Università degli Studi di Salerno

Dipartimento di Studi e Ricerche Aziendali

Corso di dottorato di Ricerca in "SCIENZE E TECNOLOGIE DELL'INFORMAZIONE, DEI SISTEMI COMPLESSI E DELL'AMBIENTE"

Ciclo XII

Tesi di dottorato in:

A FRAMEWORK TO ASSESS RISKS AND DERIVE REQUIREMENTS FOR A COMPLEX SYSTEM

*Tu*tor: Professoressa Giuliana Vitiello

Coordinatore: Professore Roberto Scarpa

Dottorando: Angela Vozella

Anno Accademico 2014

A FRAMEWORK TO ASSESS RISKS AND DERIVE REQUIREMENTS FOR A COMPLEX SYSTEM

Angela Vozella

Doctor of Philosophy

SCIENZE E TECNOLOGIE DELL'INFORMAZIONE, DEI SISTEMI COMPLESSI E DELL'AMBIENTE

Università degli Studi di Salerno
Dipartimento di Scienze Matematiche Fisiche e Naturali

2013

Approved by: Professoressa Giuliana Vitiello

AKNOWLEDGEMENT

TO MY PARENTS CARLO & CARLA

ABSTRACT

This thesis provides an innovative framework, based on the risk assessment methodology, to support the design of a pioneering complex system, strongly ICT based, whose failures could threaten people, environment and society thus resulting safety critical.
Beyond the technical risks, the study identifies possible concerns of the society raised by the use of new technology (complementary measures), which have to be managed to guarantee a sustainable adoption.
The framework is applied to a case study in the aviation domain.

TABLE OF CONTENTS

LIST OF FIGURES/TABLES

ACRONYMS

A/C aircraft.

CO2 carbon dioxide

COMM Communication

D-GPS Differential Global Positioning System

EASA European Aviation Safety Agency

ENAC Ente Nazionale per l'Aviazione Civile

FMEA Failure Mode Effect Analysis

FMECA Failure Mode Effect Criticality Analysis

GABRIEL Integrated Ground and on-Board system for Support of the Aircraft SafeTake-off and Lan

GBS Ground Based System

HW/SW Hardware/Software

ICT Information & Communication Technology

MAGLEV magnetic levitation

NOx nitrogen oxides

SO2 sulphur dioxide

S/s subsystems

Sw Software

Tol take-off and landing

1 SCOPE

The Global challenges defined at European level - Environment and Safety (Safety and Security), Competitiveness and Sustainable Development, Energy Availability - provide a number of constraints to be respected and problems to solve. Osmosis between seemingly unrelated disciplines bud many of the solutions to these problems. The approach requires the ability to "use the system" tools and skills from different disciplines and to apply them in a synergistic way (holistic approach).

Each domain has to address the previous challenges guaranteeing sustainable results and traditional models of system engineering need to be extended to handle today's risks.

The future air transport system will be confronted with these new challenges too: it must be safer, greener and more effective than the current system (Horizon 2020, Flightpath 2050 [1,2]). All these have influences on aircraft take-off and landing (TOL) systems and generate needs in the development of radically new technologies, methods and structural solutions for TOL process realization.

The EU supported FP7 project GABRIEL [3], tends to develop a radically new, so called "out-of-the-box" technology to launch and recover aircraft with ground-based magnetic levitation technology[4]. This unique solution is envisioned to reduce aircraft fuel consumption since aircraft weight could be reduced as possibly no undercarriage might be needed, less fuel would be necessary to carry on-board and engines could be smaller as less thrust could be required. Using ground power could also reduce CO2 and NOx emissions at airports whilst noise levels could be substantially reduced since only airframe (and engine with reduced power) noise will be produced during take-off. Airport capacity could be also increased by introducing multiple launch and recovery ramps thus alleviating the problem of limited runway capacity in Europe. **The author was involved in this project performing a large contribution to the safety aspects.**

Most common accident causality models assume that accidents are caused by component failures and making them highly reliable will prevent accidents. While this assumption is right for systems of the past, it is no longer true for new complex innovative systems. Indeed due to critical infrastructure interdependency, many situations and emerging hazards can lead to undesired events which are not easy to forecast. Another difficulty during the design for radically innovative systems is the lack of historical data and, for specific situations, even the lack of standard rules and prescriptions to base the analysis on.

The first part of this thesis provides an innovative framework, based on the risk assessment methodology, to support the design of a pioneering complex system, strongly ICT based, whose failures could threaten people, environment and society (e.g. safety critical system or infrastructure).

Beyond the technical risks, the study identifies possible societal concerns raised by the use of a new technology which have to be managed to guarantee a sustainable adoption. Among these topics:

- liability in case of accident (incl. issues like enforcement, impact of automation) and insurance;
- privacy, data protection, security;

- public acceptance of new technology.

In the second part of the Thesis, the derived framework is applied to a specific case study: a radically innovative system for aircraft take-off and landing based on maglev (magnetic levitation) technology. The application of the framework supports the systems requirements' definition phase.

2 INTRODUCTION

2.1 Rationale and Structure of the thesis

Focus of this thesis is the design and the application of a theoretical framework based on system engineering and system safety engineering, to support the design and development of a complex system, based on a new technology [27, 28, 29, 30, 31]. This system is safety critical as its failures can threaten human life and the environment.

Traditional risk analysis methods cannot satisfy the needs of modern complex systems for the following reasons:

- Lack of specific standard rules and prescriptions.
- Lack of historical data.
- High system complexity.
- Interdependence with the 'outside world' System of Systems .
- New specific mission phases and related functions, environmental issues.
- Composition issues. Complex systems tend to be composite and some parts of the systems can be changed. This dynamic nature affects the overall risk level of the system.
- Changing and emerging threats. Statistical data on which classical risk analysis is based is not constant in time. Some threats become more frequent than others after some time of operation of a system. Moreover, a system designed for protection against one set of threats may, after its release, find itself in a different, changed or unforeseen environment.
- System requirements evolution. Some security goals may vary over time and, thus, again cause change of risk level.

So an innovative approach has been defined and implemented driven by risks which can be extended to every new technology design to drive requirement definition in a sustainable perspective.

The thesis aims to enrich and expand the state-of-art and state-of-practice of reliable complex system design and deployment.

The derived framework is applied to a case study which represents a “worst case” in terms of complexity and safety issues. Thanks to its rigour, the framework can be applied to every complex system design, provided the necessary tailoring is performed.

In the remainder of this section, some basic concepts which represent the ingredients of the thesis are provided: Complex systems, the Environment, ICT and their relationships. Then, a description of the classic paradigm of risk follows.

Section 3 starts from the problems and limits of the traditional approaches to be overcome in order to guarantee sustainability for the new technology. As a first contribution to the state of the art the theory of the complementary measures is introduced. Complementary measures are to be managed at system design level and implemented within the system life cycle until its disposal.

In section 4 the new framework proposed is shown.

Sections 5 to 12 describe the case study and the application of the risk assessment framework to it. All the processes and the related analysis aimed to obtain the system requirements are presented in details. The references section contains all the mentioned documents and standards while in the Appendix A all the used terms and definitions are reported.

2.2 Progress beyond the state of the art

The result will be an assurance framework for the evaluation and communication of risks that will cope with the heterogeneous requirements of complex systems. A specific challenge is to support and mediate issues among all actors that have to contribute to collect requirements for the system components and communication of the results to authorities and other stakeholders, while increasingly updating the case when new information on vulnerabilities, threats and countermeasures becomes available.

This framework will consist of methods, processes, tools and scenarios to support the aggregation of risks and evidence about the reliability of complex systems to provide a sound and reviewable judgement that can be effectively communicated to different stakeholders.

When implemented, this framework will represent a genuine breakthrough that will allow service operators, authorities and other stakeholders to substantiate their claims about the trustworthiness of their systems, services and business models.

This approach moves along a well-defined path:

- starts from the preliminary system concept and functions,
- identifies among hazard classes the ones applicable to this case,
- allocates the hazards to the system components,
- performs functional failure mode criticality analysis,
- focuses on the most critical functions (according to the FMECA results),
- identifies those hazards which represent initiator events for those failure modes,
- characterizes the risk scenarios in order to identify requirements for those components involved in the scenario.

Another original element is the complementary measures management which is to be implemented from the design phase addressing plans and actions to promote public acceptance of a new technology evaluating the new concept in terms of perceived risks and benefits.

This study represents a first step towards a unified applicable methodology to ensure a reliable and safe process for designing complex critical systems guaranteeing their sustainability. All the disciplines linked to the "RAMSS[1]" (Reliability, Availability, Maintainability Safety and Security) activities, have been used together with failure mode effect analysis, fault tree analysis, impact analysis.

[1] Original term defined as the combination of RAMS with Security aspects

Furthermore, this framework supports business model design related to a new technology adoption as it has to address the cost benefit analysis.

2.3 Complex System concept

Complexity comes in many forms, and complexity is increasing in the systems we are building today. Examples include interactive complexity (related to interactions among system components), dynamic complexity (related to changes over time), decomposition complexity (where the structure decomposition is not consistent with the functional decomposition), and non-linear (where cause and effect are not related in a direct or obvious way).

Many systems or processes**,** both natural and man-defined, are characterized as complex systems. A complex system is a system in which the elements undergo continuous changes individually predictable, but which it is very difficult, to predict a future state in a deterministic manner. Ecosystems (even the simplest) are examples of complex systems, with relations between their components non-linear.

Another feature of complex non-linear systems is that they can produce an emergent behaviour, i.e. a complex behaviour not predictable and not deduced from the simple summation of the behaviour of the elements which compose the system.

To model a complex system, the most appropriate approach is holistic. The holistic approach is a scientific paradigm to study complex systems. It is not a scientific discipline in itself; rather it defines a philosophical approach that is considered in applying the principle of emergency, often using a multidisciplinary or interdisciplinary approach. This approach is in contrast with the traditional purely analytical, which proposes to interpret the complex systems by dividing them into their components and studying the properties separately.

From a mathematical point of view this means to distinguish between an approach in which the equations that model more disciplines are coupled, via an exchange of information or made available to the system trying to characterize the interactions between the disciplines, and the case in which a unified model characterizes the system as a whole.

2.4 The Environment

Environment is a complex system (nonlinear) consisting of the natural resources, infrastructures built by man, by human activities and their interactions.

Economic development, security and quality of life in industrialized countries depend on the operation, continuous and coordinated of critical infrastructure. These comprise the physical resources, services and information technology facilities, networks and infrastructure assets which, if disrupted or destroyed, would have a serious impact on the health, safety and economic well-being of citizens or the governance of the states.

2.5 Relationship between ICT and Environment

ICT, being applied across many disciplines, is in a position of privilege, and it is now an integral part of many organizational processes / industrial and public utility services.
ICT helps to identify data relevant for understanding the phenomena under study, scanned in real-time, process them, simulate and / or predict their behaviour over time, manage risk, to give decision support, store the data to build a base for historical purposes validation / prediction.
Therefore, critical infrastructure management needs monitoring operations over time and potential risks taking decisions to prevent accidents or restoring nominal behaviour.
Faced with the challenges of sustainable development, energy and the environment it is necessary to relate ICT and its effects (negative or positive) on the environment, deriving statistical data, distinguishing between ICT products and processes:

- Products / processes which bring improvements to the environment in terms of efficiency, dematerialisation (replacement of tools and actions with software processes), ability to control, modelling, management and dissemination;
- Products / processes which contribute to environmental degradation in terms of energy waste, increase in emissions due to increase in production, delivery of larger volumes of goods and / or passengers and operations, disposal without recycling.

Any trial to improve the overall impact requires collecting data and developing metrics, characteristic parameters and operating procedures.

The collection, storage and analysis of data made through ICT applications, allow us to study the phenomena themselves and derive useful information to achieve the objectives set by the global challenges mentioned above.

2.6 Classical Paradigm of risk management

Risks can be identified and evaluated based on an analysis of several factors as discussed below.

Definition of Danger (Hazard)

A hazard is a potential cause of a disaster. Not every hazard will result in a disaster, but every disaster will result from a hazardous condition, whether or not that condition was recognized in advance of the event.

There are potential dangers such hazards which are specific to a territory or due to natural factors or technological / malicious, it is necessary to identify the type and indicators.

Examples of natural hazard are weather and the respective indicators. Indicators of this hazard are the type and amount of rainfall in a given interval of time, and the water levels in rivers, lakes, artificial dams, etc.

Among the technological hazards there are: accidents of industrial plants and dispersion of pollutants, indicators of these hazard can be the concentration and type of pollutants at the source that generated them.

There are also hazards which are “conflict based” as civil war, terrorism, nuclear war, etc.

Usually security hazards include the followings: hi-jacking, terrorist attacks, stowaways and illegal immigrants, people carrying weapons/banned items in hand luggage, bombs, smuggling (weapons, money, drugs), aggressive or drunk people, assaults on staff, abandoned vehicles, cyber-attacks to system software.

Definition of Severity

The severity of the impact (on people and goods) of operations outside of the nominal (disturbance) or destruction of a particular infrastructure should, possibly, be assessed on the basis of the following elements:

- Public effect (number of people affected),
- Economic effect (significance of economic loss and / or degradation of products or services),
- Environmental consequences,
- Political consequences,
- Psychological consequences,
- Public health consequences.

So "the impact of a hazard" or severity is related to the severity of the hazard that, if triggered, may cause, and is therefore linked to the value of goods that suffer damage (Va = Value of assets at risk). In such a scale intuitively human life is in first place, then there's the environment, the economy of a country etc.

Definition of Vulnerability

The Vulnerability (Vu) is the degree of fragility (natural or socio-economic) of a community or of a system to a hazard (a little vulnerable system is resilient). It is a set of conditions and processes resulting from physical, social, economic and environmental standards. Among the indicators of vulnerability are:

- Population density, which is an economic / social and provides a measure of the number of people impacted by the disaster.
- Important natural areas and / or sites of high artistic / cultural, unique places for flora / fauna and / or heritage and identity of the population.
- The level of schooling of a social type that measures the ability to understand information on the risks and put it into practice, it is assumed that the low level of education is reason to weakness in relation to the response to the risks, the readiness of the institutions that the level of mitigation.
- The morphological type and hydraulic waterways, type and state of vegetation cover, soil and use of lithographic features (i.e. permeability, porosity) and topography (slope), infiltration and water run-off.
- Temperature, wind, pressure, humidity, cloud cover, surface fluxes and soil moisture, the mixing height and friction velocity, solar radiation, vertical thermal gradient for the determination of the share of thermal inversion.
- The topographical features (location of buildings that affect the air circulation, so-called canyon effect).
- Flow of vehicles and the hot gases emitted, censuses of accidents, plant per square km.

Risk

It is important to exactly understand what the difference between risk and hazard. As mentioned above, the 'Hazard is an event capable of causing loss of life, property or environmental degradation or even a potential threat to society and its well-being.
The Risk (R) is seen as a combination of the probability of occurrence (frequency) of a given hazard and the type of impact; mathematically is a product or R = H * Va * Vu

- H = Hazard (probability of hazard event)
- Va = value (of assets at risk)
- Vu = Vulnerability (% assets at risk likely to be lost in relation to the event)

Having defined the risk as a product of three factors: Risk = Hazard x Vulnerability x Value, it can be derived a framework to monitor the overall risk not only as a parameter but also in its component factors.

Lower then the value of one or more of them is a way to break down and / or mitigate the risk. To work in this direction it is necessary "to control" the evolution of these factors. To "keep under

control" is necessary to know the dynamics that characterize them and the laws that bind them and monitor them over time.

In summary, the framework for risk monitoring consists of the following elements:

- Risk Assessment: identification of hazard, construction of risk scenarios and assignment of probability of occurrence, identifying possible solutions to mitigate / lower the risks.
- Risk Management: acquisition and control of the evolution over time of the variables of risk, implementation of the solutions identified above.

Concerning the evaluation of the probability of occurrence it is an estimate of how often a hazard event occurs.
Manufacturers with a quality system should be able to give a lot of useful statistics.
A review of historic events assists with this determination. When accident statistics for specific products exist, they can directly be used to determine the probability.

3 THE SUSTAINABILITY OF A SYSTEM BASED ON NEW TECHNOLOGIES.

3.1 Problems with Risk Evaluation

Although learning from past accidents (historical data) is still an important part of safety engineering, lessons learned over centuries about designing to prevent accidents may become ineffective when older technologies are replaced with new ones. Technology is changing much faster than the engineering techniques are responding to these changes. New technology introduces unknowns into systems and creates new paths to losses.

3.2 Problems with technology maturity level

The time to market for new products has decreased, the average time to translate a basic technical discovery into a commercial product in the early part of this century was thirty years. Today technologies get to market in two years and may become obsolete in five years. Often a careful testing to understand all the potential behaviours and risks before commercial use is missing.
System engineering and system safety engineering have not kept up with the fast pace of technological innovation, approaches to lower risks working on electromechanical components such as redundancy could result ineffective.

3.3 ICT Risks

ICT widely spreads over the every daily life, from the management of Critical Infrastructures to home automation. Risks of such pervasiveness lie in vulnerability to hazards for systems and citizens; in fact, malicious attacks and system failures may result is catastrophic effects.

This situation has lead society to be cautious in the adoption of new technology especially for safety critical applications.

Clearly identified and perceived safety critical applications, as by instance the on board software for an aircraft, must comply to strict rules, imposed by in this case by the Agency for Aviation Safety (EASA, ENAC, etc). Producers of this type of safety critical applications have to guarantee to follow a predetermined process for the product life-cycle according to relevant safety categories.

Most of the Critical Infrastructures (Internet, Banks, plants, airports…) are mainly software related and they are more and more interdependent so a disruption could lead to a domino effect.

In this field, books and cinematography have widely diffused the idea that programmers could maliciously hide dangerous behaviours in the software code like being capable of autonomous malicious actions. This is obviously not true, anyway unethical programmers could right now introduce hidden malicious code in the computers.

3.4 The Complementary measures to address Sustainability Risks

On a general basis, sustainability is an ethical imperative to protect the world for future generations. Sustainability is often misinterpreted as a goal to which aspire. In fact, sustainability does not describe a static end state, but is a characteristic of an evolving system. Sustainability can also be misunderstood as purely concerned with environmental conservation. This is not accurate. Sustainability requires the consideration of interacting and interdependent environmental, social, and economic systems.

Sustainable development is "development that meets the needs of the present without compromising the ability of future generations". Hence it follows that the identification of risks should also concern sustainability issues.

This thesis also integrates in the framework possible concerns of the society raised by the use of new technology which are related to sustainability.

Specifically it addresses:

- in case of accident: liability (incl. issues like enforcement, impact of automation) and insurance;
- the protection against abusive use: privacy, data protection, security;
- public acceptance of new technology. They are called Complementary measures:
    - Liability / insurance,
    - Privacy/ data protection,
    - Public perception (Public acceptance, acceptable risk),
    - Ethics.

The Complementary Measures analysis will be shown containing the following elements:

- a description of the areas which need to be examined;
- for each area the main issues and the proposed solutions.

3.5 Liability and ethics

In the areas where it has been identified that existing regulations cannot support new technology adoption, a regulatory framework needs to be developed to determine which technologies or procedures are essential to reach the objective of a safe introduction.

Although the matter of regulating the use of new technology is clearly relevant today and is being examined by many international authorities, the present legal framework is often inadequate.

By instance, considering the complexity of new systems, it is vitally important to make a clear distinction among people operating the system at different stages in the system life cycle.

In this perspective, the liability for damages caused by a system failure should be attributed to the operator, that is, the person or entity that, ensures its functioning and makes known his or its status as operator.

Determining the operator's liability is made without regard to personal responsibility (negligence or wilful misconduct). Therefore, it is strict liability based on the risk of a lawful activity.

Liability can be strict or based on fault of the operator. Under strict liability, no negligence of the operator needs to be proven, whereas with fault-based liability, an operator will only be found liable if some form of negligence is established.

The use of new automatic tools may shift liability for accidents from operators to technology, this means from operators to manufacturers, organisations and system developers. In this respect, various issues could be analysed from the legal perspective: (a) balancing individual liability and organisational liability, (b) determining how different degrees of autonomy of agents and machines shape the liability of the different actors (operators, end users, manufacturers designers), (c) analysing dynamic transfers of responsibility due to forthcoming operational concepts and procedures.

Indeed, automated systems add further layers of complexity with respect to traditional software/hardware artefacts, since they may possess (in different degrees depending on the capabilities of each system) autonomous cognitive states and behaviours that are relevant from a legal perspective. In these cases, the reason why the effects of what an automated system does will fall on the user is not that the user has wanted or has predicted its behaviour, but rather that the user has chosen to use the automated system as a cognitive tool and is committed to accepting the results of its cognitive activity. When in complex organisations the automation has taken over more or less completely, humans become controllers of automated systems, rather than operators: in fact, automated systems directly operate to fulfil the task, exercising cognitive functions, acquiring information from the environment, processing it, and using the knowledge so obtained to achieve the goals assigned to them, as specified by their users, while humans monitor the work of automated systems.

Moreover, in scenarios, when one or several operators/controller and one or several automated support systems interact together for the fulfilment of a task, it would be better to describe humans and technology not as two interacting "components", but as constituting a joint (cognitive) system. The term "joint cognitive system" means that control is accomplished by an ensemble of cognitive systems and (physical and social) artefacts that exhibit goal-directed behaviour. Under this perspective, a relevant (and still open) question is that of how to deal with cases in which (as in some recent aviation accidents) conflicting information is provided to operators by humans (controllers) and automated systems, and more generally what kind of priorities should be given to different signals, and when humans may override automatic devices.

Concerning enterprise liability, it should be pointed out that when automated systems are more and more introduced into a complex system (one of the main effects is that allocation of liability for damage or harm is (at least partially) transferred from humans to enterprises using the automated technology that replaced the human operator, or to the technology developer (programmer, manufacturer, etc.…), who created such technology.

Therefore, there is a shift from personal liability toward general enterprise liability (liability for creating a risk through the use of the technology) and product liability. Thus, as the tools are becoming more and more automated, then the liability will be more and more attributed to the

organisations using such tools, and those who build them, or are charge of their maintenance, rather than to the operators interacting with them.

Furthermore, speaking about the developer, the more automated the system becomes, the more organisations and individuals are involved in building, testing, and developing it: this is why the failures caused by highly automated tools will also require the solution of the problem of distributing liability among the developers involved in building it. This would mean that experts will be called to establish what went wrong in the tool, and who was responsible for that particular part of it which went wrong: the developer of hardware, the developer of software, the maintenance service provider, the software engineer who had the task to ensure the frictionless integration of different parts of the tool, etc.

As liability may emerge from the introduction of a new inadequate technology, liability may also emerge also from not adequately deploying an appropriate technology or for no using a new useful technology: the adequacy of the enterprise operations is to be measured on the basis of all available technologies. The appropriate use of such tools will require the enterprises to reorganize and reframe the internal organization of work and the distribution of tasks. Furthermore, the enterprise will be also obliged to reshape interactions between its employee and the technological tool itself so as to ensure as smooth as possible shift toward a new relation between the machines and human operators.

Finally, in addition to general product liability there are also several strict liability rules, with caps for the amount of damages that could be claimed from the enterprise.

The risk is that the current liability regime could result in unbearable costs for enterprises, so that to hamper the adoption of automated technologies, and in particular safety-enhancing technologies:

concerning product liability, the issue is whether enterprises may always rely on the “state of the art” defence, so that they should not be held liable when automated technologies were developed according to available standards and when it was impossible to foresee malfunctioning of the technologies at the current state of the scientific and technological knowledge available in the field;

concerning strict liability, we should consider whether current liability caps are appropriate also for higher level of automation, or complementary measures should be adopted to ensure that damages will be paid without creating a too high burden for enterprises (e.g. compulsory insurances for all stakeholders involved in the design/ development/ use of automated technologies, and the introduction of compensation funds).

A second question to be analysed concerns how to properly analyse and manage the shift of liability due to automation, in order to achieve an optimal allocation of burdens. This will imply reconsidering the role of liability, not only as a tool to redistribute risks and allocate sanctions for errors and accidents, but above all as a means to prevent those accidents and to increase levels of safety and performance fostering the development of a safety culture within organizations. Thus, it will be essential 1) to identify tasks and roles of operators and automated tools; 2) to identify the expected level of performance for each task; 3) to consider different kinds of errors (unintentional rule violations, reckless behaviours, intentional violations); and 4) to define the appropriate legal and disciplinary sanctions and/or safety incentives in relation to different errors, risks and accidents.

All main productive, administrative and social organisations can be seen nowadays as interconnected socio-technical systems, namely, integrated systems constituted of technical artefacts, social artefacts, and humans. Technical artefacts, like tools and machines, determine what can be done in and by an organisation, amplifying and constraining opportunities for action. Social artefacts, like norms and institutions, determine what should be done, governing task, obligations, goals, priorities, and institutional powers. However, norms need to be understood, interpreted, negotiated, and actuated by humans, who may of course deviate from them, or even decide to change them.

A third question regards the extent to which the realisation of such a system requires a change in the law in force, the extent to which public regulation is required as opposed to self-regulation, coupled with contractual mechanisms.

The aim should be to adopt an early, proactive and iterative identification of legal issues that may emerge from the use of a new technology and that may also impact on its success (acceptability and/or sustainability). The idea is to identify potential liability issues at the earliest stage of the development process of new technologies (including the development of the concept itself, and the adoption of standards or certification procedures), so that immediate remedial actions can be taken in relation to the design of such technologies, or their implementation and deployment in organisations..

In conclusion, in order to ensure a safe and responsible adoption of automated technologies, an appropriate assessment of regulation and allocation of liability is crucial. Therefore the research on liability and automation in relation to new technology should pursue the following objectives:

1) To investigate how automation changes the tasks and responsibilities of human operators, organisations, and technology providers, i.e., manufacturers, system and software developers. This requires addressing different issues: e.g., (a) how different degrees of automation in a complex organisational framework, shape the responsibilities of the different actors (operators, controller, managers, manufacturers, designers), (b) how forthcoming operational concepts and procedures provide specific challenges in the involvement of the different actors and their consequent responsibilities;
2) To analyse how existing laws and regulations (national and international, public and private, including standards and certification procedures) regulate the allocation of liabilities for the development and use of automated systems, and the assessment of whether such laws and regulations provide an adequate normative framework.
3) To reduce level of uncertainty within insurance sector or any other risk-sensitive stakeholders by providing a first solid approach on assessing risk around new technology. Conclusions can be shared amongst various stakeholders and may even contribute to achieve increased acceptance within the society of member states.

3.6 Privacy and data protection

The introduction of new technology has raised many legal questions that include, inter alia, the issues of right to privacy and data protection.

Although during the research activity issues related to privacy and data protection related to the adoption of a new technology, have been addressed, all the outcomes are not described in this thesis as such considerations are premature compared to the TRL of the system of systems which is the pilot case under study.

The data to be collected during the risk management process should be:

- processed fairly and lawfully;
- collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;
- adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
- accurate and, where necessary, kept up to date (all reasonable steps should be taken to ensure that data which are inaccurate or incomplete in relation to the purposes for which they are collected or for which they are further processed, are erased or rectified);
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are collected or for which they are further processed.

3.7 Benefits for Citizens

The benefits the new technology could ensure to Citizens represent one important cornerstone for their acceptance by people.

Among these, citizens can see a number of them as having more direct benefits on their lives and we can classify them in three groups:

- Missions related to Civil Protection: technology used in monitoring, preventing and alert system for natural disasters.
- Missions related to Security: for coastal surveillance or sensitive sites (ports, airports, power plants) monitoring.
- Mission related to Environment Protection / Preservation: monitoring and protecting natural environment.

Examining in more details the above possible utilisations emerges a variety of specific tasks that are already perceived as important by citizens, despite the possible different priorities among the States. Just recalling the results recently emerged from a number of statistical analysis and studies, it is possible to depict an almost exhaustive picture of what is actually recognised as “important benefits” by citizens in the civil protection, security and environment fields.

A number of coordinated actions of leveraging on these arguments could help in building the public awareness about new technology; as a consequence, the growth in familiarity for their technologies

will be facilitated, also considering that some of them are already available in different field of application like automotive and mobile phones.

To maximise the success of information actions toward the Citizens, all the aspects of new technology utilisation have to be addressed and analysed in advance by experts and institutions, in order to create a consistent foundations of knowledge to be used to adequately substantiate the information to be disseminated toward the population.

Monitoring and protecting natural environment is from decades a very sensitive issue for citizens. The impact on daily life of climate change, air and water pollution and other events endangering the natural environment has probably a psychological impact higher than the effective one. Despite this maybe debatable perspective, the natural environment represents formally the heritage for next generations and present generations are considered as morally responsible for its preservation.

