FEED LINE 3
Feed line 3 (cross-line) interruption
CROSS VALVE 2
Cross valve 2 failure
TANK 2
Tank 2 damage

It is clear that for each foreseen operative mode of the propulsion system, a different RBD and different FTA have been sketched. Here there is only an example of these diagrams derived for the most critical phases of the mission: the take-off. As it is easily noticeable, the analysis is carried out considering each single steerable nozzle placed in the bottom of the vehicle but no information is required for the two main nozzles since the overall exhaust mass flow is diverted in the bottom placed ones. Moreover, additional complexity of the scheme is added by the fact that different kinds of cross-feed have been envisaged in order to enhance the level of safety. As it has been explained in the Section Safety Assessment Methodology, each of the trees can be traduced in an equation that can be solved starting from the failure rates of the single components. Data coming from statistics have been selected in Military database. This could be one of the main reasons for which the expected propulsive system failure rate (0.009118 failures/1000h) is closer to a fighter than to a civil aircraft (Table 2) (Chiesa, 2010). Of course, this result is acceptable because of the high complexity of the system.

Table 2 Reference Failure rates

Propulsive system failures rates [failures/1000 h]		
Fighter	Military transportation	Civil transportation
0.01809	0.00226	0.0000263

The obtained results for the propulsion system are in line with the expectations, as for for this kind of technology, it appears to be realistic to set safety and reliability requirements with ranges between fighter and civil transportation aircraft. However, these results have been obtained considering failure rates of existing components. Within an integrated design process, these results highlight the fact that additional work should be carried out in order to increase the reliability of the basic components or of the entire systems, modifying its overall architecture. This would be necessary in case the stakeholders or the regulatory framework would superimpose a more restrictive requirement, to assimilate suborbital vehicle to civil aircraft.

Eventually, it is necessary to underline the fact that the case-study here reported, only represents an example of application of the proposed methodology, limited at system level. In future works, the application will be extended at other systems, allowing the possibility of presenting a complete case-study with the ambitious goal of deriving failure rate evaluation at aircraft level.

Conclusion

This paper presents a methodology to carry out a safety and reliability assessment suitable for application to very complex and innovative systems like the trans-atmospheric transportation systems. Unlike existing methodology, this process exploits statistical correlations only at component level, thus overcoming the problem related to lack of statistical data at system-level. Starting from the statistical data at component level, it is possible to assess reliability and safety at aircraft level thanks to the combination of typical safety assessment tools, like Functional Hazard Analysis, Failure Mode and Effect Analysis, Reliability Block Diagram and Fault Tree Analysis on the basis of previously carried out analyses such as the functional analysis and the concept of operations. It is therefore fundamental to have first a qualitative phase followed by a quantitative because the logical decomposition that comes out from the qualitative approach paves the way of the numerical evaluations that, starting from the bottom, traces back to the top. Moreover, the methodology is fully integrated within the conceptual design phase because it makes use of some basics tools of a systems engineering approach. A massive application of this approach to different case-studies will eventually allow to create a database for the generation and the update of semi-empirical models focused on high-level estimations of Reliability, Availability, Maintainability and Safety (RAMS) characteristics.

Considering the peculiar application presented in this paper, the methodology reveals to be also suitable for application at systems level. In particular, the application to the reference case-study strongly confirms the usefulness of this methodology to overcome the problem of lack of data that in this and many other cases affect the accuracy of assessment of RAMS characteristics at system level, (considering its embedded disrupting technology or high level of innovation).

Further Work

In the near future, the authors will extend the application of the methodology presented in this paper to a complete case-study, carrying out a safety and reliability assessment for the different systems, with the aim of deriving the failure rates at aircraft level. In this way, it will be possible to update the values of some parametric coefficients and to create new set of predictive equations to be used since the very beginning of the design process.

Moreover, the author will integrate the methodology in a Model Based Systems Engineering environment (Fusaro et al., 2016), creating a proper tool-chain that will enhance traceability of the safety requirements and of all the safety-related design choices. A software-based approach will provide several benefits to the methodology, facilitating, in particular, the replicability, shortening the time and costs.

References

Chiesa, S. (2010), Affidabilità, sicurezza e manutenzione nel progetto dei sistemi, CLUT, Torino.

Chiesa, S., Corpino, S., Fioriti, M., Rougier, A., Viola, N. (2013). Zonal safety analysis in aircraft conceptual design: Application to SAvE aircraft. In Proceedings of the Institution of Mechanical Engineers, Part G: Journal of Aerospace Engineering, 227 (4), pp. 714-733. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84877808329&doi=10.1177%2f0954410012441430&partnerID=40&md5=bd1d474acf73e5b5ed2641ae9e80aac1 DOI: 10.1177/0954410012441430

Chiesa, S., Aleina, S.C., Di Meo, G.A., Fusaro, R., Viola, N.(2014) Autonomous take-off and landing for unmanned aircraft system: Risk and safety analysis. 29th Congress of the International Council of the Aeronautical Sciences, ICAS 2014. Saint Petersburg (Russia) . https://www.scopus.com/inward/record.uri?eid=2-s2.0-84910662856&partnerID=40&md5=161ee6bdb52c984cff713ea3f934e839

Cresto Aleina, S., Viola, N., Fusaro, R., Saccoccia, G., & Longo, J. (2016). Technology Roadmaps Preparation For European Hypersonic And Re-Entry Space Transportation Systems, Proceedings of the International Astronautical Congress, IAC 2016 - IAC 2016, Guadalajara (Mexico).