3.8 New Technology Acceptable Risk

Perception of Risk

Insight into the cognitive processes involved when humans evaluate risk and make trade-offs is crucial to understanding how users behave when making security/safety decisions. Schneier [5] and West [6] present explorations of how cognitive processes affect decision making and risk perception. Schneier comments that security in itself is a trade-off and that 'security is both a reality and a feeling, and they are not the same'. He argues that in a digital domain our perception of security is not well aligned with the reality unlike our evolved perception of physical threats. He outlines some key features of human decision making:

1) Exaggerate spectacular but rare risks and downplay common risks.
2) Difficult to estimate risks for anything not experienced before.
3) Personified risks are perceived to be greater than anonymous risks.
4) Underestimate risks they willingly take and overestimate risks in situations they can't control.
5) Overestimate risks that are being talked about and remain an object of public scrutiny.

One relevant field of research is Prospect theory [18] that describes how humans made decisions in situations involving risk. One key observation is that when it comes to gains, humans are risk averse, and when it comes to losses are risk seeking. One relevant aspect of prospect theory is the framing effect where the decisions a user makes in a trade-off situation are affected by the information being framed as a gain or a loss. Optimism bias is the effect that humans believe they will do better than others at a particular task; in terms of computer security this translates to how humans believe they are less vulnerable to a threat than others. West [6] presents a less thorough survey of the behaviour economics field yet echoes key points made by Schneier. Humans have

limited capacity for information processing and believe they are less at risk than others; users are also more likely to gamble for a loss rather than accept a guaranteed loss.

While there are detailed methods for the objective measure of the likelihood of a hazardous event based on a quantitative measure of historical safety performance, there are substantial differences in what is measured and what is perceived. Risk perception, and not the objective measure of risk, will be the driver behind the acceptance of the new technology. Therefore, it is necessary to discuss the key factors influencing the perception of risk.

The perception of risk is driven by the magnitude of consequence more so than the associated likelihood of occurrence. Public perception of risk focuses on those hazards that have the potential to cause large consequences.

These hazardous situations, despite their likelihood, must meet a higher public expectation than those hazards of less severe consequence of higher likelihood, such as that of an impact with the ground.

Building public awareness and familiarity with new technologies will be an important aspect to gaining acceptance of the technology. People's risk perceptions are based on a combination of subjective judgment and limited knowledge of the true risks imposed by a new technology. According to a recent study there is a tendency by the public to overestimate small risks and to underestimate large risks, and that the public tends to focus on risk and how they can protect themselves from those risks. Conversely, experts tend to perceive risks within their competence area as much lower than the public. As a result, public trust seldom conforms to expert assessments of hazards associated with technologies, particularly when the technology is new to the public. That is why it is necessary to create credibility for the industry and not merely impose new products.

In most cases, society has opposed any new technology that has associated risks.. Distinctions must be made between those applications where the principal risk exposure is voluntary from those of involuntary risk exposure.

This is because the public places a higher demand for protection from involuntary risks as opposed to voluntary. Research has indicated that this extra level of protection can be as much as 1000 times more. The nature of risk exposure is therefore an important factor in the definition of acceptable risk criteria. It is worth noting that the question relates to the public's acceptance of the risks associated with a new technology and not the public's acceptance of a new technology.

The quantification of an acceptable level of risk, although an important factor, is only one component characterizing the public's acceptance of a technology. Other complex and often immeasurable factors such as morals and the economic and political climate are equally as important. A study characterizing these complex social factors and importantly a means to address them is necessary before acceptance of new technology can become a reality.

Summarising the basic theory behind the acceptance of risk is the subjective assessment between:

- Society's perception of the level of exposure to the hazard;
- Society's perception of the benefits due to the hazardous activity.

On a general basis the media and public must be convinced that the perceived benefits (i.e., higher level for security, improved information, more services, lower costs) outweigh potential "costs" (i.e., increased noise, pollution, privacy concerns, safety risks, delays).

The impact of the new technology on the environment can also influence society acceptance. New technology may be limited by noise, emissions, or other environmental constraints and, if in great numbers, will become a nuisance. Use of solar power, fuel cells, and other low emissions systems, could encourage their use among people caring for the Environment.

The perceived benefit from a hazardous activity directly influences an individual's willingness to accept risk. It has been shown that the level of benefit awareness is directly proportional to the acceptable level of risk. For human-piloted aviation, the benefits are easily identifiable to the general public, in terms of efficient transportation of people and freight. However, this was not always the case. In the early periods of human-piloted flight, the immediate benefits of aviation to the general public were not so clear. A similar situation exists for new technologies: awareness of their benefits will push acceptability in their risks. Therefore it is important that the industry acknowledges the relationship between benefit awareness and acceptability of risk.

To foster awareness in the general public, familiarity with the technology, as well as its benefits, will also reduce the risk due to the uncertainty in the unknown. In addition, the perceived benefit coupled with societal values and obligations may result in different levels of acceptance for different types of operations. It is likely that the public will make a distinction between those operations which provide a "greater good" (for example fire fighting or search and rescue) and those operations, which have only limited community benefits.

Gaining public trust in new technology needs time and specific actions. But any obtained trust could be easily damaged or lost in a high exposure accident.

To reduce the possibility of an adverse public reaction to new technology, a strategy for communicating with the public is needed based on the following actions:

- Make people perceive new technology as a natural part of future society-increasing familiarity;
- Create positive interest in awareness about benefits;
- Quickly and accurately report good and bad news concerning new technology perception versus objective evidence;
- Create a website where the public can get information and ask questions increasing familiarity;
- Select a person or group to be responsible for industry's information flow-public acceptance facilitator role assignment;
- Deliver information to the public through presentations in the media-proper dissemination;
- Select a group of public relations experts to be responsible for comments from industry public acceptance facilitator role assignment;
- Create a strategy to be used in case an accident occurs.

In line with these recommendations, the benefits of the new technology must be better explained to the public. For example, to stress the roles it has in conducting humanitarian operations or in testing for airborne toxins, rather than focusing only on the military and security applications.

Other matters of facts are listed in the following:

- cost saving issues
- noise reduction
- safety improvement

Furthermore the policy making process supporting the development of new technology applications needs to be transparent and involve the consultation of stakeholders, for example bodies like the European Group on Ethics, the LIBE Committee of the European Parliament or the European Union Agency for Fundamental Rights and European Data Protection Supervisor.

Last but not least, a certain range of permissible or forbidden uses of new technology could be defined to increase the confidence of citizens. Guidelines for certain civil uses would be based on a 'privacy and data protection impact assessment' and involve interested stakeholders.

An ad hoc group promoting Public Awareness (Public acceptance facilitator) will be responsible for researching and analysing the sentiment of an often forgotten stakeholder, the public. The public opinion of new technology must be considered in order to assess where the public stands on the issue, and what must be done to gain public acceptance. One way to do this is to get information directly from the public, specifically by means of a survey.

At its most basic level, it will give an idea of what the public knows about new technology and how they feel their safety is affected by various uses of it. Taking demographic factors into account, it will be possible to draw generalizations of different public groups. In addition, it will compare perceived risks associated with various uses with their perceived benefits.

The demographic groups will include; age, gender, level and type of education, voting status, flight frequency, and pilot status. Participants will be asked to assess the benefit and risk they associate with specific applications compared to the current way these services are being performed.

This assessment will include risks to different classes of people, and benefits to the users as well as society in general. This will also allow drawing correlations between certain types of uses in order to determine which applications are more easily accepted. It is difficult to exactly predict what the public response will be; there are some responses that seem more likely than others. It is possible that the public will have a significant level of discomfort with some applications. This discomfort will likely be more evident in older respondents, who are generally seen as more conservative when it comes to technology. Younger age groups will have a greater level of confidence in the safety and effectiveness of the technology. More prior knowledge of new technology will correlate with less risk perception, as will a higher level of education.

As far as safety concerns are associated with different applications, the closer a person is exposed to the system where new technology might be in use, the more risk they will perceive.

Responses will be compared to the various demographic responses and generalizations will be made based on different groups. Correlations will be drawn between applications that receive similar risk perception responses and a trial to analyse how or why these relationships exist.

Summarizing the approach towards public acceptance could involve the following steps:

1. Definition of a “public acceptance facilitator group”;
2. Implementation of a survey;
3. Evaluation of the survey results to plan facilitation strategy;
4. Implementation of the facilitation strategy;
5. Measurement of results and improvements.

A survey to:

- Assess current public acceptance;
- Identify ways to foster public acceptance.

The facilitation strategy will improve familiarity with new technology, benefits’ awareness. It will identify some missions to be used as demonstration of the previous aspects.

Some issues to rise:

- Familiarity;
- Awareness of risk;
- Awareness of benefits;
- Reliability data source;
- Push industry competitiveness.

4 THE RISK FRAMEWORK TO SUPPORT SYSTEM REQUIREMENT DEFINITION

4.1 The Research Contribution

The proposed approach supports system requirements definition for the design of a system based on breakthrough technologies.

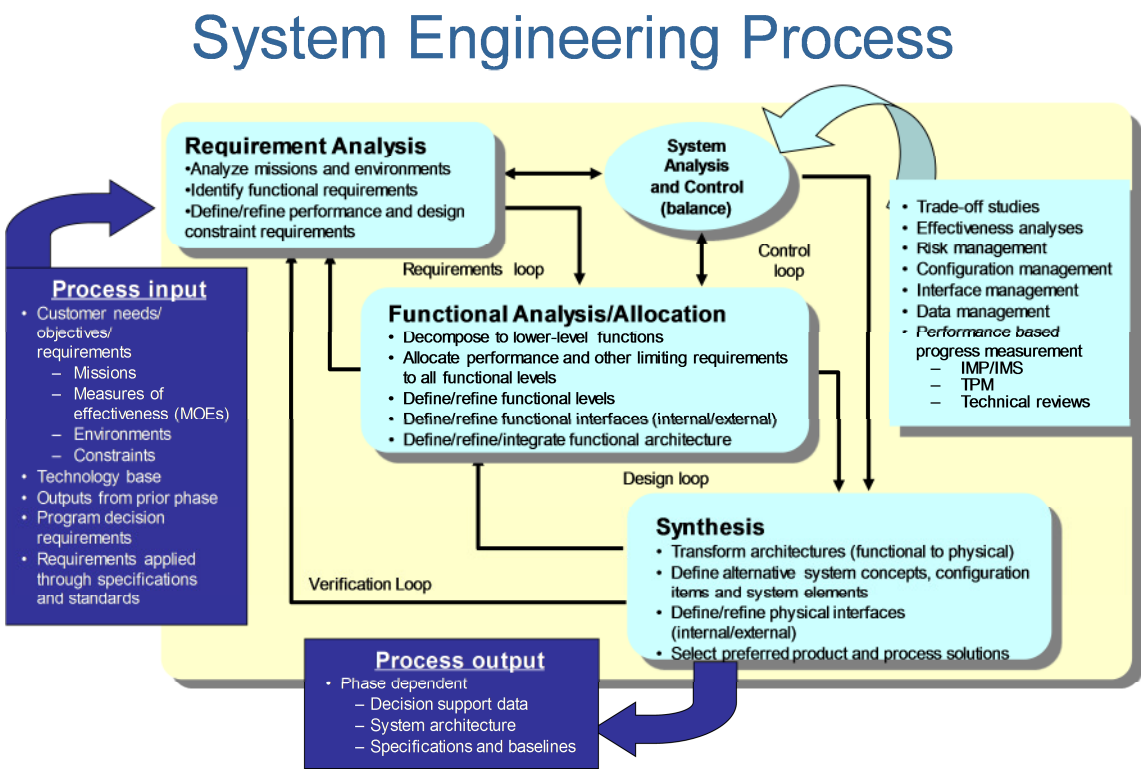
The challenge is to design the system in such a way to prevent failures or to control them when they arise, to manage their effects.

There are five main research challenges:

1. to define a joint approach to risks for new technologies, also considering complementary measure related risks
2. To identify the safety/security/complementary measure objective for the system components of a system based on new technologies
3. To define and implement an approach for the hazard identification for a new technology
4. To define a general framework to support new technology development and exploitation
5. To validate the framework by field data in different application domains.

4.2 The Risk Framework

The proposed framework derives from the application of System Engineering, Reliability Engineering and Complementary Measure Analysis. A scheme of the system engineering process is shown below [28, 29, 30, 31].



Reliability engineering is engineering that emphasizes dependability in the lifecycle management of a product. Dependability, or reliability, describes the ability of a system or component to function under stated conditions for a specified period of time. Reliability engineering is a sub-discipline within system engineering. Reliability is theoretically defined as the probability of failure, the frequency of failures, or in terms of availability, a probability derived from reliability and maintainability. Reliability plays a key role in cost-effectiveness of systems.

i. First of all, it is mandatory to reference to the applicable standards. They depend on the application domain and for safety critical technologies there are rigorous prescriptions to comply to. Usually reference standards require some processes to follow in the system development life cycle driven by a tailoring to identify the mandatory practices to implement.
ii. According to the system engineering process, a preliminary functional analysis with a preliminary product tree definition have to be performed.
iii. The third step involves identification of hazards. There are hazards belonging to the specific technology or intrinsic, hazards belonging to the specific application domains (the system under design), natural hazards, there are also hazards related to the complementary measures previously described. A new technology can bring some new hazards; furthermore, a specific new system (complex and safety critical) can be exposed to some emerging hazards. The approach proposed in this thesis to identify hazards (Reference 3 in paragraph 4.1), asks to collect all of them from the previous categories, to properly tailor the ones applicable to the system under design justifying this tailoring. This preliminary list has to be validated by the stakeholders involved in the system engineering process. Then, it is necessary to allocate the identified hazards to the system components.
iv. FMECA (failure mode effect criticality analysis) can be performed either according to a functional approach or to a hardware approach, mainly depending on the current project phase and the detail of system design information. A functional FMECA (FFMECA) is a FMECA in which the functions, rather than the items used in their implementation, are analysed. So a decomposition of the system functions to be analysed has to be derived from the system functional analysis. A hardware FMECA is a FMECA in which the hardware used in the implementation of the product functions is analysed. In this thesis, the approach to perform FMECA for a new technology is based on the following considerations. For a new technology only a functional approach can be chosen in order to properly address all the system features. The first consideration to be done is that the mission timeline is mostly automatically managed, i.e. by Sw modules and Sw at all levels can be analysed only using a functional approach. The second element to consider is the information available at S/S level. A system level FMECA, implemented using a hardware approach, is fed by S/Ss failure modes derived by S/Ss suppliers FMECAs. At this point of the analysis these data are not available yet, thus a functional approach is the only applicable one. Thanks to the functional approach a ranking can be done for the involved functions and the attention can be focussed only on the critical ones and on the corresponding S/S implementing them. In this way qualitative and quantitative failure mode and reliability data search can be limited only to the most important S/Ss.

v. Once FMECA has been performed, the proposed approach requires to choose (Reference 1, 3 in paragraph 4.1) those hazards which represent initiator events for the corresponding failure mode, as for those hazards the system components impacted by them have already been identified.

vi. According to the severity of that failure mode the requirement for the corresponding component will be derived in terms of reliability requirement for that component. If the severity is catastrophic the involved components must be highly reliable (Reference 2 in paragraph 4.1). In the following table a representation of this scheme is shown.

SEVERITY	SAFETY	DEPENDABILITY	DESCRIPTION	IMPLICATIONS
Catastrophic	Loss of life, life threatening or permanently disabling injury or occupational illness Loss of an interfacing manned flight system Severe detrimental environmental effects Loss of system facilities Loss of system	Loss of system	Including any single failure or combination of failures implying that the system can't be recovered	The corresponding components should have high reliability
Critical	Temporarily disabling but not life threatening injury, or temporary occupational illness Major detrimental environmental effects Major damage to public or private properties Major damage to interfacing	Loss of mission	Including mission abort or failures implying: 1) proper test conditions for descent system test are not guaranteed 2) proper test conditions for recovery system test are not guaranteed 3) requested test data are not stored	Theoretically the loss of the mission objectives should bring to a "loss of mission" consequence.

	external systems Major damage to ground facilities			
Major		Partial loss of mission	Including any single failure or combination of failures implying a partial recording of test data.	
Minor		Mission Degradation	Including any single failure or combination of failures not invalidating the identified test objectives: 1) system recovery 2) proper test conditions for descent system 3) proper test conditions for recovery system 4) test data storing	

For each considered function the hazard scenario is built as follows:

SCENARIO-A

FFMEA

- Function FX.Y *(a function whose failure can have catastrophic effects on human life or environment*)
- Functional Failure Mode of FX.Y
- Functional failure mode effect

Initiator Events

- Hazards = hazards corresponding to initiator events for the functional failure mode

Components

- Allocation of hazards to components relevant to the safety critical functions

Safety Requirements

- Preliminary Safety Requirements

At this stage of the project the hazard assessment identifies critical aspects to care about and gives suggestions for designing components and operations, (the terms FFMEA and FFMECA are considered equivalent for the sake of simplicity).

Each function involves a specific command chain which is made by components (elements of the product tree plus other "actors").

When the failure modes are analysed also the causes will be characterized helping in allocating **liability** for the specific failure (Reference 1, 2 in paragraph 4.1).

Risk Perception management will involve identifying potential users, impacted people, benefits for them to properly compute the ratio cost/benefit and start a roadmap to push public acceptance(Reference 1, 2,4 in paragraph 4.1).

Subsystems involved	S/Ss needed to perform the function under analysis
Mission Phase	Mission phase which the failure is assumed to occur
Id function	Function identification number
Function	A concise statement of the function under analysis
Failure mode	Description of all potential failure modes of the function under analysis
Failure cause	Description of the most probable causes associated with the assumed failure mode
Failure Liability	Identification of the related liability
Failure effects	Local effects – failure mode consequence at the level of the item under investigation. The local effects usually equals the relative failure mode. End effects - failure mode consequence at the level of the product under investigation.
Severity Level	Severity classification category assigned to each failure mode according to the worst potential end effect of the failure
Defect detection methods/ observable symptoms	Failure detection method and the observable symptoms, including telemetry, visual or audible warning devices, sensing instrumentation, other unique indications (e.g. the failure effect itself), or none
Prevention or compensating methods	The existing compensating provisions, such as: o design provisions (for example, redundant items or alternative modes of operation that allow continued and safe operation, and safety or relief devices which allow effective operation or limit the failure effects) o or operator actions (when the intervention of an operator is foreseen) which circumvent or mitigate the effect of the failure.

it is worth noting that in order to identify the risks in-depth knowledge of the system is required.

A synthesis of the framework steps is below.

i) Domain Applicable Standard Identification
ii) Product Tree, System Components, and Functional Analysis
iii) Hazard identification and allocation
iv) FFMECA (Functional FMEA/FMECA)
v) Risk Scenario definition
vi) CIL and System Requirement Definition

In the following paragraph the risk assessment is applied to the pilot scenario to support the requirement definition(Reference 5 in paragraph 4.1).

5 THE CASE STUDY

5.1 The Application Domain

In the 2050 aviation vision from the European Commission [2], objectives in terms of noise, chemical emission, energy consumption and safety level among others present a significant gap with today's transport solutions performances. However, since the current aircraft architecture and operation procedures have been optimized for decades, expected gains in terms of efficiency and environmental impact would be small with respect to the proposed goals. It is then clear that radical changes in the air transport system are necessary to make the necessary step change in terms of overall performance.

In 2007, the "Out-of-the-box" study [4] gathered an important numbers of solutions that could redefine air transportation. Among these ideas, one proposed to have ground based systems specifically designed to assist the airplane during the take-off and landing phases. Based on this proposal, the GABRIEL project [3] aimed at developing a full operational concept with a ground powered system that provides the necessary thrust to accelerate the aircraft up to lift-off speed (or more if necessary).

The idea was to use magnetic levitation to launch aircraft. (The MAGLEV system). The idea was to put an aircraft on a cart that would be attached to a rail system. The principle was that aircraft would need less power for take-off and as a result would use smaller engines during their flight.. The cart would provide electric taxi at the airport which would also reduce emissions

If landing on a maglev pad would prove to be feasible and economical, this unique and radically new solution could reduce aircraft fuel consumption; in fact, aircraft weight would be reduced due to no undercarriage, less fuel on board, smaller engines. Using ground power will also reduce the environmental impact with lower noise and emitted CO_2 and NOx emissions at TOL.

The GABRIEL project investigated if magnetic levitation assisted take-off and landing is feasible and cost effective.

Magnetic levitation is already a developed and deployed technology in rail transportation. However, research is needed to prove the technical feasibility of the concept in air transportation. The GABRIEL project investigated how to adapt the existing magnetic levitation technologies and the needs for aircraft redesign. The project also studies the feasibility of launch and recovery in connection to operating limits and aircraft flight controls. A small scale test is designed to assess the feasibility and estimate the limits of the assisted take-off and landing concept. Operational, safety, and cost-benefit related issues are studied extensively.

The author was involved in this project performing a large contribution to the safety and security aspects.

In this project the proposed Risk Framework has been applied to drive the system requirement definition.

5.2 The Risk Assessment to identify system requirements

An accurate knowledge and comprehension of the application domain are key points to develop adequate and effective risk identification and design robust systems (**step i)** of the Risk Framework). Maglev technology historical data records belong to the railway domain and a primary lesson learned from the accidents in the railway domain is the importance of risk/hazard analysis that can qualitatively focus on the severity of accidents and human factors.

These findings are not entirely consistent with current actual practices based on international railway standards; they rather conform well to the fundamentals of System Safety, which is an organized and established method to assure safety in complex systems.

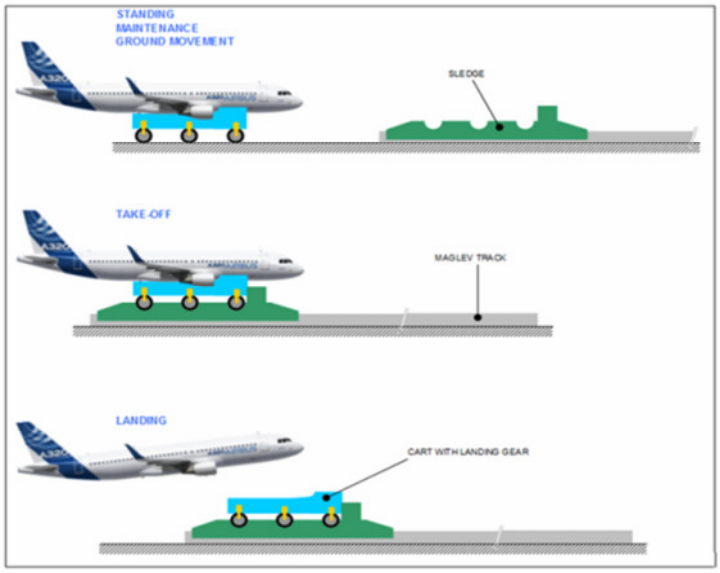
The approach, adopted in the Gabriel safety activities, derives from the application of the Risk Framework shown in the paragraph 4.2.

6 PRELIMINARY SYSTEM CONFIGURATIONS, FUNCTIONAL ANALYSIS, PHASES

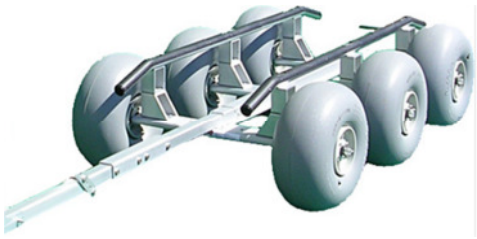
6.1 Product tree– Cart on sledge

This concept would basically allow aircraft having no undercarriage which would save weight on the aircraft. For emergency the aircraft would have a parachute to land safely. Having no undercarriage the aircraft would be placed on a cart that has its own electric engine and remote (GPS based) steering mechanism for ground taxi, which would allow for low CO2 and other emissions during ground operations and would allow for smaller and narrow taxiways[7, 8, 9, 10, 11, 12].
After some preliminary evaluations among possible system configurations, the basic system configuration has the cart loaded on the sledge for both taxying and TOL, its name is cart on sledge ***(step ii) of the Risk Framework)***.

❖ **Flight segment**



- Airframe
  - Vertical and horizontal tail surfaces
  - Fuselage
  - Nacelle
  - Aerostructure
  - Wings
  - Actuators
  - Control surfaces
- Propulsion System
- Engines
- Auxiliary Power Unit
  - Energy supply to on board systems
- Airframe Cart Interface
  - Airframe Cart connection
- Data Handling System
  - Data Handling on board computer
  - Data Acquisition System
  - Harness
  - Ethernet cable
  - Harness
  - Data Handling Software (DHSW)



- Communication System
  - Communication system between pilot, optional cart driver and the tower
  - Flight Segment and sledge Communication link
- "Landing/Take off GNC Rendezvous with Sledge"
  - Guidance
  - Navigation
  - Control
  - GPS
  - Inertial Management System
  - Air Data

❖ Ground Segment

- Ground control station
  - Communication system
  - Data acquisition system
  - Data storing system
- Cart
  - Structure
  - Landing gear
  - Sensors
- Cart Airframe Interface
- Cart Sledge Interface
- Facility to load cart on sledge
- Facility to unload the cart from the sledge, or
- Sledge
  - Frame (platform, structure)
  - Magnetic suspension
  - Magnetic propulsion
  - Auxiliary Wheels
  - Springs
  - Emergency brake
  - Auxiliary equipment
- Sledge Cart Interface
- Sledge Maglev Track Interface
- Runway
  - Ground Support Equipment [2]
- Maglev track
  - Track (may be installed on or aside a runway)
  - Electrical power supply for magnetic levitation and traction
- Sledge Control System
  - Control system for the track operations (loading, take off, landing, unloading)
  - Track condition monitoring system
  - Magnetic Levitation System
  - Magnetic propulsion system
  - Communication system between pilot, (optional cart driver) and the tower
- Hangar
- Taxiway

[2] The standard ICAO Annex 14 provisions (markings, lights, meteo); The standard cat III ILS provisions (localiser, glide path, monitoring system); Differential GPS for high accuracy landing operations

6.2 Identification *of system components for the hazard assessment*

The system components set has been derived starting from the product tree , choosing its elements at down to the third level.

This set contains the components listed here below:

Airframe	Propulsion System	Auxiliary Power Unit	Airframe Cart Interface	Airframe Sledge Interface	Data Handling System	Communication System	Landing/ Take off GNC Rendevous with Sledge	Ground control station	Cart	Cart Airframe Interface	Cart Sledge Interface	Facility to load cart on sledge	Facility to unload the cart from the sledge, or	
Facility to transfer the aircraft from the cart on the sledge	Facility to transfer the aircraft from the sledge to the cart	Sledge	Sledge Cart Interface	Sledge Airframe interface	Sledge Maglev Track Interface	Runway	maglev track	Sledge Control System	Hangar	Taxyway	Pilot	Traffic controllers	MRO	Operators

In green the components belonging to the concept "*Cart for Taxying + sledge for TOL*", this configuration has been displayed for completeness; in yellow the components belonging to the concept "*Cart on Sledge*". After a preliminary trade-off, the concept "Cart on Sledge" was chosen.