De Vita F., Viola N., Fusaro R. and Santoro F., (2015). “Assessment of Hypersonic Flights Operation Scenarios: analysis of launch and reentry trajectories, and derived top-level vehicle system and support infrastructure concepts and requirements” In 20th AIAA International Space Planes and Hypersonic Systems and Technologies Conference proceedings, AIAA (American Institute of Aeronautics & Astronautics), Reston (VA), pp 35-40. doi: 10.2514/6.2015-3540

Fusaro, R., Ferretto, D., Viola, N. (2016). Model-Based Object-Oriented systems engineering methodology for the conceptual design of a hypersonic transportation system. ISSE 2016 - 2016 International Symposium on Systems Engineering - Proceedings Papers, art. no. 7753175. Edinburgh (Great Britain). https://www.scopus.com/inward/record.uri?eid=2-s2.0-

85006483426&doi=10.1109%2fSysEng.2016.7753175&partnerID=40&md5=1b562b2b430f9afcf17384b6eff72561 DOI: 10.1109/SysEng.2016.7753175

Fusaro, R., Viola, N., , Fenoglio F., Santoro, F., (2016) “Conceptual design of a crewed reusable space transportation system aimed at parabolic flights: stakeholder analysis, mission concept selection and spacecraft architecture definition”, CEAS Space Journal 131, doi :10.1007/s12567-016-0131-7.

Musgrave, Gary E., Axel Larsen, and Tommaso Sgobba (2009). Safety design for space systems. Butterworth-Heinemann.

NASA (2014), NASA System Safety Handbook, Volume 1: System Safety Framework and Concepts for Implementation, NASA Headquarters, Washington D.C.

Raymer, D. P. (2012), Aircraft Design: A Conceptual Approach (AIAA Education Series), AIAA (American Institute of Aeronautics & Astronautics), New York.

SAE (1996), ARP 4761, Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment, Warrendale (PA).

Santoro, F., Bellomo, A., Del Bianco, A., Vittori, R., Viola, N., De Vita, F.(2014). A case study for spacegate point-to-point transportation: Evaluation of a reference end-to-end mission operations and assessment of the associated safety aspects. Proceedings of the International Astronautical Congress 2014, IAC 2014, 11, pp. 8140-8152 Toronto (Canada). https://www.scopus.com/inward/record.uri?eid=2-s2.0-84938152783&partnerID=40&md5=85fea3269015f9172bb88fd5d45a0b7d

Santoro F., Del Bianco A., Bellomo A., Martucci di Scarfizzi, G., Fenoglio, F., Viola N., Fusaro R., De Vita F., Zakaria Ridzuan N. (2015), “Approaches to development of commercial spaceport and associated ground segment driven by specific spaceplane vehicle and mission operation requirements”, IAC 2015 Conference, 12-16 October 2015, Jerusalem (Israel).

Stamatelatos, Michael, et al. (2011). Probabilistic risk assessment procedures guide for NASA managers and practitioners.

Tauri Group, Vehicles, Suborbital Reusable (2012), A 10-Year Forecast of Market Demand, The Tauri Group under contract with the Federal Aviation Administration and Space Florida, Walkerline (VA).

Viola N., Fusaro R., De Vita F., Del Bianco A., Fenoglio F., Massobrio F., Santoro F. (2015). “Conceptual design and operations of a crewed reusable space transportation system”, paper presented at IAC 2015 Conference, 12-16 October 2015, Jerusalem (Israel).

Viscio, M.A., Viola, N., Fusaro, R., Basso, V., Marello, M., Pasquinelli, M., Santoro, F. (2014). On-orbit technology demonstration and validation: Methods and tools for mission, system and operations design. Proceedings of the International Astronautical Congress 2014, IAC 2014, 9, pp. 6811-6825. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84938230837&partnerID=40&md5=a4599c9d29622d067707a5f344c19e17

Viscio, M.A., Viola, N., Fusaro, R., Basso, V.(2015). Methodology for requirements definition of complex space missions and systems. Acta Astronautica, 114, pp. 79-92. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84929380320&doi=10.1016%2fj.actaastro.2015.04.018&partnerID=40&md5=69ec14fdff93546032e85bdb1161ea68. DOI: 10.1016/j.actaastro.2015.04.018