6.3 The Functional analysis allocated to the phases.

In the following for each phase of the "mission", the functions the system has to perform are listed (step ii) of the Risk Framework);

PHASE 1 STANDING and MAINTENANCE

F1.1 to lock the coupling between the aircraft and the cart
F1.2 to allow the loading of passengers / cargo in a stable manner
F1.3 to allow the reloading of energy sources
F1.4 to enable test and maintenance operations
F1.5 to enable catering services
F1.6 to maintain the stability of the aircraft in critical weather conditions
F1.7 to avoid contact between the aircraft and the ground
F1.8 to enable movements on the ground according to need of the airport and the airlines
F1.9 to enable the security of the maintenance operators
F1.10 to enable ground stability without damaging the fuselage
F1.11 to enable a simple access for maintenance (fuselage in particular)

PHASE 2 GROUND MOVEMENT

F2.1 to move the cart with the aircraft in the airport area without consuming on-board energy
F2.2 to respect the orders of ground controllers managing ground movements
F2.3 to minimize impact on the environment during taxi
F2.4 to ensure passengers safety in case of strong wings and other adverse conditions
F2.5 to allow the positioning along the take-off area axis
F2.6 to follow the sequence provided by air traffic controllers
F2.7 to allow the positioning in the take-off position on the sledge

PHASE 3 TAKE OFF

F3.1 to secure the A/C or cart position on the sledge (Loading A/C/cart on cart/sledge)
F3.2 to accelerate to the desired speed meeting passengers constraints
F3.3 to guide and control the trajectory along the runway track
F3.4 to decide about the continuation of the take-off phase
F3.5 to control the separation between the aircraft and the cart
F3.6 to enable the minimum slope and speed for take off
F3.7 to free the take-off zone for the next aircraft
F3.8 to remain within the flight envelope
F3.9 to maintain the minimum climb slope (OEI condition included)
F3.10 to maintain the necessary speed
F3.11 to respect the air traffic controllers orders

PHASE 4 LANDING

F4.1 to synchronize the rendezvous between the aircraft and the composite system in a defined area

F4.2 to respect the sequence provided by the air traffic controllers

F4.3 to reach the final approach zone

F4.4 to align the aircraft in the landing axis (trajectory)

F4.5 to absorb the potential/dynamic energy of the aircraft

F4.6 to ensure and control the contact between the aircraft and the cart

F4.7 to lock the aircraft on the cart

F4.8 to decelerate

F4.9 to minimize environmental impact

F4.10 to free the A/C or cart from the sledge (unloading A/C or cart form sledge)

F4.11 to enable the cart to roll on the runway with the aircraft

7 APPLICABLE STANDARDS AND CRITERIA

The proposed Risk Framework has been designed according to ICAO Safety Management Manual 2009 Doc 9859 AN/474, which, representing a Reference Standard within the aviation safety domain, suggests both the civil manned aircraft safety assessment process defined in ARP 4761 and the safety certification process in ARP4754, to demonstrate compliance with EASA / FAA safety target requirements (step i) of the Risk Framework). These references provide a roadmap to be followed to perform risk assessment based on some available experience and constraints [13, 14, 15, 16, 17, 18, 19, 20, 21, 22]. For a new technology, the classic approaches do not allow to complete the analysis as some necessary data and conditions are missing. The differences introduced in the case study which need to be considered, to ensure safety – are in particular:

- Possible specific safety criteria (of the new technology)
- Lack of historical data (for the new application domain)
- Complexity of the designed system (in terms of safety, environment, economic impact public acceptance)
- Specific mission phases and related functions
- Specific emergency issues
- Coexistence with legacy systems

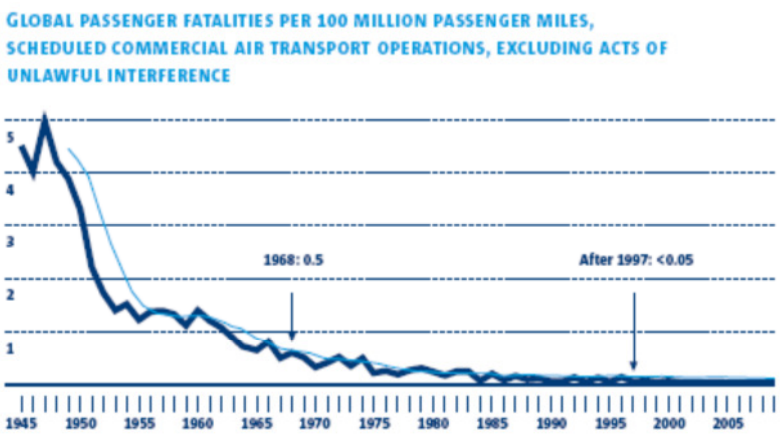
It is worth pointing out, that currently there is no applicable standard for the foreseen system.
The proposed framework has been adopted within a project funded by EC FP7 framework programme [3]; the obtained results were discussed in various official project deliverables. The deliverables were reviewed by EC officers and EASA experts and largely appreciated.
Furthermore, the framework will be adopted as a reference for specific activities in some proposals submitted to the first Call of H2020 EC Framework Programme.

8 HAZARD ASSESSMENT APPROACH

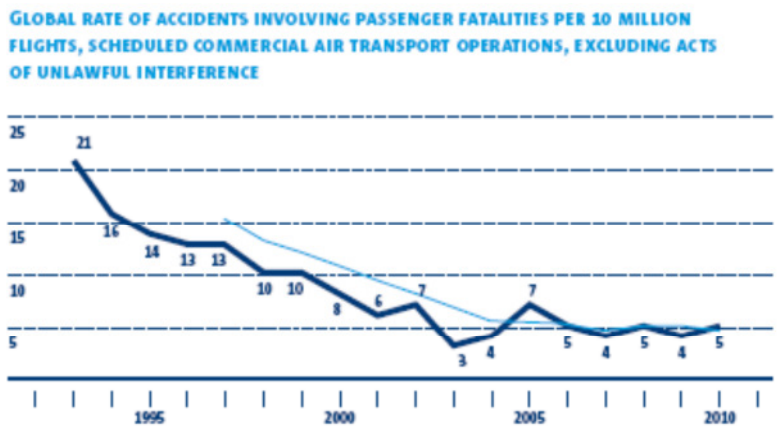
8.1 The adopted approach

According to the previous standards and criteria, the purpose is to identify hazard manifestations, and hazard scenarios and to classify them on the basis of the consequence severity.
A hazard can be considered as a dormant potential for harm which is present in one form or another within the aviation system or its environment. This potential for harm may be in the form of a natural hazard such as terrain, or a technical hazard such as wrong runway markings.

Indications are that the failure rate for MAGLEV technology is currently low [34, 35, 36, 37].
Maglev trains are designed so they can never derail. They contain systems to always make sure the train is always kept balanced on top of the tracks and never shift off of it. Maglev trains system is also designed to never have accidents with other vehicles. The guideways are kept secured so no foreign vehicles such as cars or trucks can cross them.
So far, there has never been a reported collision accident of a commercial maglev train.
Overall there has been only one accident, but this took place during testing in Germany. Since then they have taken more precautions to make sure this never occurs.



Here aside the data from the EASA Annual Safety Review 2010 reporting passenger fatalities per 100 million passenger miles since 1945.



Here aside the data from the EASA Annual Safety Review 2010 reporting passenger fatalities per 10 million flight in the last 15 years.

Studies have been underway on the subject of high speed guided ground transportation safety. According to a preliminary analysis the key areas which may be of concern as any maglev technology moves towards implementation are:

- *High-speed collision avoidance (automation, guideway integrity, shared ROW).*
- *Adequate protection for high mass low speed collisions and low mass high-speed collisions.*
- *Emergency response plans and procedures (fire safety, evacuation methods, training).*
- *Electromagnetic field generation and effects (passengers, workers, public).*
- *Operational issues (weather, automation and human factors, etc.).*

Included in the overall assessment of maglev technology there are the safety concepts from both design and operational viewpoints. Current safety studies do not indicate any safety-related issues that cannot be accommodated through system safety design considerations in an appropriate development program.

As with aircraft, the high speed of maglev appears to make it infeasible to design a practical system that could withstand a high-speed collision. Accordingly, the proper approach is to ensure that collisions do not occur. Although this approach has not been used in U.S. railroad practice in the past, the fact is that high-speed rail has a flawless record.
The Japanese Shinkansen has been in operation for 30 years, has carried 3.5 billion passengers, and has never had a high-speed collision nor caused a passenger fatality.
Likewise, the French TGV has operated for 12 years, carrying a quarter billion passengers. There has never been a passenger fatality on the grade-separated French high-speed line. Thus, it is possible to reduce the probability of collisions to an acceptable level.
This has been the focus of the design for maglev safety as contrasted with crash survivability.
The overall safety for the case study system needed to be reviewed and analysed right from the start of the design phase and including the operational phases in a systematic manner. Keeping the overall safety of a maglev system within acceptable levels as the technology proceeds to the deployment stage will reduce: the potential for unplanned design modifications, adoption of prohibitive operational restrictions, adoption of procedures that could threaten the basic viability of the maglev system.

8.2 Applicable Hazard list

In order to derive the applicable hazard list the implemented process has consisted of:
Collection and analysis of possible safety requirements and lessons-learnt associated with similar previous missions
The sources of information have been:

- Generic hazards applicable to the system design and operation using classical standard list of hazards;
- Specific Maglev Hazard associated with system design, its operation and the operation Environment;
- Hazards resulting from the physical and functional propagation of initiator events;

- Hazards resulting from the failure of system functions and functional components;
- Hazards resulting from the Complementary measure Analysis.

The obtained list contains the following hazard categories: basic design hazard, inherent hazard, malfunctions, meteorological/environmental hazards, human factors.

The design hazard belongs to design phase and if it is critical, attention on design and related system reliability has to be applied in order to avoid it.

The inherent hazard is bound to the system characteristics (nominal) and has to be carefully managed in operations; the malfunctions must be detected, prevented or managed.

Malfunctions are possible failure modes for the system functions.

The Meteorological/Environmental hazards are caused by external events related to extreme natural events or related to environmental impact of the system.

Human factors consist of hazards which could cause human errors as well as hazards which are caused by people.

Some of the identified hazards could belong to more than one category and redundancies within the hazard list are possible. This won't turn in a problem because the aim is to identify all of them, in order to allocate them to the system components.

The complementary measures analysis identifies for each applicable category of complementary measure, the possible hazards.

They belong to: Liability, Data Protection/Security, Public Acceptance [23, 24, 25, 26].

Liability hazards are those hazards which can prevent the liability identification in case of system failure.

Public acceptance hazards are hazards which can spoil the risk perception.

In the following the preliminary applicable hazard list is shown.

❖ BASIC DESIGN DEFICIENCIES

- Structural instability
- Excessive weight
- Inadequate speed
- Inadequate acceleration (positive and negative)
- Inability of aircraft to rotate due to incorrect centre of gravity (CG) location (mistake in performance calculation, or flight control anomalies)
- Lack of accessibility (e.g. inspections, etc.)
- Sharp corners
- Inadequate clearance (among parts)
- Temperature of sensitive equipment

❖ INHERENT HAZARDS

- Vertical kinetic energy
- Horizontal kinetic energy

- High mass and dynamic inertia
- Dynamic stability
- Acceleration (vertical, horizontal)
- Deceleration (vertical, horizontal)
- Contaminated runways (debris, etc)
- Crosswind
- Runway, taxiway incursion (other A/C, other ground vehicles, animals, etc)
- Electromagnetic field
- Mechanical (i.e., rotating equipment, vibration)
- Electrical
- Explosives
- Flammable gases or liquids
- Toxic substances
- Temperature
- Mechanical anomalies

❖ MALFUNCTIONS

- Missing synchronization between sledge and A/C
- Aircraft, cart untimely disconnection/connection
- Aircraft, sledge untimely disconnection/connection
- Cart, Sledge untimely disconnection/connection
- Structural failures
- Mechanical malfunctions
- Electrical malfunctions
- High/Low Pressure in hydraulic systems (actuators, dampers)
- Power failures
- Software failures
- Software Hardware Interface Failures
- Man Machine Interface Failures
- Rapid fire spread, smoke/toxic gas build-ups

❖ METEO/ENVIRONMENTAL

- Noise
- Engine emissions
- thunderstorms lighting
- wind shear
- icing, freezing
- snow
- heavy rain

- low visibility
- floods
- volcanic ash
- Heat
- Cold
- Dryness
- Wetness
- Low friction (slipperiness)
- Glare
- Darkness
- Earthquake

❖ HUMAN FACTORS

- Pilot's or driver or controller perception of a catastrophic failure
- Stress (sensory, mental, motor)
- Physical surroundings (environment)
- Illumination
- Vibration
- Errors
- Omission
- Commission
- No recognition of hazards
- Incorrect decisions
- Tasks done at wrong time (untimely)
- Tasks not performed or incorrectly performed

8.3 Hazard manifestation list

According to the identified system configuration product trees and the functions for each phase, the previous hazards have been allocated to the involved system components.

Each row of the list describes the manifestation of the hazard for each subsystem within each specific mission phase.

Hazard matrices for PHASE 3 - TAKE OFF

Generic hazards	Airframe	Propulsion System	Auxiliary Power Unit	Airframe Cart Interface	Airframe Sledge Interface	Data Handling System	Communication System	Landing/ Take off GNC Rendevous with Sledge	Ground control station	Cart
BASIC DESIGN DEFICIENCIES										
Sharp corners	X									X
Structural Instability										X
Excessive weight										
Inadequate clearance										
Temperature										
Lack of accessibility										
Inadequate speed		X								
inadequate acceleration		X								
Inability to rotate due to incorrect center of gravity (CG) location, mistake in performance calculation, or flight control anomalies										

Generic hazards	Cart Airframe Interface	Cart Sledge Interface	Facility to load cart on sledge	Facility to unload the cart from the sledge	Facility to transfer the aircraft from the cart on the sledge	Facility to transfer the aircraft from the sledge to the cart	Sledge	Sledge Cart Interface	Sledge Airframe Interface	Sledge Maglev Track Interface
BASIC DESIGN DEFICIENCIES										
Sharp corners	X	X	X	X	X	X	X	X	X	
Structural Instability	X	X					X	X	X	
Excessive weight										
Inadequate clearance										
Temperature										
Lack of accessibility										
Inadequate speed										X
inadequate acceleration										X
Inability to rotate due to incorrect center of gravity (CG) location, mistake in performance calculation, or flight control anomalies										

Generic hazards	Runway	maglev track	Sledge Control System	Hangar	Taxyway	Pilot	Traffic controllers	MRO	Operators
BASIC DESIGN DEFICIENCIES									
Sharp corners									
Structural Instability	X								
Excessive weight									
Inadequate clearance									
Temperature									
Lack of accessibility									
Inadequate speed		X	X			X			X
inadequate acceleration		X	X			X			X
Inability to rotate due to incorrect center of gravity (CG) location, mistake in performance calculation, or flight control anomalies									X

Generic hazards	Airframe	Propulsion System	Auxiliary Power Unit	Airframe Cart Interface	Airframe Sledge Interface	Data Handling System	Communication System	Landing/ Take off GNC Rendevous with Sledge	Ground control station	Cart
INHERENT HAZARDS										
Vertical kinetic energy	X			X	X			X	X	X
Horizontal kinetic energy	X			X	X			X	X	X
High mass and dynamic inertia	X			X	X			X	X	X
Mechanical (i.e., rotating equipment, vibration)	X	X	X	X	X					X
Electrical	X	X	X	X	X	X	X		X	X
Explosives										
Flammable gases or liquids		X	X							
Toxic substances										
Acceleration		X								X
Deceleration		X								X
Temperature										
Mechanical anomalies		X		X	X					X
Contaminated runways										
Crosswind				X	X					X
Runway, taxyway incursion						X	X		X	X

Generic hazards	Cart Airframe Interface	Cart Sledge Interface	Facility to load cart on sledge	Facility to unload the cart from the sledge	Facility to transfer the aircraft from the cart on the sledge	Facility to transfer the aircraft from the sledge to the cart	Sledge	Sledge Cart Interface	Sledge Airframe Interface	Sledge Maglev Track Interface
INHERENT HAZARDS										
Vertical kinetic energy	X	X					X	X	X	X
Horizontal kinetic energy	X	X					X	X	X	X
High mass and dynamic inertia	X	X					X	X	X	X
Mechanical (i.e., rotating equipment, vibration)	X	X					X	X	X	X
Electrical	X	X					X	X	X	X
Explosives										
Flammable gases or liquids										
Toxic substances										
Acceleration							X			X
Deceleration							X			X
Temperature										
Mechanical anomalies	X	X					X	X	X	X
Contaminated runways										
Crosswind	X	X					X	X	X	X
Runway, taxyway incursion							X			X

Generic hazards	Runway	maglev track	Sledge Control System	Hangar	Taxyway	Pilot	Traffic controllers	MRO	Operators
INHERENT HAZARDS									
Vertical kinetic energy		X	X			X			X
Horizontal kinetic energy		X	X			X			X
High mass and dynamic inertia		X	X			X			X
Mechanical (i.e., rotating equipment, vibration)		X							
Electrical		X	X						X
Explosives									
Flammable gases or liquids									
Toxic substances									
Acceleration		X	X			X			X
Deceleration		X	X			X			X
Temperature									
Mechanical anomalies		X	X						
Contaminated runways	X	X							
Crosswind			X			X	X		
Runway, taxyway incursion		X	X			X	X		X

Generic hazards	Airframe	Propulsion System	Auxiliary Power Unit	Airframe Cart Interface	Airframe Sledge Interface	Data Handling System	COMM System	Landing/Take off GNC Rendevous with Sledge	Ground control station	Cart
MALFUNCTIONS										
Aircraft, cart untimely disconnection/connection				X					X	
Aircraft, sledge untimely disconnection/connection				X	X				X	
Cart, Sledge untimely disconnection/connection				X					X	
Structural failures	X			X	X					X
Mechanical malfunctions		X		X	X					X
Electrical malfunctions				X	X	X	X		X	X
Power failures		X								
Software failures		X		X	X	X	X		X	X
Software Hardware Interface Failures		X		X	X	X	X		X	X
Man Machine Interface Failures		X		X	X	X	X		X	X
Malicious attacks to system componenets (HW/SW)	X	X				X	X	X	X	X

Generic hazards	Cart Airframe Interface	Cart Sledge Interface	Facility to load cart on sledge	Facility to unload the cart from the sledge	Facility to transfer the aircraft from the cart on the sledge	Facility to transfer the aircraft from the sledge to the cart	Sledge	Sledge Cart Interface	Sledge Airframe Interface	Sledge Maglev Track Interface
MALFUNCTIONS										
Aircraft, cart untimely disconnection/connection	X	X						X		
Aircraft, sledge untimely disconnection/connection	X	X							X	
Cart, Sledge untimely disconnection/connection	X	X						X		
Structural failures	X	X					X	X		X
Mechanical malfunctions	X	X					X	X		X
Electrical malfunctions	X	X					X	X		X
Power failures										
Software failures	X	X					X	X		X
Software Hardware Interface Failures	X	X					X	X		X
Man Machine Interface Failures	X	X					X	X		
Malicious attacks to system componenets (HW/SW)			X	X	X	X				

Generic hazards	Runway	maglev track	Sledge Control System	Hangar	Taxyway	Pilot	Traffic controllers	MRO	Operators
MALFUNCTIONS									
Aircraft, cart untimely disconnection/connection			X			X			X
Aircraft, sledge untimely disconnection/connection			X			X			X
Cart, Sledge untimely disconnection/connection			X			X			X
Structural failures	X	X	X						
Mechanical malfunctions		X	X						
Electrical malfunctions		X	X						
Power failures		X	X						
Software failures			X						
Software Hardware Interface Failures		X	X						
Man Machine Interface Failures			X			X	X		X
Malicious attacks to system componenets (HW/SW)		X	X	X	X				

Generic hazards	Airframe	Propulsion System	Auxiliary Power Unit	Airframe Cart Interface	Airframe Sledge Interface	Data Handling System	COMM System	Landing/Take off GNC Rendevous with Sledge	Ground control station	Cart
METEO/ENVIRONMENTAL										
thunderstorms lighiting	x	x	x	x	X					X
windshear										
icing, freezing	x	x		x	X					X
snow	x	x		x	X					X
heavy rain		x		x	X					X
low visibility										
floads	x	x	x	x	X					X
vulcanic ash	x	x	x	x	X					X
Rapid fire spread, smoke/toxic gas buildup	x	x	x	x	X					X
Heat		X		X	X					X
Cold		X		X	X					X
Dryness										
Wetness		X		X	X					X
Low friction (slipperiness)				X	X					X
Glare										
Darkness										
Earthquake									X	
Noise	X	X		X	X					X
Engine emissions		X								
Electormagnetic field										

Generic hazards	Cart Airframe Interface	Cart Sledge Interface	Facility to load cart on sledge	Facility to unload the cart from the sledge	Facility to transfer the aircraft from the cart on the sledge	Facility to transfer the aircraft from the sledge to the cart	Sledge	Sledge Cart Interface	Sledge Airframe Interface	Sledge Maglev Track Interface
METEO/ENVIRONMENTAL										
thunderstorms lighiting	X	X	X	X	X	X	X	X	X	X
windshear										
icing, freezing	X	X	X	X	X	X	X	X	X	X
snow	X	X	X	X	X	X	X	X	X	X
heavy rain	X	X	X	X	X	X	X	X	X	X
low visibility										
floads	X	X	X	X	X	X	X	X	X	X
vulcanic ash	X	X	X	X	X	X	X	X	X	X
Rapid fire spread, smoke/toxic gas buildup	X	X	X	X	X	X	X	X	X	X
Heat	X	X					X	X	X	X
Cold	X	X					X	X	X	X
Dryness										
Wetness	X	X					X	X	X	X
Low friction (slipperiness)	X	X					X	X	X	X
Glare										
Darkness										
Earthquake										X
Noise	X	X					X	X	X	X
Engine emissions										
Electormagnetic field							X			X

Generic hazards	Runway	maglev track	Sledge Control System	Hangar	Taxyway	Pilot	Traffic controllers	MRO	Operators
METEO/ENVIRONMENTAL									
thunderstorms lighiting		X	X	X		X	X		
windshear						X			
icing, freezing		X	X		X	X	X		
snow		X	X	X	X	X	X		
heavy rain		X	X		X	X	X		
low visibility					X	X	X		
floads		X	X	X	X	X	X		
vulcanic ash		X	X	X	X	X	X		
Rapid fire spread, smoke/toxic gas buildup		X	X	X	X	X	X		X
Heat		X	X						
Cold		X	X						
Dryness									
Wetness	X	X	X						
Low friction (slipperiness)	X	X							
Glare						X	X		X
Darkness						X	X		X
Earthquake	X	X	X				X		X
Noise		X	X						
Engine emissions									
Electormagnetic field		X	X						

Generic hazards	Airframe	Propulsion System	Auxiliary Power Unit	Airframe Cart Interface	Airframe Sledge Interface	Data Handling System	COMM System	Landing/Take off GNC Rendevous with Sledge	Ground control station	Cart
HUMAN FACTORS										
Pilot's perception of a catastrophic failure										
Stress (sensory, mental, motor)										
Physical surroundings (environment)										
Illumination										
Vibration	X	X		X	X					X
Errors										
Omission										
Commission										
Nonrecognition of hazards										
Incorrect decisions										
Tasks done at wrong time (untimely)										
Tasks not performed or incorrectly performed										

Generic hazards	Cart Airframe Interface	Cart Sledge Interface	Facility to load cart on sledge	Facility to unload the cart from the sledge	Facility to transfer the aircraft from the cart on the sledge	Facility to transfer the aircraft from the sledge to the cart	Sledge	Sledge Cart Interface	Sledge Airframe Interface	Sledge Maglev Track Interface
HUMAN FACTORS										
Pilot's perception of a catastrophic failure										
Stress (sensory, mental, motor)										
Physical surroundings (environment)										
Illumination										
Vibration	X	X					X	X	X	X
Errors										
Omission										
Commission										
Nonrecognition of hazards										
Incorrect decisions										
Tasks done at wrong time (untimely)										
Tasks not performed or incorrectly performed										

Generic hazards	Runway	maglev track	Sledge Control System	Hangar	Taxyway	Pilot	Traffic controllers	MRO	Operators
HUMAN FACTORS									
Pilot's perception of a catastrophic failure						X			
Stress (sensory, mental, motor)						X	X		X
Physical surroundings (environment)						X	X		X
Illumination						X	X		X
Vibration		X	X						
Errors						X	X		X
Omission						X	X		X
Commission						X	X		X
Nonrecognition of hazards						X	X		X
Incorrect decisions						X	X		X
Tasks done at wrong time (untimely)						X	X		X
Tasks not performed or incorrectly performed						X	X		X

Hazard matrices for PHASE 4 - LANDING

Generic hazards	Airframe	Propulsion System	Auxiliary Power Unit	Airframe Cart Interface	Airframe Sledge Interface	Data Handling System	Communication System	Landing/ Take off GNC Rendevous with Sledge	Ground control station	Cart
BASIC DESIGN DEFICIENCIES										
Sharp corners				X	X					X
Instability (structural				X	X					X
Excessive weight				X	X					X
Inadequate clearance				X	X					X
Temperature										
Lack of accessibility										
Inadequate speed										
inadequate acceleration										
Inability to rotate due to incorrect center of gravity (CG) location, mistake in performance calculation, or flight control anomalies										

Generic hazards	Cart Airframe Interface	Cart Sledge Interface	Facility to load cart on sledge	Facility to unload the cart from the sledge	Facility to transfer the aircraft from the cart on the sledge	Facility to transfer the aircraft from the sledge to the cart	Sledge	Sledge Cart Interface	Sledge Airframe Interface	Sledge Maglev Track Interface
BASIC DESIGN DEFICIENCIES										
Sharp corners	X	X					X	X	X	
Instability (structural	X	X					X	X	X	X
Excessive weight	X	X					X	X	X	X
Inadequate clearance	X	X					X	X	X	X
Temperature										X
Lack of accessibility										
Inadequate speed							X			X
inadequate acceleration							X			X
Inability to rotate due to incorrect center of gravity (CG) location, mistake in performance calculation, or flight control anomalies										

Generic hazards	Runway	maglev track	Sledge Control System	Hangar	Taxyway	Pilot	Traffic controllers	MRO	Operators
BASIC DESIGN DEFICIENCIES									
Sharp corners									
Instability (structural	X	X							
Excessive weight									
Inadequate clearance		X							
Temperature		X	X						
Lack of accessibility									
Inadequate speed		X	X			X			X
inadequate acceleration		X	X			X			X
Inability to rotate due to incorrect center of gravity (CG) location, mistake in performance calculation, or flight control anomalies									

Generic hazards	Airframe	Propulsion System	Auxiliary Power Unit	Airframe Cart Interface	Airframe Sledge Interface	Data Handling System	Communication System	Landing/ Take off GNC Rendevous with Sledge	Ground control station	Cart
INHERENT HAZARDS										
Vertical kinetic energy	X			X	X			X	X	X
Horizontal kinetic energy	X			X	X			X	X	X
High mass and dynamic inertia	X			X	X			X	X	X
Mechanical (i.e., rotating equipment, vibration)		X	X	X	X					X
Electrical		X	X	X	X	X	X		X	X
Explosives										
Flammable gases or liquids		X	X							
Toxic substances										
Acceleration		X								
Deceleration		X								
Temperature		X	X							
Mechanical anomalies	X									X
Contaminated runways										
Crosswind				X	X					X
Runway, taxyway incursion						X	X		X	X

Generic hazards	Cart Airframe Interface	Cart Sledge Interface	Facility to load cart on sledge	Facility to unload the cart from the sledge	Facility to transfer the aircraft from the cart on the sledge	Facility to transfer the aircraft from the sledge to the cart	Sledge	Sledge Cart Interface	Sledge Airframe Interface	Sledge Maglev Track Interface
INHERENT HAZARDS										
Vertical kinetic energy	X	X					X	X	X	X
Horizontal kinetic energy	X	X					X	X	X	X
High mass and dynamic inertia	X	X					X	X	X	X
Mechanical (i.e., rotating equipment, vibration)	X	X					X	X	X	X
Electrical	X	X					X	X	X	X
Explosives										
Flammable gases or liquids										
Toxic substances										
Acceleration							X			X
Deceleration							X			X
Temperature										
Mechanical anomalies	X	X					X	X	X	X
Contaminated runways										X
Crosswind	X	X					X	X	X	X
Runway, taxyway incursion							X			X

Generic hazards	Runway	maglev track	Sledge Control System	Hangar	Taxyway	Pilot	Traffic controllers	MRO	Operators
INHERENT HAZARDS									
Vertical kinetic energy		X	X			X			X
Horizontal kinetic energy		X	X			X			X
High mass and dynamic inertia		X	X			X			X
Mechanical (i.e., rotating equipment, vibration)		X							
Electrical		X	X						X
Explosives									
Flammable gases or liquids									
Toxic substances									
Acceleration		X	X			X			X
Deceleration		X	X			X			X
Temperature									
Mechanical anomalies		X	X						
Contaminated runways	X	X	X						
Crosswind			X			X	X		
Runway, taxyway incursion		X	X			X	X		X

Generic hazards	Airframe	Propulsion System	Auxiliary Power Unit	Airframe Cart Interface	Airframe Sledge Interface	Data Handling System	Communi cation System	Landing/Tak e off GNC Rendevous with Sledge	Ground control station	Cart
MALFUNCTIONS										
Aircraft, cart untimely disconnection/connection				X						X
Aircraft, sledge untimely disconnection/connection				X	X					X
Cart, Sledge untimely disconnection/connection				X						X
Structural failures	X			X	X					X
Mechanical malfunctions	X	X		X	X					X
Electrical malfunctions		X		X	X	X	X	X	X	X
Power failures			X							
Missing synchronization between sledge and Aircraft		X				X	X	X		
Software failures		X		X	X	X	X	X	X	X
Software Hardware Interface Failures		X		X	X	X	X	X	X	
Man Machine Interface Failures		X		X	X	X	X	X	X	
Malicious attacks to system componenets (HW/SW)	X	X				X	X	X	X	X

Generic hazards	Cart Airframe Interface	Cart Sledge Interface	Facility to load cart on sledge	Facility to unload the cart from the sledge	Facility to transfer the aircraft from the cart on the sledge	Facility to transfer the aircraft from the sledge to the cart	Sledge	Sledge Cart Interface	Sledge Airframe Interface	Sledge Maglev Track Interface
MALFUNCTIONS										
Aircraft, cart untimely disconnection/connection	X	X					X	X		X
Aircraft, sledge untimely disconnection/connection	X	X					X	X	X	X
Cart, Sledge untimely disconnection/connection	X	X					X	X		X
Structural failures	X	X					X	X	X	X
Mechanical malfunctions	X	X					X	X	X	X
Electrical malfunctions	X	X					X	X	X	X
Power failures										X
Missing synchronization between sledge and Aircraft										X
Software failures	X	X					X	X	X	X
Software Hardware Interface Failures	X	X						X	X	X
Man Machine Interface Failures	X	X						X	X	X
Malicious attacks to system componenets (HW/SW)			X	X	X	X				

Generic hazards	Runway	maglev track	Sledge Control System	Hangar	Taxyway	Pilot	Traffic controllers	MRO	Operators
MALFUNCTIONS									
Aircraft, cart untimely disconnection/connection						X	X		X
Aircraft, sledge untimely disconnection/connection						X	X		X
Cart, Sledge untimely disconnection/connection						X	X		X
Structural failures	X	X							
Mechanical malfunctions		X	X						
Electrical malfunctions		X	X						
Power failures		X	X						
Missing synchronization between sledge and Aircraft		X	X			X	X		X
Software failures		X	X						
Software Hardware Interface Failures		X	X			X	X		X
Man Machine Interface Failures		X	X			X	X		X
Malicious attacks to system componenets (HW/SW)		X	X	X	X				

Generic hazards	Airframe	Propulsion System	Auxiliary Power Unit	Airframe Cart Interface	Airframe Sledge Interface	Data Handling System	Communication System	Landing/Take off GNC Rendevous with Sledge	Ground control station	Cart
METEO/ENVIRONMENTAL										
thunderstorms lighiting	X	X	X	X	X					X
windshear										
icing, freezing	X	X		X	X					X
snow	X	X		X	X					X
heavy rain		X		X	X					X
low visibility										
floads	X	X	X	X	X					X
vulcanic ash	X	X	X	X	X					X
Rapid fire spread, smoke/toxic gas buildup	X	X	X	X	X					X
Heat										
Cold				X	X					X
Dryness										
Wetness		X		X	X					X
Low friction (slipperiness)										
Glare										
Darkness										
Earthquake										
Noise	X	X	X	X	X					X
Engine emissions		X	X							
Electormagnetic field										

Generic hazards	Cart Airframe Interface	Cart Sledge Interface	Facility to load cart on sledge	Facility to unload the cart from the sledge	Facility to transfer the aircraft from the cart on the sledge	Facility to transfer the aircraft from the sledge to the cart	Sledge	Sledge Cart Interface	Sledge Airframe Interface	Sledge Maglev Track Interface
METEO/ENVIRONMENTAL										
thunderstorms lighiting	X	X	X	X	X	X	X	X	X	X
windshear										
icing, freezing	X	X	X	X	X	X	X	X	X	X
snow	X	X	X	X	X	X	X	X	X	X
heavy rain	X	X	X	X	X	X	X	X	X	X
low visibility										
floads	X	X	X	X	X	X	X	X	X	X
vulcanic ash	X	X	X	X	X	X	X	X	X	X
Rapid fire spread, smoke/toxic gas buildup	X	X	X	X	X	X	X	X	X	X
Heat										X
Cold	X	X					X	X	X	X
Dryness										
Wetness	X	X					X	X	X	X
Low friction (slipperiness)										X
Glare										
Darkness										
Earthquake										X
Noise	X	X	X	X	X	X	X	X	X	X
Engine emissions										
Electormagnetic field							X			

Generic hazards	Runway	maglev track	Sledge Control System	Hangar	Taxyway	Pilot	Traffic controllers	MRO	Operators
METEO/ENVIRONMENTAL									
thunderstorms lighiting		X	X	X		X	X		
windshear						X			
icing, freezing		X	X		X	X			
snow		X	X	X	X	X			
heavy rain		X	X		X	X			
low visibility					X	X	X		
floads		X	X	X	X		X		
vulcanic ash		X	X	X	X		X		
Rapid fire spread, smoke/toxic gas buildup		X	X	X	X		X		
Heat		X	X						
Cold	X	X	X						
Dryness									
Wetness	X	X	X						
Low friction (slipperiness)	X	X	X						
Glare						X	X		X
Darkness						X	X		X
Earthquake	X	X	X				X		
Noise	X	X	X						
Engine emissions						X			
Electormagnetic field		X	X			X			

Generic hazards	Airframe	Propulsion System	Auxiliary Power Unit	Airframe Cart Interface	Airframe Sledge Interface	Data Handling System	Communication System	Landing/Take off GNC Rendevous with Sledge	Ground control station	Cart
HUMAN FACTORS										
Pilot's perception of a catastrophic failure										
Stress (sensory, mental, motor)										
Physical surroundings (environment)										
Illumination										
Vibration	X	X			X					X
Errors										
Omission										
Commission										
Nonrecognition of hazards										
Incorrect decisions										
Tasks done at wrong time (untimely)										
Tasks not performed or incorrectly performed										

Generic hazards	Cart Airframe Interface	Cart Sledge Interface	Facility to load cart on sledge	Facility to unload the cart from the sledge	Facility to transfer the aircraft from the cart on the sledge	Facility to transfer the aircraft from the sledge to the cart	Sledge	Sledge Cart Interface	Sledge Airframe Interface	Sledge Maglev Track Interface
HUMAN FACTORS										
Pilot's perception of a catastrophic failure										
Stress (sensory, mental, motor)										
Physical surroundings (environment)										
Illumination										
Vibration	X	X					X	X	X	X
Errors										
Omission										
Commission										
Nonrecognition of hazards										
Incorrect decisions										
Tasks done at wrong time (untimely)										
Tasks not performed or incorrectly performed										

Generic hazards	Runway	maglev track	Sledge Control System	Hangar	Taxyway	Pilot	Traffic controllers	MRO	Operators
HUMAN FACTORS									
Pilot's perception of a catastrophic failure						X			
Stress (sensory, mental, motor)						X	X		X
Physical surroundings (environment)						X	X		X
Illumination	X					X	X		X
Vibration	X	X	X						
Errors						X	X		X
Omission						X	X		X
Commission						X	X		X
Nonrecognition of hazards						X	X		X
Incorrect decisions						X	X		X
Tasks done at wrong time (untimely)						X	X		X
Tasks not performed or incorrectly performed						X	X		X

8.4 Hazard Scenarios

The next step of the Framework requires to define the hazard scenarios associated with the hazard manifestations by identifying the causes, events and safety consequences.
According to the current maturity of the system concepts, the analysis proceeds with:

- the preliminary functional FMEA for each safety critical function in each phase,
- the cause determination, choosing among hazards the ones which may represent initiator events for the functional failures,
- the identification of the propagation of events from functional failure mode to the consequences/effects together with a preliminary qualitative severity categorization,
- some considerations about the requirements for the system components.

In the current preliminary step of safety assessment, the most critical phases and most critical related functions are identified on the basis of the previous hazard manifestation list.
The most critical phases to focus on are: take-off and landing.
Anyhow, most of the hazard scenarios are common to the classical TOL technology and it has no use to focus on them in this stage of the project.
This preliminary safety assessment of the most critical phases has a twofold objective: to perform a preliminary trade off analysis between two identified system configurations, to trace the critical scenarios and involved components for further developments.
In building the safety scenarios for each phase, among the identified hazards, the ones which could lead to a degradation of the functions whose effects are critical for life, environment, and systems have been analysed.
For both of the considered phases, the most critical functions have been chosen considering their failure modes' impact and for the failure modes the ones with the worst case effects have been analysed.
This approach leads to identify the most critical components in the system to care about (e.g. whose reliability has to be properly assured).
Provided that there is a share of responsibilities among all the system components the emphasis has been put on the innovative equipment's and on their contribution to increase the hazards' occurrences or severity.
The following functions:

- ❖ F3.11 : to respect the air traffic controllers orders
- ❖ F4.2 : to respect the sequence provided by the air traffic controllers
- ❖ F4.10 : to free the A/C or cart from the sledge (unloading A/C or cart form sledge)

- corresponding to scenarios 10, 12, 20, - are mostly related to the "Human factors" Pilot, Traffic Controllers, Operators, Maintenance, Repair and Overhaul (MRO) personnel.
For these functions (scenarios) all the command chains must have adequate reliability possibly involving fail safe mechanisms. The related operations have to be supported by detection and checking mechanisms, rigorous testing and where necessary redundancies should be foreseen.

For take-off the critical functions are considered in the followings.

SCENARIO-1

- F3.1 to secure the A/C or cart position on the sledge (Loading A/C/cart on cart/sledge)

- F3.1 Functional failure mode
  - unstable position

- Functional failure mode effect
  - Local effect of the function failure modes: unsecure connection
  - End effect: Untimely separation and fall down

- **Severity**
  - Hazardous

Initiator Events - Hazards

- High/Low Pressure in hydraulic systems (actuators, dampers)
- Electrical malfunctions
- Acceleration
- Deceleration
- Mechanical anomalies
- Aircraft, cart untimely disconnection/connection
- Aircraft, sledge untimely disconnection/connection
- Cart, Sledge untimely disconnection/connection
- Structural failures
- Mechanical malfunctions
- Electrical malfunctions
- Power failures
- Software failures
- Software Hardware Interface Failures
- Man Machine Interface Failures
- Malicious attacks to system components (HW/SW)
- Incorrect decisions
- Tasks done at wrong time (untimely)
- Tasks not performed or incorrectly performed

- **Components**
  - Airframe Cart Interface
  - Airframe Sledge Interface
  - Data Handling System

- Communication System
- Cart
- Cart Airframe Interface
- Cart Sledge Interface
- Sledge
- Sledge Cart Interface
- Sledge Airframe Interface
- Sledge Control System
- Operators

❖ **Preliminary Safety Requirements**

Fail safe for: Lock operations, lock equipment, lock data handling

SCENARIO-2

FFMEA

❖ F3.2 to accelerate to the desired speed meeting passengers constraints

❖ Functional failure mode

- F3.2 to accelerate to inadequate speed meeting passengers constraints
- F3.2 to accelerate to inadequate speed violating passengers constraints
- F3.2 to accelerate to the desired speed violating passengers constraints

❖ Functional failure mode effect

- Insufficient speed
- Over speed
- End Effect: passenger trouble, abort take-off

❖ **Severity**

- Hazardous

Initiator Events - Hazards:

- Excessive weight
- Inadequate thrust
- High mass and dynamic inertia
- Electrical malfunctions
- Pilot's perception of a catastrophic failure
- Stress (sensory, mental, motor)

- Physical surroundings (environment)
- Errors
- Omission
- Commission
- No recognition of hazards (over limit acceleration)
- Incorrect decisions
- Tasks done at wrong time (untimely)
- Tasks not performed or incorrectly performed
- Mechanical malfunctions
- Electrical malfunctions
- Power failures
- Software failures
- Software Hardware Interface Failures
- Man Machine Interface Failures
- Malicious attacks to system components (HW/SW)

❖ **Components**

- Propulsion system
- Data Handling System
- Sledge
- Runway
- Maglev track
- Sledge Control System
- Pilot

❖ **Preliminary Safety Requirements**

- Weight budget estimation of the flight segment components
- Dimensions of the maglev systems
- Instrumentation panel

SCENARIO-3

FFMEA

- Function : F3.4 to decide about the continuation of the take-off phase

- Functional failure mode
  - F3.4 wrong decision to abort take off
  - F3.4 wrong decision to take off
  - F3.4 inability to decide

- Functional failure mode effect

  End Effect
  - Wrong decision 1: Unjustified Abort take off and Unsafe abort take off
  - Wrong decision 2: Take off and unsafe take off

- **Severity**
  - Catastrophic

Initiator Events - Hazards

- Inadequate clearance
- Mechanical anomalies
- Contaminated runways
- Crosswind
- Runway, taxiway incursion
- Aircraft, cart untimely disconnection/connection
- Aircraft, sledge untimely disconnection/connection
- Cart, Sledge untimely disconnection/connection
- Structural failures
- Mechanical malfunctions
- Electrical malfunctions
- Power failures
- Software failures
- Software Hardware Interface Failures
- Man Machine Interface Failures

Components

- Data Handling System
- Communication System
- Pilot
- Traffic controllers

Preliminary Safety Requirements

- Human factors
- Detection failure
- Communication failure
- Data Handling system

SCENARIO-4

FFMEA

❖ Function F3.5 to control the separation between the aircraft and the cart

❖ Functional failure mode
- F3.5 separation command failure (delayed or not actuated)
- F3.5 inadvertent separation

❖ Functional failure mode effect
- End Effect : Inadvertent/ untimely separation and fall down/crash/collision

❖ **Severity**
- Catastrophic

Initiator Events - Hazards
- Horizontal kinetic energy
- High mass and dynamic inertia
- Mechanical (i.e., rotating equipment, vibration)
- Electrical
- Aircraft, cart untimely disconnection/connection
- Pilot's perception of a catastrophic failure
- Stress (sensory, mental, motor)
- Physical surroundings (environment)
- Illumination
- Vibration
- Errors
- Omission
- Commission
- Non recognition of hazards
- Incorrect decisions
- Tasks done at wrong time (untimely)
- Tasks not performed or incorrectly performed
- Components

Components

- Airframe
- Cart Interface
- Airframe Sledge Interface
- Data Handling System
- Communication System
- Landing/Take off GNC
- Rendezvous with Sledge
- Cart Airframe Interface
- Cart Sledge Interface
- Sledge Cart Interface
- Sledge Airframe Interface
- Sledge Maglev Track Interface
- Sledge Control System
- Pilot
- Operators

Preliminary Safety Requirements

- Fail safe Separation devices and separation controls

SCENARIO-5

FFMEA

❖ Function F3.6 to enable the minimum climb slope and speed for take off

❖ Functional failure mode

- F3.6 Unable to reach the minimum climb slope and speed for take off

❖ Functional failure mode effect

End Effect : Collision, Crash

❖ **Severity**

- Catastrophic

Initiator Events- Hazards

- Excessive weight
- Inadequate speed
- inadequate acceleration
- Inability to rotate due to incorrect centre of gravity (CG) location, mistake in performance calculation, or flight control anomalies
- Acceleration
- Deceleration
- Mechanical anomalies

- Contaminated runways
- Crosswind
- Runway, taxiway incursion
- Aircraft, cart untimely disconnection/connection
- Aircraft, sledge untimely disconnection/connection
- Cart, Sledge untimely disconnection/connection
- Mechanical malfunctions
- Electrical malfunctions
- Power failures
- Software failures
- Software Hardware Interface Failures
- Man Machine Interface Failures
- Malicious attacks to system componenets (HW/SW)
- wind shear
- icing, freezing
- snow
- heavy rain
- floods
- volcanic ash
- Pilot's perception of a catastrophic failure
- Stress
- Omission
- Non recognition of hazards
- Incorrect decisions
- Tasks done at wrong time (untimely)
- Tasks not performed or incorrectly performed

Components

- Propulsion System
- Airframe Cart Interface
- Airframe Sledge Interface
- Data Handling System
- COMM System
- Landing/Take off GNC
- Ground control station
- Cart Airframe Interface
- Cart Sledge Interface
- Sledge
- Sledge Cart Interface
- Sledge Airframe Interface
- Sledge Maglev Track Interface

- Maglev track
- Sledge Control System
- Pilot
- Operators

Preliminary Safety Requirements

- "Acceleration chain" command and detection

SCENARIO-6

FFMEA

❖ Function F3.7 to free the take-off zone for the next aircraft

❖ Functional failure mode
  - F3.7 Unable to free the take-off zone for the next A/C

❖ Functional failure mode effect
  - Slowdown of operations

❖ **Severity**
  - Major

Initiator Events- Hazards

- Mechanical anomalies
- Contaminated runways
- Runway, taxiway incursion
- Aircraft, cart untimely disconnection/connection
- Aircraft, sledge untimely disconnection/connection
- Cart, Sledge untimely disconnection/connection
- Mechanical malfunctions
- Electrical malfunctions
- Power failures
- Software failures
- Software Hardware Interface Failures
- Man Machine Interface Failures
- Malicious attacks to system components (HW/SW)
- snow
- floods
- volcanic ash
- Pilot's perception of a catastrophic failure

- Stress
- Omission
- Non recognition of hazards
- Incorrect decisions
- Tasks done at wrong time (untimely)
- Tasks not performed or incorrectly performed

Components

- Airframe Cart Interface
- Airframe Sledge Interface
- Data Handling System
- COMM System
- Ground control station
- Cart Airframe Interface
- Cart Sledge Interface
- Sledge
- Sledge Cart Interface
- Sledge Airframe Interface
- Sledge Maglev Track Interface
- Maglev track
- Sledge Control System
- Pilot
- Operators

Preliminary Safety Requirements

- To design and properly test the related operations (adequate reliability)

SCENARIO-7

FFMEA

- Function F3.8 : to remain within the flight envelope

- Functional failure mode
  - F3.8 Large acceleration on sledge, too large over speed, too large deceleration (see F 3.2)

- Functional failure mode effect
  - Aerostructure failure

- **Severity**
  - Catastrophic

Initiator Events - Hazards:

- Excessive weight
- Inadequate thrust
- High mass and dynamic inertia
- Electrical malfunctions
- Pilot's perception of a catastrophic failure
- Stress (sensory, mental, motor)
- Physical surroundings (environment)
- Errors
- Omission
- Commission
- No recognition of hazards (over limit acceleration)
- Incorrect decisions
- Tasks done at wrong time (untimely)
- Tasks not performed or incorrectly performed
- Mechanical malfunctions
- Electrical malfunctions
- Power failures
- Software failures
- Software Hardware Interface Failures
- Man Machine Interface Failures

Malicious attacks to system components (HW/SW)

- **Components**
  - Propulsion system
  - Data Handling System
  - Sledge
  - Runway

- maglev track
- Sledge Control System
- Pilot

❖ **Preliminary Safety Requirements**

- Weight budget estimation of the flight segment components
- Dimensions of the maglev systems
- Instrumentation panel
- Fail safe involved components and operations

SCENARIO-8

FFMEA

❖ Function F3.9 to maintain the minimum climb slope (OEI condition included)

Provided the aircraft will reach the necessary acceleration it is a classical issue, not specific of maglev

SCENARIO-9

FFMEA

❖ Function F3.10 : to maintain the necessary speed (*after rotation*)

Provided the aircraft will reach the necessary acceleration it is a classical issue, not specific of maglev

For landing the critical functions are considered in the following.

SCENARIO-11

FFMEA

❖ Function : F4.1 to synchronize the rendez-vous between the aircraft and the Cart/Sledge system

❖ Function Failure mode

- F4.1 undetected rendezvous failure
- F4.1 detected rendezvous failure

❖ Functional failure mode effect

- End Effect :
  - Catastrophic Landing

❖ Emergency landing (with or without touch down)

❖ **Severity**

- Catastrophic

Initiator Events - Hazards

- Sledge cannot accelerate
- Missing synchronization between Sledge and Aircraft
- Software failures (related to rendezvous)
- Software Hardware Interface Failures
- Man Machine Interface Failures

Components

- Sledge
- Cart
- Landing/Take off GNC
- Rendezvous with Sledge
- Sensors for rendezvous
- Pilot
- Traffic controller
- Operators
- Data Handling system
- Communication system
- Ground control station
- Cart Airframe Interface
- Cart Sledge Interface
- Sledge
- Sledge Cart Interface
- Sledge Airframe Interface
- Sledge Maglev Track Interface
- Sledge Control System
- Maglev track

Preliminary Safety Requirements

- High reliability for Rendezvous related systems
- Fail safe aircraft sledge/cart connection (able to connect the aircraft to sledge even in case of low precision rendezvous

SCENARIO-13FFMEA

❖ Function F4.3: to reach the final approach zone

It is not specifically related to the maglev technology

SCENARIO-14

FFMEA

❖ Function F4.4: to align the aircraft in the landing axis (trajectory)

❖ Function Failure Mode

- F4.4 detected wrong alignment
- F4.4 undetected wrong alignment

❖ Functional failure mode effect

- End Effects :
  - Abort landing (with or without touch down)
  - Catastrophic landing

❖ **Severity**

- Hazardous

Initiator Events - Hazards

- Inadequate speed
- inadequate acceleration
- Crosswind
- Software failures (related to rendezvous and its components: INS, GPS, ...)
- Software Hardware Interface Failures
- Man Machine Interface Failures
- Malicious attacks to system components SW

Components

- Data Handling System
- Communication System
- Landing/Take off GNC
- Rendezvous with Sledge
- Ground control station
- Sledge Control System
- Pilot
- Traffic controllers
- Operators

Preliminary Safety Requirements

The misalignment between aircraft and sledge can be in width and/or in side angle.
The resulting requirement might be on a moving (in width) and rotating sledge.
The alternative requirement might be on a smart sledge/cart-aircraft interface able to connect the two systems also in case of misalignment.

SCENARIO-15

FFMEA

❖ Function F4.5 : to absorb the potential/dynamic energy of the aircraft

❖ Functional failure mode

- F4.5 to fail absorbing the potential/dynamic energy of the aircraft

❖ Functional failure mode effect
- End Effect: Crash, Collision

❖ **Severity**
- Hazardous

Initiator Events - Hazards
- Excessive weight
- Inadequate speed
- inadequate acceleration
- Vertical kinetic energy
- Horizontal kinetic energy
- High mass and dynamic inertia
- Mechanical (i.e., rotating equipment, vibration)
- Structural failures
- Missing synchronization between maglev systems and Aircraft

Components
- Airframe
- Airframe Cart Interface
- Airframe Sledge Interface
- Data Handling System
- Communication System
- Landing/Take off GNC
- Rendezvous with Sledge
- Ground control station
- Cart
- Cart Airframe Interface
- Cart Sledge Interface
- Sledge
- Runway
- Maglev track
- Sledge Control System
- Pilot

Preliminary Safety Requirements

Requirements for:
- Max vertical speed of A/C
- rendezvous system,
- airframe/cart/sledge structure,
- cart/sledge absorbing springs and dumpers,

- landing position and attitude,
- weight,
- approach speed.

SCENARIO- 16

FFMEA

❖ Function F4.6: to ensure and control the connection between the aircraft and the cart

❖ Functional Failure Mode
- F4.6 to miss the right connection between the aircraft and the cart
- F4.6 to lose the connection between the aircraft and the cart

❖ Functional failure mode effect
- End effect: Airframe collisions and fall down

❖ **Severity**
- Hazardous

Initiator Events - Hazards
- Instability
- Excessive weight
- Wind-shear
- icing, freezing
- snow
- floods
- Mechanical (i.e., rotating equipment, vibration)
- Electrical
- Mechanical anomalies
- Aircraft, cart untimely disconnection/connection
- Aircraft, sledge untimely disconnection/connection
- Cart, Sledge untimely disconnection/connection
- Structural failures
- Mechanical malfunctions
- Electrical malfunctions
- Power failures
- Missing synchronization between sledge and Aircraft
- Software failures (related to rendezvous)
- Software Hardware Interface Failures
- Man Machine Interface Failures
- Pilot's perception of a catastrophic failure

- Stress (sensory, mental, motor)

Components

- Airframe
- Airframe Cart Interface
- Airframe Sledge Interface
- Data Handling System
- Landing/Take off GNC
- Rendezvous with Sledge
- Ground control station
- Cart
- Cart Airframe Interface
- Cart Sledge Interface
- Sledge
- Sledge Cart Interface
- Sledge Airframe Interface
- Sledge Maglev Track Interface
- Sledge Control System
- Pilot

Preliminary Safety Requirements

Strict requirements for the relevant components to ensure and control the connection between airframe and cart/sledge.

SCENARIO-17

FFMEA

- ❖ Function F4.7: to lock the aircraft on the cart/sledge
- ❖ Functional Failure Mode
  - F4.7 undetected lock failure
  - F4.7 detected lock failure

- ❖ Functional failure mode effect
  - Effect: Fall down, collision
- ❖ **Severity**
  - Hazardous

Initiator Events Hazards

- Aircraft, cart untimely disconnection/connection
- Aircraft, sledge untimely disconnection/connection
- Cart, Sledge untimely disconnection/connection
- Structural failures
- Mechanical malfunctions
- Electrical malfunctions
- Power failures
- Missing synchronization between sledge and Aircraft
- Software failures (related to rendezvous)
- Software Hardware Interface Failures
- Man Machine Interface Failures
- Malicious attacks to system components (HW/SW)

Components

- Airframe Cart Interface
- Airframe Sledge Interface
- Data Handling System
- Cart
- Cart Airframe Interface
- Cart Sledge Interface
- Sledge
- Sledge Cart Interface
- Sledge Airframe Interface
- Sledge Maglev Track Interface
- Operators

Preliminary Safety Requirements

- Airframe Maglev System interfaces and connections,
- connection sensors,

- mechanical devices/connections
- Electrical components
- data handling systems
- operations

SCENARIO-18

FFMEA

❖ Function F4.8: to decelerate

❖ Functional Failure Mode
- F4.8 inability to properly reduce speed

❖ Functional failure mode effect
- End effects: Collisions

❖ **Severity**
- Hazardous

Initiator Events - Hazards
- Inadequate speed
- inadequate acceleration
- Inability to rotate due to incorrect centre of gravity (CG) location, mistake in performance calculation, or flight control anomalies
- Vertical kinetic energy
- Horizontal kinetic energy
- High mass and dynamic inertia
- Mechanical malfunctions
- Electrical malfunctions
- Power failures
- Pilot's perception of a catastrophic failure
- Stress (sensory, mental, motor)
- Non recognition of hazards
- Incorrect decisions
- Tasks done at wrong time (untimely)
- Tasks not performed or incorrectly performed

Components

- Airframe
- Propulsion System
- Data Handling System
- Communication System
- Ground control station
- Cart
- Sledge
- Maglev track
- Sledge Control System
- Pilot

Preliminary Safety Requirements

- the length of the runway and track,
- the maglev braking system,
- the instrument panel,
- proper use of aerodynamic braking systems in conjunction with maglev deceleration

SCENARIO-19

FFMEA

❖ Function F4.9 : to minimize environmental impact (noise and emissions)
Not safety critical

❖ Functional Failure Mode

- F4.9 to exceed noise limits
- F4.9 to exceed emission limits

❖ Functional failure mode effect

- exceed noise emission regulation

❖ **Severity**

- Minor

Initiator Events - Hazards

❖ Inadequate speed
❖ inadequate acceleration
❖ Electrical malfunctions
❖ Power failures
❖ Software failures
❖ Software Hardware Interface Failures
❖ Man Machine Interface Failures
❖ Malicious attacks to system components (HW/SW)

Components

- Airframe
- Propulsion System
- Airframe Cart Interface
- Airframe Sledge Interface
- Cart
- Cart Airframe Interface
- Cart Sledge Interface
- Sledge
- Sledge Cart Interface
- Sledge Airframe Interface
- Sledge Maglev Track Interface
- Sledge Control System

Preliminary Safety Requirements

- Maglev system (in case of maglev failure the Aircraft/sledge should be free to accelerate exploiting the Aircraft propulsion thrust)
- Sledge Control System,

SCENARIO-21

❖ **FFMEA**

❖ F4.11 to enable the cart to roll on the runway with the aircraft

❖ Functional Failure Mode
  - rigid connection between A/C and Cart/sledge

❖ Functional failure mode effect
  - Missed A/C cart/sledge connection

❖ Severity
  - Major

Initiator Events - Hazards

- High/Low Pressure in hydraulic systems (actuators, dampers)
- Electrical malfunctions
- Mechanical anomalies
- Structural failures
- Mechanical malfunctions
- Electrical malfunctions
- Power failures
- Software failures
- Software Hardware Interface Failures

- Man Machine Interface Failures
- Malicious attacks to system components (HW/SW)
- Incorrect decisions

❖ **Components**

- Airframe Cart Interface
- Airframe Sledge Interface
- Data Handling System
- Communication System
- Cart
- Cart Airframe Interface
- Cart Sledge Interface
- Sledge
- Sledge Cart Interface
- Sledge Airframe Interface
- Sledge Control System
- Operators

❖ **Preliminary Safety Requirements**

Fail safe for:

- Cart/sledge roll mechanism
- Lock operations,
- lock equipment,
- lock data handling

In the following two synthetic tables show the FMEA results for take-off and landing phases.

PHASE 3 - TAKE OFF

Function	Failure mode	Failure mode effect	Severity
F3.1 to secure the A/C or cart position on the sledge (Loading A/C/cart on cart/sledge)	unstable position	Local effect of the function failure modes: unsecure connection End effect: Untimely separation and fall down	Hazardous
F3.2 to accelerate to the desired speed meeting passengers constraints	F3.2 to accelerate to inadequate speed meeting passengers constraints F3.2 to accelerate to inadequate speed violating passengers constraints F3.2 to accelerate to the desired speed violating passengers constraints	Insufficient speed, Over speed End Effect: passenger trouble, abort take-off	Hazardous
F3.3 to guide and control the trajectory	N.A. (trajectory controlled by sledge and maglev track)		
F3.4 to decide about the continuation of the take-off phase	F3.4 wrong decision to abort take off F3.4 wrong decision to take off F3.4 inability to decide	Wrong decision 1: Unjustified Abort take off and Unsafe abort take off Wrong decision 2: Take off and unsafe take off	Catastrophic
F3.5 to control the separation between the aircraft and the cart	F3.5 separation command failure (delayed or not actuated) F3.5 inadvertent separation	Inadvertent/ untimely separation and fall down/crash/collision	Catastrophic

Function	Failure mode	Failure mode effect	Severity
F3.6 to enable the minimum slope and speed for take off	Unable to reach the minimum climb slope and speed for take off	Collision, Crash	Catastrophic
F3.7 to free the take-off zone for the next aircraft	Unable to free the take-off zone for the next A/C	Slowdown of operations	Major
F3.8 to remain within the flight envelope	Large acceleration on sledge, too large over speed, too large deceleration (see F 3.2)	Aero structure failure	Catastrophic
F3.9 to maintain the minimum climb slope (OEI condition included)	Provided the aircraft will reach the necessary acceleration it is a classical issue, not specific of maglev		

PHASE 4 LANDING

Function	Failure mode	Failure mode effect	Severity
F4.1 to synchronize the rendezvous between the aircraft and the composite system in a defined area	F4.1 undetected rendezvous failure F4.1 detected rendezvous failure	Catastrophic Landing Emergency landing (with or without touch down)	Catastrophic
F4.3 to reach the final approach zone	It is not specifically related to the maglev technology		
F4.4 to align the aircraft in the landing axis (trajectory)	F4.4 detected wrong alignment F4.4 undetected wrong alignment	Abort landing (with or without touch down) Catastrophic landing	Hazardous
F4.5 to absorb the potential energy of the aircraft	to fail absorbing the potential energy of the aircraft	Crash, Collision	Hazardous
F4.6 to ensure and control the contact between the aircraft and the cart	to miss the right connection between the aircraft and the cart to lose the connection between the aircraft and the cart	Airframe collisions and fall down	Hazardous
F4.7 to lock the aircraft on the cart	undetected lock failure detected lock failure	Fall down, collision	Hazardous
F4.8 to decelerate	inability to properly reduce speed	Collision	Hazardous
F4.9 to minimize environmental impact	to exceed noise limits to exceed emission limits	exceed noise emission regulation	Minor
F4.10 to free the A/C or cart from the sledge (unloading A/C or cart form sledge)	Less critical leads to operational implications		Minor
F4.11 to enable the cart to roll on the runway with the aircraft	rigid connection between A/C and Cart/sledge	Missed A/C cart/sledge connection	Major

9 ITERATION OF THE RISK FRAMEWORK APPLICATION

The prosed risk framework can be iteratively applied to further specified design options, to properly detail component requirements.

As the design phase has produced a new design option for the Ground Based System (GBS), a system product tree for the GBS has been developed together with a functional analysis. They are shown and described in section 10.1 and 10.2.

The hazard list has been updated and specialised to new GBS concept, a FFMEA (functional failure mode effect analysis) has been performed for the GBS Functions, considering those hazards which represent initiating events for them.

The identification of the CIL (Critical Item List) for the GBS is derived and provided in paragraph 11.4 while the preliminary requirement list for the GBS is shown in paragraph 11.5.

The case study Ground Based System design has been inspired by the corresponding GBS in the railway domain.

Maglev technology historical data records belong to the railway domain and a primary lesson learned from the accidents in the railway domain is the importance of risk/hazard analysis that can qualitatively focus on the severity of accidents and human factors.

These findings are not entirely consistent with current actual practices based on international railway standards; they rather conform well to the fundamentals of System Safety, which is an organized and established method to assure safety in complex systems.

The adopted approach completely matches the fundamentals of System Safety, as already stated.

The adopted approach provides a reference framework for future developments for the Ground Based System design. Related topic areas include: levitation, propulsion, energy and control systems, loads, vehicle and guide-way stability, design, production and quality assurance of mechanical structures, switches, lightning protection, electromagnetic compatibility, electrostatic discharge, fire protection and rescue plan.

10 GABRIEL GROUND BASED SYSTEM

10.1 GBS product tree

LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5
0 GROUND BASED SYSTEM	1 INFRASTRUCTURE	11 OPERATION / MAINTENANCE CENTER		
		12 SUBSTATION / CONTROL CENTER BUILDING		
		13 SWITCH GEAR CABINETS		
		14 DATA TRANSMISSION		
	2 GUIDEWAY	21 CUTTINGS		
		22 FOUNDATIONS		
		23 PILLERS		
		24 BEARINGS		
		25 GIRDERS		
		26 RECTION RAILS		
		27 BRAKING RAILS		
		28 RAILS FOR WHEELS		
		29 POSITION INDICATORS		
		210 CABLE TRENCHES		
	3 PROPULSION	31 SUPPLY CABLE SYSTEMS		
		32 SWITCHING STATIONS		
		33 STATOR PACKS GUIDEWAYSIDE		
		34 CABLE WINDINGS GUIDEWAYSIDE		
		35 ELECTRICAL CONNECTIONS		
		36 PROTECTION EQUIPMENT		

LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5
0 GROUND BASED SYSTEM	4 POWER CHAIN	41 INCOMING FEEDER		
		42 110 kV SWITCHING GEAR		
		43 HIGH VOLTAGE TRANSFORMERS		
		44 20 kV SWITCHGEAR		
		45 CONVERTER UNITS	451 TRANSFORMER	
			452 RECTIFIER	
			453 DC-LINK	
			454 INVERTER	4541 ENCLOSURE
				4542 POWER ELECTRONICS
				4543 CONTROL ELECTRONICS
				4544 MEASURING DEVICE
				4545 PROTECTION
				4546 COOLING DUCTS
				4547 ELECTRICAL CONNECTIONS
			455 CONNECTIONS	
			456 COOLING	
		46 REACTIVE POWER COMPENSATION		
		47 6 kV SWITCHGEAR		
		48 AUXILIARY VOLTAGE		
		49 OUTGOING SWITCHGEAR		

LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5
0 GROUND BASED SYSTEM	5 SLEDGE	51 STRUCTURE		
		52 CART FIXATION	521 LOCKING MECHANISM	
			522 FLIP-UP PANELS	
		53 LEVITATION FRAMES	531 STRUCTURE	
			532 SPRINGS / DAMPERS	
			533 LEVITATION MAGNETS	
			534 PROPULSION MAGNETS	
			535 UNDERCARRIAGE	
			536 EMERGENCY BRAKES	
			537 AUXILIARY WHEELS	
			538 LOCATING	
			539 DATA TRANSMISSION	

LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5
0 GROUND BASED SYSTEM	5 SLEDGE	54 RENDEZ-VOUS CONTROL	541 SLEDGE LONGITUDINAL CONTROL	
			542 SLEDGE PITCH CONTROL	
			543 SLEDGE YAW CONTROL	
			544 SENSORS OF SLEDGE CONTROL	5441 GROUND SPEED
				5443 PALTFORM YAW AND PITCH ANGLE
				5443 VELOCITY AND ACCELERATION
				5444 POSITION
				5445 GROUND CONNECTION STATUS
			545 SENSORS OF AIRCRAFT CONTROL	5451 PITCH ATTITUDE AND RATE
				5452 PITCH, ROLL AND YAW ANGLE
				5453 FLIGHT PATH, BANK, SLIDESLIP, TRACK ANGLE
				5454 AIR- AND GROUNDSPEED
				5455 ALTITUDE
				5456 LONGITUDINAL AND LATERAL POSITION
			546 RENDEZ-VOUS CONTROL MONITORING SYSTEM	
		55 ROTATIONAL PLATFORM	551 BEARINGS	
			551 ACTUATORS	
			551 HYDRAULICS	

LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5
	6 CART	61 STRUCTURE		
		62 UNDERCARRIAGE		
		63 PROPULSION		
		64 ENERGY SUPPY		
		65 AIRCRAFT FIXATION	651 HARPOON GRID	
			652 ADAPTED FIFTH WHEEL	
		66 SPRING DAMPER COMBINATION		
		67 PITCH MECHANISM	671 ACTUATORS	
			672 HYDRAULICS	
		68 CART CONTROL SYSTEM FOR REMOTE CONTROL (OPTIONAL)		
		69 BALLOONS (OPTIONAL)		
	7 MAGLEV CONTROL CENTER	71 SIGNALLING / DATA TRANSMISSION		
		72 PROPULSION CONTROL		
		73 CONTROL / SUPERVISION		
		74 SAFE AUXILIARY VOLTAGE SUPPLY		

10.2 GBS Functional Analysis

Going on with the functional analysis four different ways in which the aircraft can be launched have been identified:

1. Case1 is a *conventional take off* where the aircraft is accelerated to take off speed with idle engine thrust. (note that the engines need to spool up during the take-off to generate sufficient power after leaving the track)
2. In case of using so called *conventional II take-off*, the aircraft is accelerated before lift-off up to the take-off speed while the aircraft (current generation) engines generate an average thrust of 50% at the start.
3. The *accelerated take-off* may be realised at engine idle condition and higher acceleration using an even shorter track. Again engines need to spool up.
4. Finally, in the *unconventional take-off* (the accelerated climb of aircraft during which the engines will be operated at 100 % of power). Take-off over-speed will be sufficient to climb the aircraft to altitude 300 m, while the engine power will be reduced immediately after lift-off to 92% power. Such take-off and climb will results to the minimum noise in the nearby airport region. After reaching the altitude 300 m the aircraft may continue its normal flight at normal thrust settings.

Take Off

- F3.1 Secure the cart position on the sledge
  - F3.1.1 check that the cart is secured on the sledge

- F3.2. Take-off procedure (e.g. accelerated, unconventional)
  - F3.2.1 decide about the take-off procedure (e.g. accelerated, unconventional)
  - F3.2.2 communication to all involved systems (maglev motor, sledge, a/c) the data of the chosen TO procedure

- F3.3.a Decide on semi or fully automatic procedure

- F3.3. Acceleration
  - F3.3.1. check the position of the sledge
  - F3.3.2. check the condition of the maglev track (levitation, obstacles, etc.)
  - F3.3.3.check the engine condition
  - F3.3.4 Propulsion voltage and frequency control according to preset speed profile.
  - F3.3.5. monitor the acceleration process

- F3.3.5.1. monitor the take-off speeds
- F3.3.5.2. monitor the rotation of the sledge (pitch and yaw)

❖ F3.4 decide about the continuation of the take-off phase

❖ F3.5 Detach the A/C from the sledge

  - F3.5.1 check / monitor the separation between the aircraft and the cartThis check is made when velocity and position on the runway are correct for take-off

These Functions are allocated to the A/C and to the pilot.

❖ F3.6 to enable the minimum slope and speed for takeoff
❖ F3.7 to remain within the flight envelope
❖ F3.8 to maintain the minimum climb slope (OEI condition included)
❖ F3.9 to maintain the necessary speed
❖ F3.10 to respect the air traffic controllers orders

❖ F3.11 decelerate the sledge

❖ F3.12. re-establish the initial position of the sledge/cart (pitch and yaw)

❖ F3.13 bring the sledge back to the initial position for the next take-off

❖ F3.14. change the cart on the sledge if required (new take-off, or different a/c category)

❖ F3.15 disconnect the cart from the sledge (according to F3.12)

Landing

- Function: F4.1 to synchronize the rendezvous between the aircraft and the Cart/Sledge system
- Function F4.3: to reach the final approach zone
- Function F4.4: to align the aircraft in the landing axis (trajectory)
- Function F4.5 : to absorb the potential/dynamic energy of the aircraft
- Function F4.6: to ensure and control the connection between the aircraft and the cart
- Function F4.7: to lock the aircraft on the cart/sledge
- Function F4.8: to decelerate
- Function F4.9: to minimize environmental impact (noise and emissions)
- F4.11 to enable the cart to roll on the runway with the aircraft

11.1 Applicable Hazard list for the GBS

BASIC DESIGN DEFICIENCIES

- Sharp corners
- Structural Instability
- Excessive weight
- Inadequate clearance
- Temperature
- Lack of accessibility
- Inadequate speed
- inadequate acceleration
- Inability to rotate due to incorrect center of gravity (CG) location, mistake in performance calculation, or flight control anomalies

All the previous hazards are to be managed at design phase impacting all the GBS level 2 items. They represent hazards for all the GBS life-cycle and are to be approached by proper design, structural tests, stress tests, simulation tests.

INHERENT HAZARDS

- Vertical kinetic energy
- Horizontal kinetic energy
- High mass and dynamic inertia
- Mechanical (i.e., rotating equipment, vibration)
- Electrical
- Maglev forces
- Explosives
- Flammable gases or liquids
- Toxic substances
- Acceleration
- Deceleration
- Temperature
- Mechanical anomalies
- Contaminated runways
- Crosswind
- Runway, taxy-way incursion

They represent hazards originated by the specific technology and mission

MALFUNCTIONS

- Aircraft, cart untimely disconnection/connection
- Aircraft, sledge untimely disconnection/connection
- Cart, Sledge untimely disconnection/connection
- Structural failures
- Mechanical malfunctions
- Electrical malfunctions
- Maglev malfunctions
- Power failures
- Software failures
- Software Hardware Interface Failures
- Man Machine Interface Failures
- Malicious attacks to system components (HW/SW)

METEO/ENVIRONMENTAL

- Thunderstorms lighting
- wind shear
- icing, freezing
- snow
- heavy rain
- low visibility
- floods
- volcanic ash
- Rapid fire spread, smoke/toxic gas build-up
- Heat
- Cold
- Dryness
- Wetness
- Low friction (slipperiness)
- Glare
- Darkness
- Earthquake
- Noise
- Engine emissions
- Electromagnetic field

HUMAN FACTORS

- Pilot's perception of a catastrophic failure
- Stress (sensory, mental, motor)
- Physical surroundings (environment)
- Illumination
- Vibration
- Errors
- Omission
- Commission
- Missed recognition of hazards
- Incorrect decisions
- Tasks done at wrong time (untimely)
- Tasks not performed or incorrectly performed

11.2 Hazard Scenarios for the GBS

F3.1 secure the cart position on the sledge

- F3.1.1 check that the cart is secured on the sledge

Failure mode

1) unexecuted check

2) wrong check

Hazards acting as initiator event

- Inherent Hazards: Electrical, Mechanical anomalies, Crosswind
- Malfunctions: Electrical malfunctions, Power failures, Software failures, Software Hardware Interface Failures, Man Machine Interface Failures, Malicious attacks to system components (HW/SW),
- Meteo/Environmental Hazards: icing, freezing, snow, heavy rain, untimely task, low visibility, volcanic ash, darkness,
- Human Factors: stress, environmental, untimely task

Failure Mode Effect

1) unkown status

2.1) Cart not secured to the sledge

2.2) Cart initially secured to the sledge and during acceleration loss of locked status

Severity

1) **Minor** - if operations are stopped

2.1) and 2.2) **Catastrophic** - unstable position, and Fall down of A/C from the sledge

Requirements

1) If the cart locking on the sledge is unknown, operations have to be stopped

2) The lock system to secure the cart on the sledge must be highly reliable. The check of the lock status should be performed from both the cart and the sledge and info about the status should be transferred to the control system on independent channels

F3.2. take-off procedure (.e.g accelerated, unconventional)

- F3.2.1 decide about the take-off procedure (.e.g accelerated, unconventional)

Failure mode

1) wrong decision

2) untimely decision"

Hazards acting as initiator event

- "Malfunctions: Man Machine Interface Failures, Malicious attacks to system components (HW/SW),
- Meteo/Environmental: thunderstorms lighting, wind shear, icing, freezing, snow, heavy rain, low visibility , untimely task, low visibility, volcanic ash, darkness,
- Human Factors: stress, environmental, untimely task" "

Failure Mode Effect

1) wrong decision

The Failure mode effect depend on the requirements for choosing one or another procedure; these can be: rules, weather conditions, power supply condition, type of a/c, a/c weight, Air Traffic conditions

Severity

1) Major - if pilot applying accelerated and sledge is following unconventional procedure

2) Catastrophic - if pilot applying unconventional and sledge is following accelerated

Requirements

1) & 2) The choice of the take-off procedure must be well defined and based on data which are measure with high accuracy and reliability

F3.2. take-off procedure (.e.g accelerated, unconventional)

F3.2.2 communication to all involved systems (maglev motor, sledge, a/c) the data of the chosen TO procedure

Failure mode

1) data link down

2) different procedures are read by different systems

Hazards acting as initiator event

- Inherent Hazards: Electrical, Mechanical anomalies,
- Malfunctions: Electrical malfunctions, Power failures, Software failures, Software Hardware Interface Failures,
- Meteo/Environmental: icing, freezing, snow, heavy rain, volcanic ash, earthquake,

Failure Mode Effect

1) STOP procedure

2) a different procedure is implemented by the various systems

Severity

1) Minor

2) Catastrophic

Requirements

1) In order to avoid delays due to take-off abort the data link should be stable and highly reliable

2) The communication of the take-off procedure must be highly reliable

F3.3. Acceleration

F3.3.1. check the position of the sledge

Failure mode

1) unexecuted check of the sledge position

2) wrong check of the sledge position

Hazards acting as initiator event

- Inherent Hazards: Electrical, Mechanical anomalies, Crosswind,
- Malfunctions: Electrical malfunctions, Power failures, Software failures, Software Hardware Interface Failures, Man Machine Interface Failures, Malicious attacks to system components (HW/SW),
- Meteo/Environmental: icing, freezing, snow, heavy rain, untimely task, low visibility, volcanic ash, darkness,
- Human Factors: stress, environmental, untimely task

Failure Mode Effect

1) unknown position of the sledge
2) wrong position of the sledge

Severity

1) Minor - might have an effect on operations
2) Catastrophic - if the sledge is considered at a proper position the acceleration is maintained - if this is not true the sledge will not be decelerated and the A/C will not take-off but crash

Requirements

1) if the position of the sledge is unknown the emergency deceleration must be applied
2) the system to check the position of the sledge must be highly reliable in order to abort the take-off in case of need

F3.3. Acceleration

F3.3.2. check the condition of the maglev track (including the levitation capability)

Failure mode

1) unexecuted check of the maglev track condition

2) wrong check of the maglev check condition

Hazards acting as initiator event

- Malfunctions: Man Machine Interface Failures, Malicious attacks to system components (HW/SW),
- Meteo/Environmental: thunderstorms lightening, wind shear, icing, freezing, snow, heavy rain, low visibility , untimely task, low visibility, volcanic ash, darkness,
- Human Factors: stress, environmental, untimely task

Failure Mode Effect

1) unknown maglev track conditions

2.1) maglev track not able to levitate the sledge/cart/aircraft

2.2) maglev tack untimely failure of levitation function

2.3) maglev track not suitable for TO due to obstacles or material "

Severity

1) and 2.1) Minor - might have an effect on operations

2.2) Hazardous

2.3) Catastrophic

Requirements

1) and 2.1) The system to check the maglev condition must be highly reliable (e.g. check temperature, …) - SLEDGE WHEELS are needed; these wheels have to be able to stand the sledge/cart/aircraft/ without magnetic levitation and will allow to move system in case of failure

2.2) SLEDGE WHEELS are needed; these wheels have to be able to stand the sledge/cart/aircraft/ WITH HIGH SPEED and without magnetic levitation and will allow to avoid the crash of the system on ground in case of failure during the acceleration phase

2.3.a) runway incursion should be avoided by proper operations and taxiway design

2.3.b) during sledge repositioning to the runway head a safety cleaning of the maglev might be enforced together with an automatic inspection to check obstacles presence

F3.3. Acceleration

F3.3.3.check the engine (of the maglev acceleration system) condition

Failure mode

1) unexecuted check of the engine condition

2) wrong check of the engine condition

Hazards acting as initiator event

- Inherent Hazards: Electrical, Mechanical anomalies
- Malfunctions: Electrical malfunctions, Power failures, Software failures, Software Hardware Interface Failures,
- Meteo/Environmental:, icing, freezing, snow, heavy rain, volcanic ash, earthquake, "

Failure Mode Effect

1) unknown engine condition
2) engine start failure
3) engine not in the right condition to properly accelerate the sledge
4) untimely engine shut down (during operation)

Severity

1) and 2) Minor - might have an effect on operations

3) and 4) Hazardous

Requirements

1) if the engine condition are unknown the take-off should be aborted
3) an auxiliary braking system must be available in case the propulsion engine fails

F3.3. Acceleration

F3.3.4 Propulsion voltage and frequency control according to preset speed profile

Failure mode

1) unexecuted check
2) wrong check

Hazards acting as initiator event

- Inherent Hazards: Electrical
- Malfunctions: Electrical malfunctions, Power failures, Software failures, Software Hardware Interface Failures, Man Machine Interface Failures, Malicious attacks to system components (HW/SW),

- Meteo/Environmental: thunderstorms lightening, wind shear, icing, freezing, snow, heavy rain, low, untimely task, low visibility, volcanic ash, darkness, earthquake,
- Human Factors: stress, environmental, untimely task

Failure Mode Effect

1) unknown engine condition
2) Propulsion voltage and frequency control disaligned with the chosen nominal speed profile
2.1) engine start failure
2.2) engine start with wrong performances
2.3) engine in the proper range
2.4) engine damages
2.5) engine heavy damages

Severity

1) Minor - might have an effect on operation
2.1) Minor
2.2) Hazardous
2.3) None
2.4) Catastrophic
2.5 Catastrophic

Requirements

1) if engine condition is unknown the take-off is aborted
2.1) if engine start is failed an emergency operation has to be defined
2.2a) system to check voltage and frequency must be highly reliable
2.2b) after start of acceleration the performance should be monitored, in case acceleration is not respecting nominal profile abort the take-off
2.4-2.5) the engine condition should be monitored during operation; safety procedures must be defined to recover form fail conditions

F3.3. Acceleration

F3.3.5. monitor the acceleration process

F3.3.5.1. monitor the take-off speeds

Failure mode

1) unexecuted check
2) wrong check

Hazards acting as initiator event

- Inherent Hazards: Electrical, Mechanical anomalies, Mechanical (e.g. rotating eq., vibration)

- Malfunctions: Electrical malfunctions, Power failures, Software failures, Software Hardware Interface Failures, Man Machine Interface Failures, Malicious attacks to system components (HW/SW),
- Meteo/Environmental Hazards: icing, freezing, snow, heavy rain, untimely task, low visibility, volcanic ash, darkness,
- Human Factors: stress, environmental, untimely task

Failure Mode Effect

1) no speed info for the sledge by the ground system: this info is mandatory
2) wrong sledge + a/c speed is provided by the ground system

Severity

1) Major/Hazardous (if an alternative speed measure is ensured)
2) Catastrophic (if an alternative speed measure is not ensured)

Requirements

1) & 2) A high reliable system for speed checking is required; a redundancy system to check speed might be required (e.g. a/c data or external system)

F3.3. Acceleration

F3.3.5. monitor the acceleration process

F3.3.5.2. monitor the stability of the combined system a/c, cart spring and dampers, maglev levitation, maglev damping

Failure mode

1) unexecuted check
2) wrong check

Hazards acting as initiator event

- Inherent Hazards: Electrical, Mechanical anomalies, Mechanical (e.g. rotating eq., vibration)
- Malfunctions: Electrical malfunctions, Power failures, Software failures, Software Hardware Interface Failures, Man Machine Interface Failures, Malicious attacks to system components (HW/SW),
- Meteo/Environmental Hazards: icing, freezing, snow, heavy rain, untimely task, low visibility, volcanic ash, darkness,
- Human Factors: stress, environmental, untimely task

Failure Mode Effect

1) no info on stability conditions are provided; this info is mandatory

2.1) the system is considered unstable but it is in a stable condition

2.2 the system is considered stable but is unstable

Severity

1) and 2.1) Minor if an emergency deceleration is applied; operations can be affected

2.2) Catastrophic (if an alternative stability measure is not ensured)

Requirements

1) & 2) A high reliable system for stability checking is required; a redundancy system to check stability should be required

F3.4 decide about the continuation of the take-off phase

Failure mode

Wrong decision

1) the decision is made by human

2) the decision is made by a SW

3) the decision is made by both human and SW

Hazards acting as initiator event

- Malfunctions: Electrical malfunctions, Power failures, Software failures, Software Hardware Interface Failures, Man Machine Interface Failures, Malicious attacks to system components (HW/SW),
- Meteo/Environmental Hazard: icing, freezing, snow, heavy rain, untimely task, low visibility, volcanic ash, darkness,
- Human Factors: stress, environmental, untimely task

Failure Mode Effect

a) if the wrong decision is to stop TO phase the effect will be on delay of operations and uncomfortable experience by passengers

b) if the wrong decision is to continue but there was the need to stop the TO phase the effect can be a A/C crash

Severity

a) Minor or Major

b) Catastrophic

Requirements

All the tools supporting decision making for continuation of TO phase have to be highly reliable.

The needed data to take a decision have to be highly reliable (speed, position, status of subsystems, ...)

1) appropriate training of operators and continuous monitoring

2) SW has to be certified and qualified level A

3) The hybrid decision mechanism (human + SW) requires high reliability

F3.5 pitch up of the cart and aircraft

F3.5.1 monitor the rotation of the sledge (pitch and yaw)
The cart can be rotated by: 1) actuators 2) using the aircraft elevator and the car are left free to rotate

Failure mode

1) unexecuted check
2) wrong check

Hazards acting as initiator event

- Inherent Hazards: Electrical, Mechanical anomalies, Mechanical (e.g. rotating eq., vibration)
- Malfunctions: Electrical malfunctions, Power failures, Software failures, Software Hardware Interface Failures, Man Machine Interface Failures, Malicious attacks to system components (HW/SW),
- Meteo/Environmental Hazards: icing, freezing, snow, heavy rain, untimely task, low visibility, volcanic ash, darkness,
- Human Factors: stress, environmental, untimely task

Failure Mode Effect

1) no info on sledge rotation from the ground system; this info is needed
2) wrong sledge + a/c rotation status is provided ;
2.1) a/c rotated properly but check provides wrong status
2.2) a/c NOT rotated properly but check provides the info that the pitch is correct

The wrong rotation can be due to: A) The actuators are not working properly
B) the cart free movement is blocked and the aircraft elevator is not able to pitch the aircraft"

Severity

1) Major/Hazardous (if an alternative rotation measure is ensured)
2.1) Minor: the system will be decelerated and operation will be negatively affected
2.2) Catastrophic (if an alternative rotation measure is not ensured)

Requirements

1) & 2.2) A high reliable system for rotation checking is required. A redundancy system to check rotation of the cart/sledge might be required (e.g. a/c data or external system)
2.1) An emergency procedure must be envisaged to decelerate the system in case the aircraft pitch is not properly ensured.

F3.6 Detach the A/C from the sledge

F3.6.1 check / monitor the separation between the aircraft and the cart
(This check is made when velocity and position on the runway are correct for take-off)

Failure mode

1) unexecuted check

2) wrong check

Hazards acting as initiator event

- Inherent Hazards: Electrical, Mechanical anomalies, Mechanical (e.g. rotating eq., vibration)
- Malfunctions: Electrical malfunctions, Power failures, Software failures, Software Hardware Interface Failures, Man Machine Interface Failures, Malicious attacks to system components (HW/SW),
- Meteo/Environmental Hazard: icing, freezing, snow, heavy rain, untimely task, low visibility, volcanic ash, darkness,
- Human Factors: stress, environmental, untimely task

Failure Mode Effect

1) unknown separation condition

2)The information about the separation is wrong

2.1) A/C and cart are considered separated but are connected

2.2) A/C and cart are considered connected but are separated

Severity

1.1) if the A/C is detached and the horizontal tail surface is in the proper position with respect to A/C rotation (e.g. attitude and AoA) the take-off will take place - **Severity is Minor**

1.2) if the A/C is detached and the horizontal tail surface is not in the proper position with respect to A/C rotation (e.g. attitude and AoA) the take-off will NOT take place

Severity is Catastrophic

2.1.a) the A/C does not take-off - if structure is able to stand the loads the control system will brake the sledge and cart.

Severity is Major

2.1.b) the A/C does not take-off - if structure is not able to stand the loads the control system will brake the sledge and cart

Severity is Catastrophic

2.2.a) The control system will brake

Severity is Hazardous

Requirements

1.1 and 1.2) A system to ensure the coherence between the cart attitude, cart speed and the horizontal control surface must be provided

2.1.a) structure must be able to stand the loads at take-off speed (plus safety coefficient).

2.2) in order to avoid this Hazard a specific new operational function must be ensured: before starting the deceleration of the sledge (whatever is the reason) the F3.1 ""secure the A/c on cart"" must be executed. This will work if the A/C did not shift his position or anyhow the mechanism to secure the A/C works properly.

The system to check the separation must have a very high reliability

F3.5 + F3.6 STANDARD take-off: enable the minimum slope (a/c pitch) and speed for takeoff

This function is related to the standard take-off procedure and is not applicable to an assisted take-off like in the GABRIEL system.

Thus these functions are NOT APPLICABLE

F3.7 to remain within the flight envelope
F3.8 to maintain the minimum climb slope (OEI condition included)
F3.9 to maintain the necessary speed
F3.10 to respect the air traffic controllers orders

These Functions are allocated to the A/C and to the pilot.

Thus, these functions are not analysed here

F3.11 decelerate the sledge

Failure mode

1) unexecuted deceleration

2) wrong deceleration

Hazards acting as initiator event

- Inherent Hazards: Electrical, Mechanical anomalies, Mechanical (e.g. rotating eq., vibration)
- Malfunctions: Electrical malfunctions, Power failures, Software failures, Software Hardware Interface Failures, Man Machine Interface Failures, Malicious attacks to system components (HW/SW),
- Meteo/Environmental Hazard: icing, freezing, snow, heavy rain, untimely task, low visibility, volcanic ash, darkness,
- Human Factors: stress, environmental, untimely task

Failure Mode Effect

1) the sledge will keep speed or acceleration

2) the sledge does not reduce speed according to nominal profile

Severity

a) **Major** - the sledge might crash at the end of the runway or loss connection to maglev track- no human injuries or losses if nobody or any vehicle can be at the end of the runway/maglev track or aside

b) **Hazardous** if people or vehicles are at the end of the runway/maglev track or aside; this in case sledge will derail

Requirements

1) & 2) A high reliable system for rotation checking is required. A redundancy system to check rotation of the cart/sledge might required (e.g. a/c data or external system)

F3.12 Re-establish the initial position of the sledge/cart (pitch and yaw)
F3.13 Bring the sledge back to the initial position for the next take-off
F3.14 Change the cart on the sledge if required (new take-off, or different a/c category)
F3.15 Disconnect the cart from the sledge (according to F3.12)

Failure mode

1) unexecuted reposition of the cart/sledge

2) wrong reposition of the cart/sledge

Hazards acting as initiator event

- Inherent Hazards: Electrical, Mechanical anomalies, Mechanical (e.g. rotating eq., vibration)
- Malfunctions: Electrical malfunctions, Power failures, Software failures, Software Hardware Interface Failures, Man Machine Interface Failures, Malicious attacks to system components (HW/SW),
- Meteo/Environmental Hazard: icing, freezing, snow, heavy rain, untimely task, low visibility, volcanic ash, darkness,
- Human Factors: stress, environmental, untimely task"

Failure Mode Effect

1) delay of operations

2.a) if a check is performed and there is the awareness of the failure a delay of operations may be expected

2.b) if failure is undetected this might propagate to the following take-off

Severity

1) & 2.a) Minor

2.b) Hazardous

Requirements

Actuation of cart must be reliable, a check of the cart repositioning must be performed; the information of cart positioning on the sledge must be available to both the pilot and ATC operator.

According to the preliminary Functional FMEA, summarized in section 11.3, a provisional Critical Item Lists has been derived and is presented in section 11.4.

Finally, in section 11.5 the derived requirements are mapped onto the product tree.

In section 11.6 additional safety considerations are presented.

11.3 Summary of FMEA for the take-off phase

In the following table a summarising table of the FMEA is provided; the following elements are shown:

- function
- failure mode
- failure mode effect
- severity

TABLE 1 – FMEA for TAKE OFF phase

Function	Failure mode	Failure mode effect	Severity	Requirements
F3.1 secure the cart position on the sledge *F3.1.1 check that the cart is secured on the sledge*	1) unexecuted check 2) wrong check	1) Unknown status 2.1) Cart not secured to the sledge 2.2) Cart initially secured to the sledge and during acceleration loss of locked status	1) and 2.1) **Minor** - if operations are stopped 2.1) **Catastrophic** - unstable position, and fall down of A/C from the sledge	1) If the cart locking on the sledge are unknown operations have to be stopped 2) The lock system to secure the cart on the sledge must be highly reliable. The check of the lock status should be performed from both the cart and the sledge and info about the status should be transferred to the control system on independent channels
F3.2. take-off procedure (.e.g accelerated, unconventional) *F3.2.1 decide about the take-off procedure (.e.g accelerated, unconventional)*	1) unexecuted check 2) wrong check	1) wrong decision The Failure mode effect depend on the requirements for choosing one or another procedure; these can be: rules, meteorological conditions, power supply condition, type of a/c, a/c weight, Air Traffic conditions"	1) **Major** - if pilot applying accelerated and sledge is following unconventional procedure 2) **Catastrophic** - if pilot applying unconventional and sledge is following accelerated"	1) & 2) The choice of the take off procedure must be well defined and based on data which are measure with high accuracy and reliability

Function	Failure mode	Failure mode effect	Severity	Requirements
F3.2. take-off procedure (.e.g accelerated, unconventional) F3.2.2 communication to all involved systems (maglev motor, sledge, a/c) the data of the chosen TO procedure	Failure mode 1) data link down 2) different procedures are read by different systems	1) STOP procedure 2) a different procedure is implemented by the various systems	1) **Minor** 2) **Catastrophic**	1) In order to avoid delays due to take-off abort the data link should be stable and highly reliable 2) The communication of the take-off procedure must be highly reliable
F3.3. Acceleration F3.3.1. check the position of the sledge	1) unexecuted check of the sledge position 2) wrong check of the sledge position	1) unknown position of the sledge 2) wrong position of the sledge	1) **Minor** - might have an effect on operations 2) **Catastrophic** - if the sledge is considered at a proper position the acceleration is maintained - if this is not true the sledge will not be decelerated and the A/C will not take-off but crash	1) if the position of the sledge is unknown the emergency deceleration must be applied 2) the system to check the position of the sledge must be highly reliable in order to abort the take-off in case of need

Function	Failure mode	Failure mode effect	Severity	Requirements
F3.3. Acceleration F3.3.2. check the condition of the maglev track (including the levitation capability)	1) unexecuted check of the maglev track condition 2) wrong check of the maglev check condition	1) unknown maglev track conditions 2.1) maglev track not able to levitate the sledge/cart/aircraft 2.2) maglev tack untimely failure of levitation function 2.3) maglev track not suitable for TO due to obstacles or material	1) and 2.1) **Minor** - might have an effect on operations 2.2) **Hazardous** 2.3) **Catastrophic**	1) and 2.1) The system to check the maglev condition must be highly reliable (e.g. check temperature, …) - SLEDGE WHEELS are needed; these wheels have to be able to stand the sledge/cart/aircraft/ without magnetic levitation and will allow to move system in case of failure 2.2) SLEDGE WHEELS are needed; these wheels have to be able to stand the sledge/cart/aircraft/ WITH HIGH SPEED and without magnetic levitation and will allow to avoid the crash of the system on ground in case of failure during the acceleration phase 2.3.a) runway incursion should be avoided by proper operations and taxiway design 2.3.b) during sledge repositioning to the runway head a safety cleaning of the maglev might be enforced together with an automatic inspection to check obstacles presence

Function	Failure mode	Failure mode effect	Severity	Requirements
F3.3. Acceleration *F3.3.3.check the engine (of the maglev acceleration system) condition*	1) unexecuted check of the engine condition 2) wrong check of the engine condition	1) unknown engine condition 2) engine start failure 3) engine not in the right condition to properly accelerate the sledge 4) untimely engine shut down (during operation)	1) and 2) **Minor** - might have an effect on operations 3) and 4) **Hazardous**	1) if the engine condition are unknown the take-off should be aborted 3) an auxiliary braking system must be available in case the propulsion engine fails
F3.3. Acceleration *F3.3.4 Propulsion voltage and frequency control according to preset speed profile*	1) unexecuted check 2) wrong check	1) unknown engine condition 2) Propulsion voltage and frequency control misaligned with the chosen nominal speed profile 2.1) engine start failure 2.2) engine start with wrong performances 2.3) engine in the proper range 2.4) engine damages 2.5) engine heavy damages	1) **Minor** - might have an effect on operation 2.1) **Minor** 2.2) **Hazardous** 2.3) **None** 2.4) **Catastrophic** 2.5 **Catastrophic**	1) if engine condition is unknown the take-off is aborted 2.1) if engine start is failed an emergency operation has to be defined 2.2a) system to check voltage and frequency must be highly reliable 2.2b) after start of acceleration the performance should be monitored, in case acceleration is not respecting nominal profile abort the take-off 2.4-2.5) the engine condition should be monitored during operation; safety procedures must be defined to recover form fail conditions

Function	Failure mode	Failure mode effect	Severity	Requirements
F3.3. Acceleration *F3.3.5. monitor the acceleration process* ***F3.3.5.1. monitor the take-off speeds***	1) unexecuted check 2) wrong check	1) no speed info for the sledge by the ground system: this info is mandatory 2) wrong sledge + a/c speed is provided by the ground system	1) **Major**/**Hazardous** (if an alternative speed measure is ensured) 2) **Catastrophic** (if an alternative speed measure is not ensured)	1) & 2) A high reliable system for speed checking is required; a redundancy system to check speed might be required (e.g. a/c data or external system)
F3.3. Acceleration *F3.3.5. monitor the acceleration process* ***F3.3.5.2. monitor the stability of the combined system a/c, cart spring and dampers, maglev levitation, maglev damping***	1) unexecuted check 2) wrong check	1) no info on stability conditions are provided; this info is mandatory 2.1) the system is considered unstable but it is in a stable condition 2.2 the system is considered stable but is unstable	1) and 2.1) **Minor** if an emergency deceleration is applied; operations can be affected 2.2) **Catastrophic** (if an alternative stability measure is not ensured)	1) & 2) A high reliable system for stability checking is required; a redundancy system to check stability should be required

Function	Failure mode	Failure mode effect	Severity	Requirements
F3.4 decide about the continuation of the take-off phase	Wrong decision 1) the decision is made by human 2) the decision is made by a SW 3) the decision is made by both human and SW	a) if the wrong decision is to stop TO phase the effect will be on delay of operations and uncomfortable experience by passengers b) if the wrong decision is to continue but there was the need to stop the TO phase the effect can be a A/C crash"	a) **Minor** or **Major** b) **Catastrophic**	All the tools supporting decision making for continuation of TO phase have to be highly reliable. The needed data to take a decision have to be highly reliable (speed, position, status of subsystems, ...) 1) appropriate training of operators and continuous monitoring 2) SW has to be certified and qualified level A 3) The hybrid decision mechanism (human + SW) requires high reliability
F3.5 pitch up of the cart and aircraft *F3.5.1 monitor the rotation of the sledge (pitch and yaw)* **The cart can be rotated by: 1) actuators 2) using the aircraft elevator and the car are left free to rotate**	unexecuted check wrong check	1) no info on sledge rotation from the ground system; this info is needed 2) wrong sledge + a/c rotation status is provided ; 2.1) a/c rotated properly but check provides wrong status 2.2) a/c NOT rotated properly but check provides the info that the pitch is correct The wrong rotation can be due to: A) The actuators are not working properly B) the cart free movement is blocked and the aircraft elevator is not able to pitch the aircraft"	1) Major/Hazardous (if an alternative rotation measure is ensured) 2.1) Minor: the system will be decelerated and operation will be negatively affected 2.2) Catastrophic (if an alternative rotation measure is not ensured)	1) & 2.2) A high reliable system for rotation checking is required. A redundancy system to check rotation of the cart/sledge might be required (e.g. a/c data or external system) 2.1) An emergency procedure must be envisaged to decelerate the system in case the aircraft pitch is not properly ensured.

Function	Failure mode	Failure mode effect	Severity	Requirements
F3.6 Detach the A/C from the sledge *F3.6.1 check / monitor the separation between the aircraft and the cart* **This check is made when velocity and position on the runway are correct for take-off)**	1) unexecuted check 2) wrong check	1) unknown separation condition 2)The information about the separation is wrong 2.1) A/C and cart are considered separated but are connected 2.2) A/C and cart are considered connected but are separated	1.1) if the A/C is detached and the horizontal tail surface is in the proper position with respect to A/C rotation (e.g. attitude and AoA) the take-off will take place **- Severity is Minor** 1.2) if the A/C is detached and the horizontal tail surface is not in the proper position with respect to A/C rotation (e.g. attitude and AoA) the take-off will NOT take place - **Severity is Catastrophic** 2.1.a) the A/C does not take-off - if structure is able to stand the loads the control system will brake the sledge and cart. -**Severity is Major** 2.1.b) the A/C does not take-off - if structure is not able to stand the loads the control system will brake the sledge and cart - Severity is Catastrophic 2.2.a) The control system will brake **Severity is Hazardous**	1.1 and 1.2) A system to ensure the coherence between the cart attitude, cart speed and the horizontal control surface must be provided 2.1.a) structure must be able to stand the loads at take-off speed (plus safety coefficient). 2.2) in order to avoid this Hazard a specific new operational function must be ensured: before starting the deceleration of the sledge (whatever is the reason) the F3.1 ""secure the A/c on cart"" must be executed. This will work if the A/C did not shift his position or anyhow the mechanism to secure the A/C works properly. **The system to check the separation must have a very high reliability**

Function	Failure mode	Failure mode effect	Severity	Requirements
F3.5 + F3.6 STANDARD take-off: enable the minimum slope (a/c pitch) and speed for takeoff This function is related to the standard take-off procedure and is not applicable to an assisted take-off like in the L system under study. **Thus these functions are NOT APPLICABLE**				
F3.7 to remain within the flight envelope F3.8 to maintain the minimum climb slope (OEI condition included) F3.9 to maintain the necessary speed F3.10 to respect the air trafic controllers orders **These Functions are allocated to the A/C and to the pilot.** **Thus, these functions are not analysed here**				

Function	Failure mode	Failure mode effect	Severity	Requirements
F3.11 decelerate the sledge	1) unexecuted deceleration 2) wrong deceleration	1) the sledge will keep speed or acceleration 2) the sledge does not reduce speed according to nominal profile	a) **Major** - the sledge might crash at the end of the runway or loss connection to maglev track- no human injuries or losses if nobody or any vehicle can be at the end of the runway/maglev track or aside b) **Hazardous** if people or vehicles are at the end of the runway/maglev track or aside; this in case sledge will derail	1) & 2) A high reliable system for rotation checking is required. A redundancy system to check rotation of the cart/sledge might required (e.g. a/c data or external system)
F3.12 Re-establish the initial position of the sledge/cart (pitch and yaw) F3.13 Bring the sledge back to the initial position for the next take-off F3.14 Change the cart on the sledge if required (new take-off, or different a/c category) F3.15 Disconnect the cart from the sledge (according to F3.12)	1) unexecuted reposition of the cart/sledge 2) wrong reposition of the cart/sledge	1) delay of operations 2.a) if a check is performed and there is the awareness of the failure a delay of operations may be expected 2.b) if failure is undetected this might propagate to the following take-off	1) & 2.a) **Minor** 2.b) **Hazardous**	Actuation of cart must be reliable, a check of the cart repositioning must be performed; the information of cart positioning on the sledge must be available to both the pilot and ATC operator.

11.4 Provisional Critical Item List (CIL)

Provisional Critical Item List (CIL) for take off

For the GBS components there are hazards and additional system complexity related to the interfaces among components (e.g. aircraft, cart, sledge) to be considered in terms of:

- Proper connection/disconnection systems and procedures (fail safe).
- Proper operations for avoiding runway and maglev track contamination/incursion
- Proper operations and equipment to guarantee needed acceleration and abort take off sequence
- Proper instrumentation panel to monitor acceleration levels (fail safe)
- Proper instrumentation panel to monitor configuration state for the GBS
- Proper instrumentation panel to monitor locking mechanisms
- Mechanisms and eventually actuators for pitching and yawing the cart
- Reaction Rails (*Product Tree ID 26*)
- Braking Rails (*Product Tree ID 27*)
- Emergency Braking (*Product Tree ID 271*)
- Position Indicators (*Product Tree ID 29*)
- Location of Sledge (*Product Tree ID 291*)
- Propulsion (*Product Tree ID 3*)
- Power Chain (*Product Tree ID 4*)
- Supply of Propulsion with Adjusted Electric Energy (*Product Tree ID 4.1*)
- Sledge (*Product Tree ID 5*)
- Structure (*Product Tree ID 51*)
- Cart Fixation (*Product Tree ID 52*)
- Levitation Frames (*Product Tree ID 53*)
- Rendezvous Control (*Product Tree ID 54*)

Each of the previous items must have a very high reliability by design.

11.5 Preliminary Requirement List

For each level 0 item in the product tree a preliminary requirement list is provided.

INFRASTRUCTURE

A proper infrastructure shall be built consisting of the following items and preliminary requirements.

11 OPERATION / MAINTENANCE CENTER –This site shall be dedicated to cart recovery and maintenance, sledge recovery and maintenance, electrical component recovery and maintenance.

12 SUBSTATION / CONTROL CENTER BUILDING - This site shall be dedicated to LODGING OF SWITCHING STATIONS; CONVERTERS; COMPENSATION EQUIPMENT AND CONTROL CENTER

13 SWITCH GEAR CABINETS

14 STATIONARY DATA TRANSMISSION - This site shall be dedicated to TRANSMITTING OF SIGNALS TO CONTROL CENTER

GUIDEWAY

This system is in charge of SUPPORTING AND GUIDING THE Sledge WITH CART AND AIRCRAFT.

It is consisting of the following items and preliminary requirements.

21 CUTTINGS

22 FOUNDATIONS

23 PILLERS

24 BEARINGS

25 GIRDERS

26 REACTION RAILS – This item shall be in charge of TRANSFERING FORCES AND MOMENTS TO THE GIRDERS

27 BRAKING RAILS – This item shall be in charge of EMERGENCY BRAKING

28 RAILS FOR WHEELS – This item shall be in charge of:281 STARTING AND LANDING

29 POSITION INDICATORS – This item shall be in charge of LOCATION OF SLED

210 CABLE TRENCHES

Additional preliminary requirements for the Guide-way:

- The system to check the maglev condition shall be highly reliable (temperature sensors, maglev status parameters.
- A high reliable system for stability checking is required; a redundancy system to check stability should be required
- The information on the position of the sledge shall be available at a proper rate in order to abort the take-off in case of need
- The sledge position information shall be highly accurate
- Runway incursion should be avoided by proper operations and taxiway design
- The runway status shall be monitored and managed
- During sledge repositioning to the runway head a safety cleaning of the maglev shall be enforced together with an automatic inspection to check obstacles presence if engine condition is unknown the take-off is aborted
- A high reliable system for speed checking is required; a redundant system to check speed might be required (e.g. a/c data or external system)
- An auxiliary braking system must be available in case the propulsion engine fails"

MAGLEV ENGINE

This system shall be in charge of: ACCELERATING; BRAKING; PASSIVE GUIDANCE AND LEVITATION FORCES.

It is consisting of the following items and preliminary requirements.

31 SUPPLY CABLE SYSTEMS

32 SWITCHING STATIONS (ELECTRONIC SWITCHES, CONTROL AND SUPERVISION, ELECTRICAL CONNECTIONS) – This item shall be in charge of SWITCHING OF CABLE WINDING SECTIONS ON AND OFF

33 STATOR PACKS GUIDEWAYSIDE

34 CABLE WINDINGS GUIDEWAYSIDE

35 ELECTRICAL CONNECTIONS

36 PROTECTION EQUIPMENT- This item shall be in charge of DETECTION OF SHORT CIRCUITS

Additional preliminary requirements for the Propulsion:

- if the engine conditions are unknown the take-off should be aborted
- if engine start is failed an emergency operation has to be defined
- system to check voltage and frequency must be highly reliable
- after start of acceleration the performance should be monitored, in case acceleration is not respecting nominal profile abort the take-off

- the engine condition should be monitored during operation; safety procedures must be defined to recover form fail conditions
- the system to check the maglev condition shall be highly reliable (temperature sensors, maglev status parameters)
- if engine start is failed an emergency operation shall be defined
- system to check voltage and frequency must be highly reliable
- after start of acceleration the performance should be monitored, in case acceleration is not respecting nominal profile abort the take-off
- the engine condition should be monitored during operation; safety procedures must be defined to recover from fail conditions

POWER CHAIN

This system shall be in charge of SUPPLYING OF PROPULSION WITH ADJUSTED ELECTRIC ENERGY.

It is consisting of the following items and preliminary requirements.

41 INCOMING FEEDERS

42 110 kV SWITCHING GEAR

43 HIGH VOLTAGE TRANSFORMERS

44 20 kV SWITCHGEAR

45 CONVERTER UNITS shall be in charge of: 4.5.1 CONVERTING FIX VOLTAGE AND FREQUENCY INTO VARIABLE VALUES

46 REACTIVE POWER COMPENSATION shall be in charge of:4.6.1 REDUCING APPARENT POWER; OBSERVING STIPULATIONS OF POWER GRID PROVIDER

47 6 kV SWITCHGEAR

48 AUXILIARY VOLTAGE

49 OUTGOING SWITCHGEAR

Additional preliminary requirements for the Power Chain:

- the system to check the maglev condition shall be highly reliable (temperature sensors, maglev status parameters)
- the system to check voltage and frequency must be highly reliable
- after start of acceleration the performance should be monitored, in case acceleration is not respecting nominal profile abort the take-off

- the engine condition should be monitored during operation; safety procedures must be defined to recover from fail conditions

SLEDGE

This system is consisting of the following items and preliminary requirements:

51 STRUCTURE

52 CART FIXATION this item shall be made of 521 LOCKING MECHANISM, 522 FLIP-UP PANELS

53 LEVITATION FRAMES this item shall be in charge of TRANSFERRING FORCES AND MOMENTS FROM CART / PLATFORM TO REACTION RAIL AT GUIDEWAY, PROVIDE MAGNETIC FIELD FOR PROPULSION

The involved subsystem of 53 are:

532 SPRINGS / DAMPERSin charge of CARE FOR EQUAL LOAD DISTRIBUTION AND DAMPING OF OSCILLATIONS

533 LEVITATION MAGNETS in charge of PASSIVE MAGNETIC FIELD FOR LEVITATION

534 PROPULSION MAGNETS in charge ofPASSIVE MAGNETIC FIELD FOR PROPULSION AND GUIDANCE

535 EMERGENCY BRAKES in charge of HALT AFTER FAILURE OF POWER GRID

536 AUXILIARY WHEELS STARTING / LANDING in charge of STARTING/LANDING

537 LOCATING

538 DATA TRANSMISSION

539 AUXILIARY ENERGY

54 RENDEZ-VOUS CONTROL

The involved subsystem of 54 are:

541 SLEDGE LONGITUDINAL CONTROL shall have an accuracy of +/- 1 m

542 SLEDGE PITCH CONTROL shall have 20 degrees

543 SLEDGE YAW CONTROL shall have +/- 10 degrees

544 SENSORS OF SLEDGE CONTROL shall acquire:

5441 GROUND SPEED

5443 PLATFORM YAW AND PITCH ANGLE

5443 VELOCITY AND ACCELERATION

5444 POSITION

5445 GROUND CONNECTION STATUS

545 SENSORS OF AIRCRAFT CONTROL shall acquire:

5451 PITCH ATTITUDE AND RATE

5452 PITCH, ROLL AND YAW ANGLE

5453 FLIGHT PATH, BANK, SLIDESLIP, TRACK ANGLE

5454 AIR- AND GROUNDSPEED

5455 ALTITUDE

5456 LONGITUDINAL AND LATERAL POSITION

546 RENDEZ-VOUS CONTROL MONITORING SYSTEM

55 ROTATIONAL PLATFORM

The involved subsystem of 55 are:

551 BEARINGS

551 ACTUATORS

551 HYDRAULICS

Additional preliminary requirements for the SLEDGE:

- If the cart locking on the sledge are unknown operations have to be stopped
- The lock system to secure the cart on the sledge must be highly reliable. The check of the lock status should be performed from both the cart and the sledge and info about the status should be transferred to the control system on independent channels
- An auxiliary braking system must be available in case the propulsion engine fails
- SLEDGE WHEELS are needed. These have to be able to stand: a) the sledge/cart/aircraft/ without magnetic levitation and will allow to move system in case of failure; b) the sledge/cart/aircraft/ WITH HIGH SPEED and without magnetic levitation and will allow to avoid the crash of the system on ground in case of failure during the acceleration phase
- The information on the cart/sledge locking status flag shall be highly reliable
- The system chain to acquire/display the cart/sledge locking status flag must be highly reliable
- if the position of the sledge is unknown the emergency deceleration must be applied

- the system to check the position of the sledge shall be highly reliable in order to abort the take-off in case of need
- the information on the position of the sledge shall be available at a proper rate in order to abort the take-off in case of need
- The sledge position information shall be highly accurate
- Structure shall be able to stand the loads at take-off speed (plus safety coefficient).

CART

This system shall have the dimensions: 15,9*8,52*2,1 m (l-w-h) and
consists of the following items and preliminary requirements.

61 STRUCTURE
62 UNDERCARRIAGE
63 PROPULSION
64 ENERGY SUPPY
65 AIRCRAFT FIXATION

The involved subsystem of 65 are:

651 HARPOON GRID
652 ADAPTED FIFTH WHEEL

66 SPRING DAMPER COMBINATION
67 PITCH MECHANISM

The involved subsystem of 67 (PITCH MECHANISM) are:

671 ACTUATORS
672 HYDRAULICS

68 CART CONTROL SYSTEM FOR REMOTE CONTROL (OPTIONAL)
69 BALLOONS (OPTIONAL)

Additional preliminary requirements for the Cart

- A high reliable system for rotation checking is required. A redundancy system to check rotation of the cart/sledge might require (e.g. a/c data or external system)

- A system to ensure the coherence between the cart attitude + speed and the horizontal control surface shall be provided
- Structure shall be able to stand the loads at take-off speed (plus safety coefficient).
- In order to avoid an unwanted separation between the aircraft and the cart a specific new operational function shall be ensured: before starting the deceleration of the sledge (whatever is the reason) the F3.1 "secure the A/c on cart" must be executed. This will work if the A/C did not shift its position or anyhow the mechanism to secure the A/C works properly
- The system to check the separation shall have a very high reliability
- Actuation of cart shall be reliable, a check of the cart repositioning must be performed; the information of cart positioning on the sledge must be available to both the pilot and ATC operator.

MAGLEV CONTROL CENTER

This system shall consist of the following items and preliminary requirements.

71 SIGNALLING / DATA TRANSMISSION in charge of HIGHEST LEVEL DATA TRANSFER CONTROL

72 PROPULSION CONTROL in charge of REVENUE VALUES SETTING

73 CONTROL / SUPERVISION in charge of HIGHEST LEVEL CONTROL, SAFETY AND MONITORING EQUIPMENT performing:

- CENTRALISED CONTROL SYSTEM
- SAFE PROPULSION SHUT OFF SIGNAL
- DIAGNOSIS
- SUPERVISION

74 SAFE AUXILIARY VOLTAGE SUPPLY in charge of ENSURING SAFE CONDITIONS IN CASE OF A FAILURE OF THE POWER GRID feeding:

- SWITCHGEAR
- RECTIFIER
- BATTERIES
- AUTOMATIC CONTROL
- ELECTRICAL CONNECTIONS
- SUPERVISION

Additional preliminary requirements for the cart

- All the tools supporting decision-making for continuation of TO phase have to be highly reliable
- The needed data to take a decision have to be highly reliable and accurate (speed, position, status of subsystems. ...)
- appropriate training of operators and continuous monitoring
- SW has to be certified and qualified level A
- The hybrid decision mechanism (human + SW) requires high reliability"
- The cart/sledge locking status flag shall be acquired and displayed to operators and control systems
- The system chain to acquire/display the cart/sledge locking status flag must be highly reliable
- If the cart locking on the sledge status flag is unknown operations have to be stopped
- Data for the take-off procedure shall be available with high reliability and accuracy (weather, velocity, acceleration, position of the sledge on the maglev track, status of the GBS parameters for take-off)
- If the position of the sledge is unknown the emergency deceleration must be applied
- The system to check the position of the sledge shall be highly reliable in order to abort the take-off in case of need
- The information on the position of the sledge shall be available at a proper rate in order to abort the take-off in case of need
- The system to check the maglev condition shall be highly reliable (temperature sensors, maglev status parameters)
- runway incursion should be avoided by proper operations and taxiway design
- If engine start is failed an emergency operation shall be defined

- The runway status shall be monitored and managed
- During sledge repositioning to the runway head a safety cleaning of the maglev shall be enforced together with an automatic inspection to check obstacles presence if engine condition is unknown the take-off is aborted
- After start of acceleration the performance should be monitored, in case acceleration is not respecting nominal profile abort the take-off
- The engine condition should be monitored during operation; safety procedures must be defined to recover from fail conditions
- A high reliable system for speed checking is required; a redundant system to check speed might be required (e.g. a/c data or external system)
- A high reliable system for rotation checking is required. A redundancy system to check rotation of the cart/sledge might require (e.g. a/c data or external system)
- An emergency procedure must be envisaged to decelerate the system in case the aircraft pitch is not properly ensured
- In order to avoid an unwanted separation between the aircraft and the cart a specific new operational function shall be ensured: before starting the deceleration of the sledge (whatever is the reason) the F3.1 "secure the A/c on cart" must be executed. This will work if the A/C did not shift its position or anyhow the mechanism to secure the A/C works properly
- Actuation of cart shall be reliable, a check of the cart repositioning must be performed; the information of cart positioning on the sledge must be available to both the pilot and ATC operator.

AIRCRAFT

Additional preliminary requirements for the Aircraft

- A system to ensure the coherence between the cart attitude, speed and the horizontal control surface shall be provided
- In order to avoid an unwanted separation between the aircraft and the cart a specific new operational function shall be ensured: before starting the deceleration

of the sledge (whatever is the reason) the F3.1 "secure the A/c on cart" must be executed. This will work if the A/C did not shift his position or anyhow the mechanism to secure the A/C works properly.

- The system to check the separation shall have a very high reliability
- Actuation of cart shall be reliable, a check of the cart repositioning must be performed; the information of cart positioning on the sledge must be available to both the pilot and ATC operator.

According to the Functional FMEA, one of the most critical function during landing phase is is F4.1(to synchronize the rendezvous between the aircraft and the Cart/Sledge system) which is allocated to the rendezvous control system.

The automation of the GBS system allows performing a complete automatic landing as if the aircraft has a traditional undercarriage.
The control system can be subdivided into two main systems; the aircraft control system and the sledge control system.
From the analysis it results one of the most critical system, thus specific requirements have been derived for it and a detailed description is provided in the following.

Aircraft control system
One key challenge is to improve lateral system accuracy during landing. A requirement has been determined for the lateral touchdown accuracy to be less than 1 meter. This requirement on accuracy is much higher than current specifications for large aircraft. In particular, crosswind conditions can introduce lateral deviation at touch-down. Typically aircraft performs the landing approach with a correction angle (crab angle) relative to the runway heading in order to compensate for the lateral wind component. Before touchdown on the runway a de-crab manoeuvre is performed to align the conventional aircraft with the runway centreline. Being a highly dynamic manoeuvre, the de-crab manoeuvre affects virtually all degrees of freedom of the aircraft motion just prior to touchdown and therefore has a great negative impact on touchdown accuracy.
The ability of the proposed system to rotate with respect to the runway direction the rendezvous platform above the sledge allows the aircraft to completely omit the de-crab manoeuvre. As a result, this degree of freedom of the sledge system will increase the lateral (and longitudinal) landing accuracy and reduce the complexity of the aircrafts auto land system.

The longitudinal landing accuracy is less critical, due to the longitudinal degree of freedom of the sledge, which can compensate for landing position and velocity deviations. However, to keep the rendezvous and deceleration length at minimum, longitudinal landing accuracy should also be as precise as possible.
Landing position accuracy is also directly connected to sensor accuracy. Potential improvements to the aircraft sensor suite need to be investigated. This comprises advances in satellite navigation systems as well as optical (visual / laser) guidance systems for close range positioning of aircraft and sledge. Actually the sensors should be placed also on the sledge.

As a consequence, the general requirements on the aircraft autoland system resemble to those of a conventional autoland system, but with the additional ability:

- to fly with a crab angle until touchdown,
- to integrate new high precision sensors,
- a lateral touchdown accuracy of less than 1m.

Sledge control system
For a successful landing, the sledge system has to fulfil three main tasks:

- position itself accurately with the right speed below the aircraft at the moment of touch-down,
- align the yaw angle of the landing platform with the heading of the aircraft during landing,
- align the pitch angle of the landing platform with the pitch angle of the aircraft.

Given the lateral accuracy requirement of less than 1 meter for the aircraft autoland system, a lateral alignment of the platform with the aircraft position (which would increase GBS complexity) is at this moment considered to be not necessary. This however, should be confirmed by upcoming simulation test.

Longitudinal positioning and speed adjustment of the sledge will be achieved by electromagnetic acceleration along the maglev rail. Alignment with the aircraft heading will be done by rotation of the landing platform along its vertical axis. Geometrically, for an aircraft similar in size to the A320 an alignment error of 1° will lead to a positional error of ca. 0.2 meter at the front contact point, given that the contact point is located at the former front wheel position. The error of the contact points would be even less due to the fact that they are located closer to the centre of gravity. Therefore, a requirement of less than 1° for the yaw alignment accuracy is considered to be sufficient.

Alignment with the aircraft pitch angle will be done by rotating the landing platform along its pitch axis. Misalignment during landing will lead to a corresponding rotation of the aircraft along the pitch axis after touch down. Similar to the yaw alignment, accuracy better than 1° for the pitch alignment is considered to be sufficient.
During take-off, yaw and pitch angle of the platform/aircraft will be adjusted to minimize the forces between the aircraft and the sledge, in order to reduce the overall load requirements of the aircraft structure.

RENDEZVOUS

The general recipe to design a safe rendezvous concept is:
1. Redundancy in systems and procedures
2. Failsafe degrading
3. A-priori safety assessment and mitigation
4. Use of dissimilar systems for the same purpose
5. Follow the standards, draft new ones

The goal of the autoland system for the aircraft is to perform automatic landings on the sledge with a longitudinal and lateral precision of 1 m relative to the landing platform with a chance of landing outside this circle of 10^{-7} average and 10^{-6} limit (Gaussian distributions).
Also the chance to land with a vertical velocity higher than 6 ft/s and the chance that the pitch and yaw angle differ more than 1 degree to the platform adjustments shall be smaller than 10^{-7} average and 10^{-6} limit (Gaussian distributions).

Redundancy
The Rendezvous landing concept is automated three fold for redundancy reason. The safety oversight will be provided by a dedicated Rendezvous Health Monitoring System, positioned on the sledge:

- The aircraft flies an ILS and/or D-GPS CAT IIIc landing that is well proven to bring the aircraft within about 6 m lateral deviation from the runway centre axis. It is expected that new ILS plus D-GPS will perform with a lateral deviation of 1 m. The certification standard for CATIIIc autoland is 10^{-7} missed landing per landing.
- During the rendezvous phase of the landing, an additional high precision sensor will be used parallel to the ILS / D-GPS to synchronize aircraft and sledge positions and velocities.
- Both systems provide their projected landing spot data (Rendezvous point) to the Platform Health Monitoring System that will compare both and decide on the reliability and integrity.

- A third system is proposed to be mounted under the aircraft. It checks if the aircraft harpoons are above the grids short before the landing. This checking system might be done for instance by an infrared / optical / radar system that recognizes the grids and decides for go-ahead or abort, just prior to contact.

If the ILS / D-GPS or the high precision localization system is not indicated as ok, or if they do not predict the same landing spot, the third system is used to decide which system is erratic. The Rendezvous Health Monitoring System is added to the design to favour timely detection of failures. It is redundant to the built-in safety measures in the individual Rendezvous systems.
Additional redundancy in case of a complete ground system failure could be provided by an emergency landing system. It could consist of a ground based vehicle with a landing platform that is not magnetically levitated and propelled. Instead, it would be driven by conventional motors and wheels and could roll down the landing strip, taking over the role of the sledge if that has a failure.

Failsafe degrading
Failsafe degrading means that the Rendezvous concept is developed in such a way that in case of a failure in a part, basic functionality is remaining operational as much as possible. It also means that a failure in a part will not cause a significant out-of trim condition or deviation in flight path or attitude. But the landing is not completed automatically. The Rendezvous concept is designed to be fail passive in the sense that the pilot assumes control over the aircraft after a failure and aborts the landing. The standard ILS / D-GPS automation is complying with autoland standards. It is to be investigated if the high precision positioning system and the third aircraft carried infrared / optical / radar monitoring comply with an autoland standard up to a lateral and longitudinal accuracy of +/-0.5 m with a probability of 10^{-7} average and 10^{-6} limit to land outside this circle.
In the emergency case of a landing not on the platform but on the concrete, the aircraft shall not collide with the sledge. Therefore a collision avoidance system could be specified to keep the sledge separated from the aircraft when it eventually hits the concrete.

Use of dissimilar systems for the same purpose
The use of different systems to detect or measure the same parameters or condition has the advantage that they do not suffer from the same errors. This will enlarge the chance to detect threats and safety related items. An example is the use of ILS/ DGPS parallel to the high precision localisation system. The third, infrared/optical/radar

monitoring system can then aid to determine which of the two main systems is in fault if an error occurs.

Follow the standards

Existing standards for autoland are:

- Manual of All-Weather Operations, ICAO Doc 9365, second edition 1991
- Certification Specifications for All Weather Operations, EASA Decision ED 2003/6/RM
- FAA Adivisory Circular AC-120-28D, Criteria for approval of CATIII weather minima for take-off, landing and roll-out

These are to be applied during the validation of the system automatic landing. For landing on the platform on the magnetic track and the Rendezvous concept, no standard exists yet.

Some suggestions that result from this safety assessment:

- Sledge collision avoidance system is in charge to manoeuvre the platform and to create a safe distance between the aircraft and the sledge in case the aircraft is missing the landing platform on the sledge. The aircraft might not be able to go around and may thus perform a hard landing on the concrete. “Safe” means that the platform is accelerating away in front of the hard landing aircraft or it stays behind it, with the platform braking, to keep a distance between sledge and aircraft.
- Release the harpoons (claws) from the aircraft if for some reason the harpoons (claws) would not release the aircraft from the grids.

11.6 Additional Safety Considerations

It is worth complementing the safety analysis with some additional considerations derived by the adopted approach.

The dynamic nature of the system

A crucial issue is the "dynamic nature" of the moving systems:

- Maglev Track / Sledge / Cart / Aircraft
- Maglev Track / Sledge / Cart
- Maglev Track / Sledge
- Cart / Aircraft
- Sledge / Cart

During the mission timeline the system goes through different configurations according to a state diagram coherent with the mission phases.

The transitions between system configurations are to be highly reliable, detectable, and traceable. A remote control system will have control (full or in cooperation with aircraft pilot and operators) of mission phases and transitions. The remote control system will have to check consistency between current configuration and mission phase, and monitor that appropriate procedure and operations are implemented.

Some locking mechanisms are to be provided for each of the previous configurations.

- Cart / Aircraft locking system
- Maglev Track / Sledge locking system (unlocked only for maintenance and or substitution)
- Sledge / Cart locking system

For both aircraft and high speed maglev vehicles it appears to be unfeasible to design a practical system that could withstand a high-speed collision.

Accordingly, the proper approach is to ensure that collisions do not occur, or effectively keeping collisions occurrence under a fixed threshold.

The absolutely safe state - as in any transportation system - is the lowest state in terms of energy: parking/standing still with all energy/propulsion/levitation systems turned off.

The sledge is equipped, among other subsystems, with two safety wheel systems which allow bringing the overall system (sledge/cart/aircraft) to the safest state:

- one wheel system will act to sustain the weight of the overall system in case of failure of the levitation equipment; a safety braking subsystem will also be

installed on these wheels to stop the sledge in case of failure of both the levitation and magnetic acceleration subsystems;

- a second wheel system will act to sustain lateral dynamic forces in case of failure of the lateral maglev control system thus avoiding de-rail of the sledge from the maglev track.

Undesired events during the take off

In the following by vehicle it is meant sledge with cart and a/c.

During take-off the undesired events can be:

- to stop take off while you should have gone on
- to go on with take-off procedure while you should have stopped it.

So the undesired events are:

- Late braking
- Untimely braking

In order to avoid Late Braking a *Safe Programmed Braking* must be enforced

Causes that can lead to the Untimely Braking are:

- loss of levitation/guidance function;
- over speed;
- magnet striking by part of the sledge;
- failure of programmed braking function.

In the following of this section, functions or subsystems involved in the mentioned undesired events are discussed.

Safe Programmed Braking

In order to perform the required programmed braking, the vehicle must, under all circumstances, feature a controllable braking capability. Even in the event of breakdown, the attainable maximum value of the braking force for emergency braking must remain within established limits. The maximum attainable braking force value must be compatible with the load assumptions for the guideway and vehicle. The attainable minimum value of braking force must be in agreement with designed margin.

The following subsystems are required for the programmed braking function:

- vehicle location detector
- vehicle operational control system
- emergency braking system

- violation of clearance envelope detector

The untimely braking event can have different causes, the possibility of which must be adequately ruled out.

Levitation and Guidance Function

The required safe life property of levitation function must be achieved through adequate reliability. The levitation/guidance function can be safeguarded by an adequate number of autonomous units, ensuring that - considering the maximum conceivable number of failed levitation/guidance units during a mission - the overall levitation/guidance function will nevertheless be maintained.

The levitation/guidance function can be lost as a result of the following:

- - loss of power supply
- - faulty device control
- - software defects
- - loss of synchronism followed by set-down
- - entry into short-circuit loop before the neutral point.
- - breach of the proper gap between magnetic subsystems

The first two factors can in turn result from the effect of the following hazards: fire, lightning, or insufficient electromagnetic compatibility of the electronic control and monitoring equipment.

Loss of Energy Supply

It is necessary to ensure that the energy supply as a whole cannot fail, since in this case the sledge would set down. However, since the possibility of individual failures in the electrical system cannot be ruled out with adequate certainty, there is a need for redundancy; i.e., on a general basis for each section, an adequate number of mutually independent and electrically/mechanically safely separated power systems must be provided, so that, in the event of power system failures, levitation and track guidance are maintained without impairing the other as yet intact power systems.

It is furthermore necessary to provide installations through which the output capacity of the power systems needed to maintain the levitation/guidance function is ensured during the mission.

The possibility of an untimely shutoff of all power networks necessary to maintain the levitation/guidance function during a mission e.g., through activating the central total shutdown command—must be prevented by a suitable technical installation. A total shutdown command must be activated by an active signal and may take effect only while the vehicle is in a stationary and set-down position.
Failures in the total shutdown control system must prevent total shutdown safely. Emergency shutdown installations must be provided for this possibility. Access to these emergency shutdown installations must be made so difficult that only trained members of the operations personnel can activate them.

Defective Controls

To be able to lift the aircraft off, all levitation/guidance units must receive an acceleration command. If this should stop due to a failure, then this would be as critical as an interruption of the entire power supply network. Thus, the take-off abort command must be generated as an active signal and be linked by a logical AND-operator to the *independent* device for determining speed present in each levitation/guidance unit. Only if the vehicle speed V is less than the permitted abort speed Vab then the abort command may take effect locally. In that case, there is a controlled set-down, either intentional or due to error, but in any event uncritical.

Software Defects

Systematic flaws, if present, especially affect the control and monitoring installations of the levitation/guidance units and the rendezvous mechanism. Software must be valid and correct, i.e., error-free in the mathematical sense. This will imply to assign a proper safety objective (transforming it in reliability requirement) to the software components and verify/validate the software versus that reliability requirement. The software component of the system has to be classified in terms of criticality (A-catastrophic, B-Hazardous,…) according to the severity of its failure effects.
Depending on the Software Criticality more or less strict engineering and
Product Assurance requirements are to be implemented for the software development process (e.g. in terms of test coverage targets).

Loss of Synchronism (between acquisition sensors)

There are some acquired data (i.e. position of the sledge, vehicle speed, …) which are managed by different systems; if any inconsistency occurs between these data, this could result in a catastrophic effect.

Thus, it must be ensured that this type of situation cannot occur or that it is demonstrably harmless.

A clear, complete state diagram with a detailed timeline, comprising all the necessary telemetry data info (parameters, units, acquisition rate, source of information, communication channels, thresholds,…) for each time step must be designed.

Short-circuit Loop

If a short circuit develops and if the vehicle enters this short-circuit loop, then - depending on the geometric conditions - the result will be unacceptable braking and vertical forces that can lead to a loss of the levitation/guidance property. This type of breakdown must be prevented through a corresponding design through monitoring short circuits and ground failures.

Magnetic Gap Control

Electromagnetic levitation represents an unstable state requiring continuous control, during which a nominal gap size must be maintained between the sledge and the track. As a result of failures

The magnetic force can increase to such an extent that the gap tends to 0. Because of the resulting excessive magnetic current, the relevant overcurrent protection unit would then turn the magnet off, but the magnet striking prior to that, results in the application of unacceptable local forces.

Safe Magnetic Gap Monitoring

There is a need to introduce the shutoff or disconnect process beginning at a minimum gap to be observed in order to preserve the no-contact property, through a suitable fail-safe monitoring device. If there is a failure in the monitoring device, then this must lead to nullification of the magnetic field. The monitoring device must be allocated

autonomously to each magnet and be unconditionally activated, free of outside influences, whenever the magnetic gap control system is turned on.

Clearance Envelope and Tolerances of Reaction Surfaces

The concept of safe hovering, as can be deduced from other requirements, requires compliance with the clearance profile and with the tolerances of the reaction surfaces. This requirement, in connection with safe hovering, is significant because unacceptable maladjustments and displacements on the guide way not only mechanically endanger the vehicle but can also lead to magnet shutoff and unacceptable vehicle braking.

External and System-Specific Influencing Factors

The possibility of obstacles on or along the guide way, through which the clearance envelope is violated, must be ruled out. This is done, for example, by monitoring the guide way. This check must be determined as a function of the weather and the environmental situation.

Electromagnetic Compatibility, Electrostatic Charge, Lightning Protection. Fire Protection

In addition to the possible dangers which have been discussed so far and which are essentially inherent to the system, one must also deal with external factors which can influence this property. Special attention must be devoted here to electrical or electromagnetic influences, through which the function of the installations can be disrupted or destroyed. The most basic effect of that type is caused by lightning. Furthermore, safety brings with it special requirements for fire protection.

Levitation Function During Lightning Strike

As for lightning protection, both the direct threat to persons in the aircraft when lightning strikes, and the indirect hazard caused from the secondary effect of lightning must be addressed. Lightning strike can cause a breakdown of GBS installations which affects running performance, levitation, and operation of the braking system; i.e., impairs safe hovering as a whole. The basic requirement specifies that the lightning current be shunted off with the least possible resistance - i.e., with low dissipation.

Environmental *Requirements*

Environmental influences must impair neither the levitation/guidance function, and thus the levitation or running capacity, nor the braking capacity.

Safe hovering must not be impaired by weather-related effects on the vehicle/guideway system.

This applies particularly to wintertime operation. Snow and ice on the guideway and on the functional elements must not cause any intolerable magnetic gap deviations.

Damage to the vehicle, especially the underside of the sledge, from loose pieces of ice or ice separated must be prevented by suitable coverings.

In the following Tables the main safety critical aspects are summarised for:

- Ground Based System and Take-off
- Operational Issues during Landing
- Weather issues and condition of the track

In the tables for each safety critical aspect the following elements are provided:

- Recommended detection equipment
- Mitigation actions
- Contingency actions
- Further recommendations

Ground Based System and Take-Off

ITEM	SAFETY CRITICAL ASPECT	DETECTION	MITIGATION	CONTINGENCY	RECOMMENDATION
T1.	Proper connection/disconnection systems and procedures (fail safe).	Electrical contact made when connected	Use of primary flight controls	Three harpoons and grids being equipped, two are sufficient	Extra pilot check on proper connections and fixations
T2	Proper operations for avoiding runway and maglev track contamination / incursion	Control ride before starting operations	Cleaning		
T3.	Proper operations and equipment to guaranty needed acceleration and abort take-off sequence	Apply two independent inertial packages and an along track measurement of the sledge	See aborted take-off and landing	Pilot in the loop, can overrule the automation	Measure acceleration, velocity and position of the sledge and compare with model
T4	Proper instrumentation panel to monitor acceleration levels (fail safe)	See T3			Instrumentation panel for the pilot(s) and for the Air Traffic Controller
T5	Proper instrumentation panel to monitor configuration state for the GBS	GBS state measurement	No	No	No go item
T6	Proper instrumentation panel to monitor locking mechanisms	See T1	Use of primary flight controls	Three harpoons and grids being equipped, two are sufficient	Proper instrumentation panel for pilot(s) and Air Traffic Controllers

ITEM	SAFETY CRITICAL ASPECT	DETECTION	MITIGATION	CONTINGENCY	RECOMMENDATION
T7	Mechanisms and actuators for pitching and yawing the cart	Gyroscopes, angle encoders	No	Three systems available: gyros, angular encoders and Aircraft yaw and pitch sensors	Two parallel measurement systems on the cart, one in the aircraft, plus voting between the three sources
T8	Reaction Rails	No	The sledge will have wheels to withstand hard landings and to act as alternate emergency transport means	The sledge will have wheels to withstand hard landings and to act as alternate emergency transport means	Design mitigation and contingency measures for the sledge on the maglev track, like extra wheels and brakes to be used in emergency situations
T9.	Braking Rails	No			
T10	Emergency Braking	No			
T11	Position Indicators	Apply two independent inertial packages and an along track measurement of the sledge	See aborted take-off and landing	Pilot in the loop, can overrule the automation	Measure acceleration, velocity and position of the sledge and compare with model
T12	Location of Sledge				
T13	Propulsion	Automatic diagnosis system	Redundancy, emergency brakes	Redundancy, emergency brakes	Check the maglev system and its power supply before, during and after the take-off and landing
T14.	Power Chain	Automatic diagnosis system	Redundancy	Redundancy	
T15	Supply of Propulsion with Adjusted Electric Energy	Automatic diagnosis system	Redundancy	Redundancy	

ITEM	SAFETY CRITICAL ASPECT	DETECTION	MITIGATION	CONTINGENCY	RECOMMENDATION
T16	Sledge	Sensors to measure and detect overload	Design for safety margin when overloaded	At least three operational sledges available per track and two carts per type of aircraft	Measure overload and design for a safety margin in case of overload
T17.	Structure			Use other track	
T18	Cart Fixation			Other cart other sledge	
T19.	Levitation Frames			Other sledge	
T20.	Rendez Vous Control	Self test by RDV, extra camera observation	Camera observation of the harpoons approaching the grids	Two way relative position measurement, and camera observation	Apply redundancy in the RDV system plus camera observation of the final touch down

Operational issues during Landing

ITEM	SAFETY CRITICAL ASPECT	DETECTION	MITIGATION	CONTINGENCY	RECOMMENDATION
1b See also T1	Partial disconnection failure (aircraft from cart/sledge) after landing	Electrical contact made when connected	Use of primary flight controls	Three harpoons and grids being equipped, two are sufficient	Extra pilot check on proper connections and fixations
8b See also T1	Partial connection failure (aircraft and cart/sledge) during landing	Electrical contact made when connected	Use of primary flight controls	Three harpoons and grids being equipped, two are sufficient	Extra pilot check on proper connections and fixations
2 See also T3	High accelerations / decelerations during take-off and landing.	Apply two independent inertial packages and an along track measurement of the sledge	See aborted take-off and landing	Pilot in the loop, can overrule the automation	Measure acceleration, velocity and position of the sledge and compare with model
9a	Autoland failure with proper alternative landing option	Detection by ILS cat IIIc equivalent system and camera observation of the final touch down	Make go-around	The extra autoland checks (like ILS) and the camera's being the last source of information	Apply ILS cat IIIc equivalent autoland and camera system to watch the harpoons relative to the grids
13	Pilot late decision (before touchdown)	Detection by automation	Warn the pilot in time	Auto land system parallel with camera system	See above (9a)
14	Correct cart/sledge not available (with proper alternative landing option).	Detection by communicatio n with Tower and by data linking with type and power setting information	Alternate magnetic track or airport with the right cart / sledge	Alternate magnetic track or airport with the right cart / sledge	Design skids, arresting devices and emergency procedures for hard landing on runways, terrain and water

Weather issues and condition of the track

ITEM	SAFETY CRITICAL ASPECT	DETECTION	MITIGATION	CONTINGENCY	RECOMMENDATION
W1	Thunderstorm	Equipment for Awareness of meteorological conditions	Protect the maglev energy power supply system. Specific back-up energy supply systems must be defined	Specific actions are required in case of failure of the maglev energy power supply system. Specific procedures must be defined and adopted depending on the time of failure with respect to the take-off and landing phases.	Protect the maglev energy power supply system. Specific back-up energy supply systems must be defined
W2	Cross Wind	accurate wind data by Radar sensors	High accuracy in aligning the cart to the aircraft and ensuring that the aircraft is automatically piloted in a stable crabbed approach and accurately on the cart	Abort landing or take-off Emergency landing	Automation for high precision landing
W2	Wind Shear	accurate measurements of vortices and wind shear	Make the pilot and controller aware of wind shears	Abort landing or take-off Emergency landing	Automation for high precision landing
W3	GBS degradation	accurate checks and inspections	Maintenance planning	Abort landing or take-off Emergency landing	Autonomous Integrity Monitoring
W4	Slush/Water on runway/maglev	sensors and inspections to avoid large puddles.	In order to avoid accumulation of water and mud on the rail/track a system connected to the sledge might be adopted to remove water and dust/debris.	Abort landing or take-off Emergency landing	a system connected to the sledge might be adopted to remove water and dust/debris.

ITEM	SAFETY CRITICAL ASPECT	DETECTION	MITIGATION	CONTINGENCY	RECOMMENDATION
W5	Snow or Ice on maglev	Temperature sensors and inspection to check accumulation	A system connected to the sledge might be adopted to remove snow and ice De-icing fluids for the cart/sledge mechanisms. De-icing and anti-icing systems adopted for both cart/sledge and maglev track/rail.	Abort landing or take-off Emergency landing	Snow removal device on the sledge, heating and de-icing
W6	Flooding of the maglev track	Sensors for checking the water accumulation under the maglev track should be adopted	Passive and active draining should be in place	Abort landing or take-off Emergency landing	Passive and active draining
W7	Volcanic ash	Detection of volcanic ash is already part of standard operations	standard system to remove the ash from the runway, specific cleaning device to remove the ash from below the maglev track and from the magnetic rail.	Abort landing or take-off Emergency landing	Ash removal system on the sledge, cleaning device
W8	Low visibility	A reliable system for weather conditions detection and forecast	an augmented vision system for ensuring the awareness of both pilot and personnel in charge of the sledge/cart system during night both the sledge and the cart must be equipped with specific position lights	Abort landing or take-off Emergency landing	Augmented vision system for the pilot; light the sledge
W9	Earthquake threats on maglev Earthquake threats on maglev	The airport needs to be monitored by seismometers and an alert system has to be set-up.	Automatic system to make the pilot aware of the situation Automatic procedure for aborting take-off and landing when appropriate	Abort landing or take-off Emergency landing	Earthquake alerting system for the pilot, development of abort take-off and landing procedures

12 SECURITY ASPECTS

Usually security hazards include the followings: hi-jacking, terrorist attacks, stowaways and illegal immigrants, passengers carrying weapons/banned items in hand luggage bombs, left luggage/suspicious packages in terminal, smuggling (weapons, money, drugs), aggressive or drunk passengers, assaults on staff, abandoned vehicles, cyber-attacks to system software.

They are not specific to maglev technology so typical measures are to be taken in order to manage their related risks.

In order to prevent acts of sabotage, the case study operators will have to rely on equipment sensors, networks and various levels of security.

System components are to be monitored through use of those sensors or other means of observation such as physical inspections. Computer networks have to employ Intrusion Detection System (IDS), encryption and other forms of network security to detect and deter possible attackers.

The physical assets are to be protected as well by fences, doors and other barriers to entry which employ locks, card swipe systems, fingerprint/retinal scans or other means to allow access to the selected people while denying access to others.

The landing/take-off facility will have to employ a vast array of sensors, computers and other equipment which generate data, due to the considerable safety issues and cost of the facility maintenance and protection, a resilient design is essential.

The design must incorporate data which lead to proactive rather than reactive control and account for both mechanical and human threats.

So a first layer is physical security which records time and activity around various access points in the area. Physical security sensors acquire access time, physical breaches and the like.

Currently, debris on runways, which are sources of damages, loss of capacity, even of accidents, are removed during visual inspections. Systems for automated detection of objects and debris on runway will be necessary.

The second is cyber security which will need an Intrusion Detection System and network monitoring software of the whole facility and its components. The rendezvous system must be strictly protected as it drives the landing facility which is not a static site, so it is

vulnerable to attacks. Cyber systems have to acquire and monitor network traffic along with analysis to identify potential security hazards and threats.

13 DEFINITION OF THE BUSINESS MODEL TO EVALUATE CUSTOMER'S BENEFITS.

The scheme proposed for the complementary measure management already contains the issues to be addressed to promote the new technology adoption.
Besides the considerations about liability, data protection and legal issues, the aspect related to public acceptance has been analysed.
It has been highlighted that public acceptance for the new technology is related to public perception of risks which is the subjective assessment between:

- Society's perception of the level of exposure to the hazard;
- Society's perception of the benefits due to the hazardous activity.

Concerning the perception of the level of exposure to the hazard a strategy for communicating with the public has to be set up as stated in paragraph 3.8.
According to the derived conclusions about the need to exploit benefits of the new technology, a business model has to be outlined to identify them.
To start defining a business model for a new technology some preliminary considerations have to be done.
Business model means how the investment project would generate a profit.
Greener products/processes provide the buyer with economic and environmental benefits through their use. The case under study contains a set of innovative products which can achieve better environmental performance by, for example, saving resources and minimising emissions.

One of the most promising benefit for the public will be the noise reduction due to this system adoption.
Calculation were made based on the most promising noise scenario (Accelerated take off) to assess the effects on noise abatement using the new concept.
There are many methods in literature how to assess the cost of noise. These include the reduction of house value due to aircraft noise (the Hedonic methods), the number of people that are willing to pay for noise reduction, the welfare measurement etc. Aircraft noise: annoyance, house prices and valuation by Peter Brooker of Cranfield university explains very well the different methods to calculate the effect of noise on pricing.
In their report "Monetary valuation of aircraft noise: A hedonic analysis around Amsterdam airport" Jasper E.C. Dekkers and J. Willemijn van der Straaten, University of Amsterdam, used a threshold value for aircraft noise starting at 45dB and calculated

that a marginal benefit of 1 dB noise reduction near Schiphol on housing cost alone was 1.459 Euro per house.
For the system under study, the take-off noise is most effected by the different configuration of the aircraft as well as the trajectory flown thanks to different speed of the aircraft. The take-off noise calculations were derived for the unconventional take-off.
The biggest impact is at take-off where a reduction of the areas concerned is about 65%. The performed analysis came to the conclusion that 24% less awakenings would result from the better take off procedure in the 55dB region.
Assuming that 24% of the houses in that area is affected, considering that the total population is 309.998 people, If 24% of the population is effected, the number of people directly involved would be 24x 309.998= 74.400. Suppose that on average there are 3 people living in a house. The number of houses affected would be 24.800 houses
According to the Website of Huizenzoeker.nl the average price of a house in Noord Holland is € 240.000. According to Wout van der Toorn Vrijthof of TU Delft the average lifetime of a house in Holland is 65 years.
The total average houses value would be 240.000 x 24.800 = € 5.952.000.000. Assume all houses would be affected by a 1dB reduction of noise, the total benefit in terms of a hedonic analysis would be 24.800 x 1459= € 36.183.200. On average the depreciation on all the houses would be reduced by 36 million divided by 65 years or € 556.661 per year.
The number of cycles per year for the unconventional take-off and landing is 80.665.
The benefit per cycle of an unconventional take-off, fly over and landing would be €556.661/ 80.665 = € 6.90 per cycle.

Concerning revenue for this project on a general basis it is planned for:

- organisation of production and sales of Maglev AIRCRAFT and parts for them,
- sale of licenses for maglev systems production (flight and ground based systems),
- sale of licenses to use the new method to modify a traditional aircraft,
- sales of developed technical solutions used in a new aircraft,
- development and sales of new types flying vehicles using this method,
- production organisation of navigation equipment,

The classic approach requires a plan for the successful operation of a business, identifying sources of revenue, the intended customer base, products, and details of financing.

A plan for the investment project would contain:
1. company establishment and team building of specialists to design and manufacture a prototype of a Maglev AIRCRAFT and Ground based systems
2. development, creation and production of a prototype as well as test operation and improvement of a maglev aircraft prototype and Ground based systems
3. production of an improved Maglev AIRCRAFT and Ground based systems
4. creating a brand (brand name)
5. creation of a model family for different purposes and customer groups
6. organisation of production and sales of 2-seat and n-seat aircrafts, organisation of licenses sales
7. application of new materials in aircrafts structure (coal-plastic etc.)
8. creation of a special radio locating equipment
9. creation of infrastructure for operation, maintenance, repair and personnel training

Standard runway cost

The performed cost estimates only include those cost that are deemed to be different for the traditional runway and the innovative Maglev system. Whatever option is chosen, there is for example a need to acquire land and to create terminal buildings. Therefore, the costs considered for a runway are only related to the construction of a runway and the associated taxiways. The total cost of creating an airport would be substantially higher.

Data refer to a simple airport with one taxi taxiway without rapid exits along the runway. Exits are only provided at both ends of the runway. Cost of ILS system or platforms to service aircraft were excluded. Data were based on 2009 price levels including a percentage of 9% inflation to arrive at 2014 price levels.

Based on these data the cost of a 2400 meter long runway plus a 2 x7.5 meter wide shoulder, 3 rapid exits and taxiways with shoulders were calculated. The runway will be able to accommodate traffic taking off and landing from both runway directions. That also implies ILS equipment to guide aircraft from both sides.

In total the runway infrastructure alone would cost about € 66 million according to the rule of thumb. ILS installations and lighting would cost about € 10 million. Based on the rule of thumb the total cost would be in the order of € 75 million[3].During the first 7,5 years the maintenance cost are small.

[3] costs are excluding : possible removal of an older runway, fences;acquisition of land; VAT.

After 7,5 years reinvestments are to be foreseen: the top layer of asphalt at the touch down zone on both sides; replacement of markings and some lightning;the top-layer of asphalt for the full length of the runway; remaking of taxi way and exits ; replacement of lamps and cabling; replacement of concrete pavements and of the foundation (every 40 years), ;
The total depreciation (without taking into account inflation or RoI on capital invested) is about € 2,8 million per year.
Thus we can compute the fixed cost per cycle: if we assume 23 cycles per hour, 17 hour operations during 365 days per year, the fixed cost per cycle are about€ 19,50 per cycle for an airport operating at full capacity.

Innovative launch facility costs.

The cost of the Maglev system was calculated for each component of the product tree. The cost calculations can be summarized as follows:

	Conventional 1	Conventional 2	Accelerated	Unconventional
Guideway	27.033.705	24.679.396	20.670.273	38.535.396
Energy chain	31.973.400	32.279.000	47.110.150	47.110.150
Propulsion	17.757.084	12.566.217	12.751.653	24.821.187
Controls	9.450.000	7.700.000	7.300.000	10.650.000
Maintenance yard	1.919.000	1.919.000	1.919.000	1.919.000
Lighting	2.000.000	2.000.000	2.000.000	2.000.000
Taxiway	20.583.000	17.820.480	14.674.000	26.174.400
Carts	7.760.000	8.730.000	9.700.000	8.730.000
Sledge	9.800.000	10.400.000	10.960.000	10.960.000
Total investments	**128.358.000**	**118.175.100**	**127.166.100**	**160.981.100**

Table 1 Total cost of the launch facility

The Fixed cost depreciation estimates are depending on the following lifetimes:

- Guideway 80 years
- Energy chain 50 years
- Propulsion 50 years
- Control systems 30 years
- Maintenance yard 80 years
- Lighting 15 years

- Taxiway 15 years
- Sledge 30 years
- Carts 20 years

The total depreciation cost per year is thus assessed as follows:

	Conventional 1	Conventional 2	Accelerated	Unconventional
Guideway	337.921	308.492	258.378	481.692
Energy chain	639.468	645.580	942.203	942.203
Propulsion	355.140	251.324	255.033	496.424
Control system	315.000	256.667	243.333	355.000
Maintenance yard	24.000	24.000	24.000	24.000
Lighting	133.333	133.333	133.333	133.333
Taxiway	1.372.200	1.188.000	978.270	1.744.935
Sledge	326.666	346.666	365.333	365.333
Carts	388.000	436.500	485.000	436.500
TOTAL	3.576.728	3.590.562	3.684.883	4.979.420

Table 2 Total depreciation cost per year of the launch facility

The Crew cost for the Maglev operations per year is computed as follows. A crew of 3 full time employees was assumed at a cost of € 210.000 per year; thus the Total fixed cost per cycle is presented in the table below.

	Conventional 1	Conventional 2	Accelerated	Unconventional
Infrastructure	3.576.728	3.590.562	3.684.883	4.979.420
Crew	210.000	210.000	210.000	210.000
Total fixed cost	3.786.728	3.800.562	3.894.883	5.189.420
Number of cycles per hour, during 17 hours per hours during 365 days	13	15	17	13

Fixed cost per cycle	€ 46,95	€ 40,85	€ 36,95	€ 64,35

Table 3 Total fixed cost per cycle of the launch system

Annual Maintenance cost: GABRIEL estimated the annual maintenance cost for the different Maglev systems.

	Conventional I	Conventional II	Accelerated	Unconventional
Guideway	254.835	208.916	172.679	351.765
Energy chain	401.760	396.960	591.960	611.160
Propulsion	162.646	124.300	119.910	211.089
Sledge	147.000	147.000	147.000	147.000
Cart	880.000	1.080.000	1.260.000	880.000
Operation control system	141.750	115.500	109.500	159.750
Total maintenance costs	**1.987.991**	**2.072.676**	**2.401.049**	**2.360.764**

Table 4 Annual maintenance cost of the system.

The maximum number of cycles that is possible during 17 hour operations during 365 days/year is provided in the following table.

	Conventional 1	Conventional 2	Accelerated	Unconventional
Max number of cycles per hour	13	15	17	13
Cycles per year	80.665	93.075	105.485	80.665
Maintenance cost per cycle	**24,65**	**22,27**	**22,76**	**29,27**

Table 5 Maintenance cost per cycle of the system.

Using the source above, the total energy cost for the LTO cycle are calculated.

Energy cost	Conventional 1	Conventional 2	Accelerated	Unconventional
€	21,36	15,36	17,40	31,44

Table 6 Total energy cost per cycle of the system.

Fuel for take-off and landing: The aircraft will be modified since no landing gear is needed assumed a MTOW for a standard A-320 aircraft of 73,7 tons for a 5000km trip with 150 passengers. The aircraft will have no undercarriage or fairings. This saves weight and reduces drag. The result is that the MTOW would ultimately be reduced by 7% and the fuel weight for a 5000km trip would be reduced by 11%. These data include a smaller and lighter engine as the Maglev system in most cases provides initial acceleration for the aircraft.

Conclusion on total cost for the system per LTO cycle (excluding noise cost):

	Conventional 1	Conventional 2	Accelerated	Unconventional
Fixed cost	46,95	40,85	36,95	64,35
Running cost	24,65	22,27	22,76	29,27
Energy for Maglev power	21,36	15,36	17,40	31,44
ATC service	same	same	same	same
Ground handling	0	0	0	0
Crew	same	same	same	same
LTO cycle fuel cost	246	320	246	364
LTO CO2 cost	4,90	6,30	4,90	7,20
Energy cost carts	9,15	8,70	8,25	9,45
Airport and handling fees	same	same	same	same
Total LTO	**€ 360,20**	**€ 413,48**	**€ 336,26**	**€ 505,71**

Table 7 total cost of the system per cycle.

Compared to the A320 aircraft the mission fuel is reduced. The fuel burn calculated in D3.6 for the segment from 3000ft to final approach was calculated to be the followings:

	Conventional	Conventional 1	Conventional 2	Accelerated	Unconventional
Fuel kg	**14.537 kg**	**13.400 kg**	**13.400 kg**	**13.400 kg**	**13.352 kg**
Fuel kg savings		**1.137 kg**	**1.137 kg**	**1.137 kg**	**1.185 kg**
Fuel cost savings in €		**€ 909,60**	**€ 909,60**	**€ 909,60**	**€ 948,00**

Table 8 Fuel cost savings due to the system

The results from the above analysis can be shown:

	Conventional 1	Conventional 2	Accelerated	Unconventional
LTO cost reference	€ 848	€ 848	€ 848	€ 848
LTO cost scenario	€ 360	€ 413	€ 336	€ 505
Difference in LTO	€ 488	€ 435	€ 512	€ 343
Difference in cruise	€ 910	€ 910	€ 910	€ 948
Total difference compared to standard procedure	**€ 1.398**	**€ 1.345**	**€ 1.422**	**€ 1.291**

Table 9 Total cost savings per cycle due to the system (relative for the conventional runway layout)

From these figures it can be concluded that the ***Maglev system shows significant cost savings compared to the traditional way of take-off and landing***. It also shows that the accelerated take-off has the best cost saving of € 1.422 per flight.
This cost benefit analysis was made to assess whether the GABRIEL system approach could bring cost benefits compared to the traditional way of take-off and landing on a traditional runway.

The analysis shows that the GABRIEL system can bring a cost reduction of about € 1.430 per flight, despite the considerable cost investment costs in the Maglev system.

The benefits can be explained as follows:

- The aircraft will not need an undercarriage and can fly with less powerful engines, which saves weight, reduces drag and allows for a lower fuel consumption .
- The taxi with an electric cart and electric push back from the gate saves a considerable amount of expensive fuel.
- The reinvestments in the Maglev system are less frequent than a traditional runway as the Maglev system is more sustainable.
- Acceleration with engine power is much more expensive than by a Maglev system.
- There are benefits in terms of reduced pollution and noise reductions. These can be translated into monetary value.

The substantial savings made possible by the Maglev system will justify further research.

In any new aircraft development program there are many important design decisions that determine profitability potential. The business model has to predict or find: 1) the costs to provide various aircraft and ground based system features; 2) the values that aircraft buyers place on these features; 3) the amount of money that buyers have to commit to them, 4) the open spaces in the market in which to place new designs and 5) the predicted profits from new designs.

Coming back to the risk framework delivered in this thesis, the public benefits to support the perceived risk computation have to be identified. The analysis for the business model will then focus on the customer's perspective.

For a new technology, whose adoption is foreseen in the medium/long term, the lack of complete certainty, that is, the existence of more than one possibility can spoil the effectiveness of the business model. The "true" outcome/state/result/value is not known.

Recently, a new approach has emerged, "business model experimentation": consisting in the methodical examination of alternative business models. Business model experimentation is a means to explore alternative value creation approaches quickly, inexpensively and, to the extent possible, through "thought experiments". In other words, treating the business model as a variable and not a constant —allows to anticipate, adjust to and capitalize on new technologies.

The business model to bring a new technology to market has to answer the following questions:

- Customer Segments – What customer segments does it serve?
- Value Propositions – What customer problems and needs will it satisfy?
- Channels – How will it get the value propositions to the customers (think communication, distribution, and sales)?
- Customer Relationships – How will it create and maintain relationships in each customer segment?
- Revenue Streams – Where will its revenue streams come from?
- Key Resources – What assets are required to do all of this?
- Key Activities – What are the most important things the company must do to make all of these elements work?
- Key Partnerships – What activities will be outsourced? What activities will be done within the enterprise?
- Cost Structure – All of the previous elements create the cost structure.

In any working business model, the answers to these questions are fixed. But for new technology whose maturity can be put in the medium long term some of the answers could be variable.
The first step in the business model exploration process is to examine possible alternative answers to the questions above. The questions that help to shape a business model represent a series of decisions, each of which has a set of possible outcomes. Selecting one possibility from each category and then linking them together forms one potential new way to proceed. And, of course, selecting different combinations creates other possible outcomes.
Focussing on the maglev system customer it is worth considering how an airline might generate alternative business models. Currently, airlines serve a range of customers with the same basic model. For example, regardless of whether the customer is going on vacation with her family, traveling on business or responding to an emergency, airlines use the standard pay-per-seat model with which we are all familiar. Minor levels of customization exist — for example, larger seats and priority boarding for those who pay for them — but the core model is the same for all.
To explore business model innovation, an airline could start by picking a specific customer group and then beginning to explore potential options other than its current model.
Working out what elements should be in a business model — and then examining different combinations of them, generating new Business Models By Changing One Variable — can be a rapid and robust way to explore the possibilities of business model innovation. A quick run-through of simple combinations of high-level strategic questions can produce a wide range of potential business models. But each of the questions could be examined in more details in a systematic way to yield deeper insight into some specific aspect of the business.
This will conduct to finalise agreements, including:
Intellectual Property Agreements, Patents, Copyright, Trademarks, Intellectual Property Rights.
Developing such a system of systems requires close interdisciplinary cooperation among researchers in aerospace, ICT, environment, human computer interaction, security, and privacy. The problem of supporting specific disciplines (like aeronautics) to perceive and consider the repercussions of safety and security and other measures in

designing issues is an example of a problem that requires this diverse research attention and even today is still sparsely applied. However in the immediate future this is likely to become a more critical research direction as the increasing deployment of pervasive computing technologies into the world around us which gives an indication of a future in which we can expect everyday interactions with complex and evolving systems and services.

14 FUTURE SCENARIOS OF USE

The framework has the potential to be used by a large plethora:

- system designers,
- service suppliers,
- information infrastructure operators,
- aviation supply chain,
- supporting specialists

Furthermore, the proposed framework is structured in a way that can be applied during different phases of a system life-cycle:

1. At design time and initial deployment to assess particular parts of the risk spectrum e.g. rare and cascade event assessment.
2. During monitoring of services and information infrastructure to identify impact of changes to evidence base and how this propagates to judgement a confidence in the system.
3. During contingency planning for the recovery of service and infrastructure, assurance in unusual modes of operation supporting operating policy.
4. For communication and negotiation of service level agreements (SLA), insurance and certification.
5. During checking of security and regulatory compliance following:
    - changes to the scenario,
    - changes to the system due to planned maintenance,
    - unauthorised changes.

It is worth mentioning that detailed analysis methods can be applied within the framework for specific applications. Thus, the framework has the potential to be applied to different fields preserving the overall logic and approach.

REFERENCES

1. website: http://ec.europa.eu/programmes/horizon2020/
2. Europe's Vision for Aviation Flightpath 2050, website: http://ec.europa.eu/research/transport/publications/items/vision2050_en.htm
3. Integrated Ground and on-Board system for Support of the Aircraft SafeTake-off and Landing ", Grant agreement no: 284884, THEME [AAT.2011.6.3-2.], FP7 [01-09-2011]
4. Ideas about the future of air transport website: http://ec.europa.eu/research/transport/pdf/oob_bookmarked_en.pdf
5. The Psychology of Security https://www.schneier.com/essay-155.html
6. Stanovich, K. E., & West, R. F. (1999). Discrepancies between normative and descriptive models of decision making and the understanding/acceptance principle. Cognitive Psychology, 38, 349-385
7. General problems of the air transportation system that need to be solved D2.1
8. Evaluation of environmental, safety and security aspects of the new technologies D2.3
9. *Possible new solutions to take-off and landing an aircraft.* D2.4
10. *Preliminary definition of the GABRIEL concept D2.8*
11. *Preliminary specification of the ground based and on-board sub-systems of the GABRIEL system D3.1*
12. Conceptual design of the ground-based systems related to the GABRIEL concept.D3.5
13. SAE. *ARP4754 System development process.*
14. *ARP4761 System safety assessment process.*
15. RTCA. *DO-178B Software Considerations in Airborne Systems and Equipment Certification.*
16. *DO-254 Hardware Considerations in Airborne Systems and Equipment Certification.*
17. International Civil Aviation Organization. *Doc 8168 Aircraft Operations.*

18. Prospect Theory: An Analysis of Decision under Risk, Daniel Kahneman, Amos Tversky, Econometrica, Vol. 47, No. 2. (Mar., 1979), pp. 263-292. Stable URL:http://links.jstor.org/sici?sici=00129682%28197903%2947%3A2%3C263%3APTAAOD%3E2.0.CO%3B2-3

19. ECSS. *ECSS-P-001B - Glossary of Terms.*

20. International Civil Aviation Organization. *Engine Exhaust Emissions Databank.*

21. U.S. Dept. of Defense. *MIL-STD-882 Standard practice for system safety.*

22. International Civil Aviation Organization. *PANS-Ops Doc 4444 Rules of the Air and ATM.*

23. EASA. Annual Safety Review. 2012. European Reference Network for Critical Infrastructure Protection Europe 2020

24. Report of the workshops on the Common Strategic Framework (CSF)for Research and Innovation: Inclusive, Innovative and Secure Societies Challenge

25. Sidney W. A. Dekker ,"Just culture: who gets to draw the line? "14 January 2008, Springer-Verlag London Limited.

26. EU Data Protection Directives http://ec.europa.eu/justice/data-protection.

27. European Group on Ethics in Science and New Technologies BEPA Bureau of European Policy Advisers.

28. Systems Engineering and Analysis, B.S. Blanchard and W. J. Fabrycky, 5th edition, Prentice-Hall, 2010.

29. Systems Engineering Handbook, A guide for System Life Cycle Processes and Activities, International Council on Systems Engineering (INCOSE), 2011.

30. NASA Systems Engineering Handbook.

31. Systems Engineering Handbook, version 2a. INCOSE. 2004.

32. "Derek Hitchins". INCOSE UK. Retrieved 2007-06-02.

33. Bonsor, Kevin. "HowStuffWorks "How Maglev Trains Work"" Howstuffworks "Science"Web.12 Mar.2011. <http://science.howstuffworks.com/transport/enginesequipment/

maglev-train.htm>.

34. " Coates, Kevin C. "Maglev To Dulles." Washington Post 2 May 2004: B08. Print.

35. Lee, Hyung-Woo, Ki-Chan Kim, and Ju Lee. "Review of Maglev Train Technologies."IEEE Transactions on Magnetics 42.7 (2006): 1917-925. Web. 3 Mar. 2011.

36. Ono, Motoharu, Shunsaku Koga, and Hisao Ohtsuki. "Japan's Superconducting Maglev Train." IEEE Instrumentation & Measurement Magazine. Mar. 2002. Web. Mar. 2011.

APPENDIX A - TERMS AND DEFINITIONS

Accident
An undesired event that results in harm to people damage to property or loss of property.

Incident
An undesired event which under slightly different circumstances, could have resulted in harm to people. damage to property, or loss of process.

Cause
that which produces an effect; that which gives rise to any action, phenomenonor condition
NOTE 1 Cause and effect are correlative terms (Oxford English Dictionary)
NOTE 2 Specific to this Standard, cause, when used in the context of hazard analysis, is the action or condition by which a hazardous event is initiated (an initiating event). The cause can arise as the result of failure, human error, designing adequacy, induced or natural environment, system con-

Critical fault
fault which is assessed as likely to result in injury to persons, significant material damage, or other unacceptable consequences[IEC 50:1992]

Fail safe
design property of an item which prevents its failures from resulting in critical faults[IEC 50:1992]

Failure
termination of the ability of an item to perform a required function[IEC 50:1992]

Failure rate
The number of failures of an item per unit measurement of life. Failure rate is considered constant over the useful life period

Fault
Noun <event> unplanned occurrence or defect in an item which may result in one or more failures of the item itself or of other associated equipment[IEC 50:1992]
NOTE An item may contain a sub--element fault, which is a defect that can manifest itself only under certain circumstances. When those circumstances occur, the defect in the sub-element will cause the item to fail, resulting in an error. This error can propagate to other items causing them, in turn, to fail. After the failure occurs, the item as a whole is said to have a fault or to be in a faulty state [definition 3.1.11above]. [ECSS--P—001B]

Hazard
existing or potential condition of an item that can result in a mishap
NOTE This condition can be associated with the design, fabrication, operation or environment of the item, and has the potential for mishaps.[ISO 14620--2:2000]
NOTE .Items. include human beings.

Hazardous event
occurrence leading to undesired consequences and arising from the triggering by one (or more) initiator events of one (or more) hazards
NOTE Adapted from ECSS--P—001B

ILS
An instrument landing system (ILS) is a radio beam transmitter that provides a direction for approaching aircraft that tune their receiver to the ILS frequency. It provides both lateral and a vertical signals. It is a ground-based instrument approach system that provides precision guidance to an aircraft approaching and landing on a runway.

Incident
unplanned event that could have been an accident but was not[ECSS--P—001B]

Maintainability
characteristic of design and installation which determines the probability that a failed equipment, machine, or system can be restored to its normal operable state within a

given timeframe, using the prescribed practices and procedures. Its two main components are serviceability (ease of conducting scheduled inspections and servicing) and reparability (ease of restoring service after a failure).

Operator error
failure of an operator to perform an action as required or trained or the inadvertent or incorrect action of an operator[ISO 14620--1]

Risk
quantitative measure of the magnitude of a potential loss and the probability of incurring that loss
[ECSS--P—001B]

Safe state
state that does not lead to critical or catastrophic consequences[ISO 14620--1]

Safety
system state where an acceptable level of risk with respect to:

- fatality,
- injury or occupational illness,
- damage to launcher hardware or launch site facilities,
- damage to an element of an interfacing manned flight system,
- the main functions of a flight system itself,
- pollution of the environment, atmosphere or outer space, and
- damage to public or private property is not exceeded

NOTE 1 The term .safety. is defined differently in ISO/IEC Guide 2as freedom from unacceptable risk of harm.

Safety-critical function
function that, if lost or degraded, or as a result of incorrect or inadvertent operation, can result in catastrophic or critical consequences
NOTE Adapted from ECSS--P—001B.

Security
security is the degree of resistance to, or protection from, harm. It applies to any vulnerable and valuable asset, such as a person, dwelling, community, nation, or organization.

System
set of interdependent elements constituted to achieve a given objective by performing a specified function
NOTE The system is considered to be separated from the environment and other external systems by an imaginary surface which cuts the links between them and the considered system. Through these links, the system is affected by the environment, is acted upon by the external systems, or acts itself on the environment or the external systems.
[IEC 50:1992]

System safety
application of engineering and management principles, criteria, and techniques to optimize all aspects of safety within the constraints of operational effectiveness, time, and cost throughout all phases of the system life cycle
[ISO 14620--1]

Hazard
existing or potential condition of an item that can result in a mishap[ISO 14620--2]
NOTE 1 This condition can be associated with the design, fabrication, operation, or environment of the item, and has the potential for mishaps.[ISO 14620--2]
NOTE 2 Hazards are potential threats to the safety of a system. They are not events, but the prerequisite for the occurrence of hazard scenarios with their negative effects on safety in terms of the safety consequences.

Hazard analysis
systematic and iterative process of the identification, classification and reduction of hazards

Hazard manifestation
presence of specific hazards in the technical design, operation and environment of a system

Hazard scenario
sequence of events leading from the initial cause to the unwanted safety consequence
NOTE The cause can be a single initiating event, or an additional action or a change of condition activating a dormant problem.

Reliability
probability that an item will perform a required function without failure under stated conditions for a stated period of time.

Severity of safety consequence
measure of the gravity of damage with respect to safety

Severity definitions - Safety Related

Severity	Definition
Catastrophic	Results in multiple fatalities and/or loss of the system
Hazardous	Reduces the capability of the system or the operator ability to cope with adverse conditions to the extent that there would be: ○ Large reduction in safety margin or functional capability ○ Crew physical distress/excessive workload such that operators cannot be relied upon to perform required tasks accurately or completely ○ Serious or fatal injury to small number of occupants of aircraft (except operators) ○ Fatal injury to ground personnel and/or general public
Major	Reduces the capability of the system or the operators to cope with adverse operating conditions to the extent that there would be: ○ Significant reduction in safety margin or functional capability ○ Significant increase in operator workload ○ Conditions impairing operator efficiency or creating significant discomfort ○ Physical distress to occupants of aircraft (except operator) including injuries ○ Major occupational illness and/or major environmental damage, and/or major property damage
Minor	Does not significantly reduce system safety. Actions required by operators are well within their capabilities. Include: ○ Slight reduction in safety margin or functional capabilities ○ Slight increase in workload such as routine flight plan changes ○ Some physical discomfort to occupants or aircraft (except operators) ○ Minor occupational illness and/or minor environmental damage, and/or minor property damage
No Safety Effect	Has no effect on safety

Likelihood of occurrence

Likelihood	Definition
Probable	Qualitative: Anticipated to occur one or more times during the entire

	system/operational life of an item. Quantitative: Probability of occurrence per operational hour is greater than 1×10^{-5}
Remote	Qualitative: Unlikely to occur to each item during its total life. May occur several times in the life of an entire system or fleet. Quantitative: Probability of occurrence per operational hour is less than 1×10^{-5}, but greater than 1×10^{-7}
Extremely Remote	Qualitative: Not anticipated to occur to each item during its total life. May occur a few times in the life of an entire system or fleet. Quantitative: Probability of occurrence per operational hour is less than 1×10^{-7} but greater than 1×10^{-9}
Extremely Improbable	Qualitative: So unlikely that it is not anticipated to occur during the entire operational life of an entire system or fleet. Quantitative: Probability of occurrence per operational hour is less than 1×10^{-9}