POLITECNICO DI MILANO

Facoltà di Ingegneria Industriale

Corso di Laurea in Ingegneria Aeronautica

Risk Analysis in Take-Off Procedure with Electronic Flight Bag

Relatore: Prof. P. Carlo Cacciabue
Correlatore: Valentina Licata

Tesi di Laurea di:
Claudia MARIANI Matr. 733422

Anno Accademico 2011/2012

Acknowledgments

To professor P. Carlo Cacciabue who gave me the possibility to develop this thesis on this interesting argument.

To Valentina Licata and Mirella Cassani for their advices and for their helpfulness.

To Italo Oddone and Alberto Ottomaniello for the information and their availability.

To my parents who gave me the opportunity to attend the university and because they have always believed in me.

To Daniele for everything, you were always there for me.

To Lara.

Contents

List of Figures

List of Tables

Abstract

This work is focused on the Management of Change evaluating the risk related to the introduction of a new instrument in a company in order to implement the Safety Management System (SMS): the instrument considered for this thesis is the Electronic Flight Bag (EFB) for the take-off briefing. The risk assessment is performed considering the influence of Human Factors in the case in exam.
The case study is analysed considering the Risk Assessment Methodology for Company Operational Processes (RAMCOP) methodology for the prospective calculation of the probabilities. This analysis consists in identifying the activities required for the take-off briefing; then the hazards, the possible consequences and the existing control measures (barriers) are determined in order to find the incident sequences and to calculate the relative risk level. The risk level is evaluated using a risk matrix modified with respect to ICAO risk matrix and its inputs are the likelihood and the severity of the incident sequence considered. When the risk level is in an unacceptable area of the risk matrix, further mitigations are introduced.
The calculation of the probability is performed using two methods, Tecnica Empirica Stima Errori Operatori (TESEO) and Technique for Human Error Rate Prediction (THERP): the first one is applied as described in literature while the second one is applied using an innovative formulation. When these methods were not applicable the Expert Judgement (EJ) method was used for probability estimation.
At the end, the risk levels calculated with the modified risk matrix are compared with the risk levels evaluated considering the ICAO risk matrix. The results show that when utilising the above mentioned methods, with carefully selected, justified and conservative probabilities of human error, the use of the risk matrix, adapted to the company data and refined with a more accurate intervals of likelihood values, and the existing barriers enable to handle all possible hazards arising from the introduction of the EFB system. On the other hand when the generic risk matrix proposed by International Civil Aviation Organization (ICAO) is utilised, it turns out that further barriers have to be introduced in order to comply with the

safety requirements. This shows that the generic matrix proposed by ICAO should be carefully utilised by organisations, as the necessary generality shown by the ICAO matrix leads always to extremely highly demanding safety measures, sometimes unmanageable in terms of cost versus benefit.

Keywords: Electronic Flight Bag, THERP, TESEO, Risk Analysis, Safety Management System, Human Factors.

Sommario

Questo lavoro è focalizzato sul Management of Change valutando il rischio relativo all'introduzione di un nuovo strumento in una compagnia al fine di implementare il SMS (Safety Management System): lo strumento considerato per questa tesi è l'EFB (Electronic Flight Bag) per il briefing pre-decollo. La valutazione del rischio è effettuata considerando l'influenza dei fattori umani nel caso in esame.
Il caso studio è analizzato considerando la metodologia RAMCOP (Risk Assessment Methodology for Company Operational Processes) per il calcolo prospettico delle probabilità. Questa analisi consiste nell'identificare le attività richieste per il briefing pre-decollo; successivamente i pericoli (hazards), le possibili conseguenze e le misure di controllo (barriere) sono determinate al fine di trovare le sequenze incidentali e calcolarne il relativo livello di rischio. Il livello di rischio è valutato usando una matrice di rischio modificata rispetto alla matrice di rischio dell'ICAO e i suoi ingressi sono la probabilità e la severità della sequenza incidentale considerata. Quando il livello di rischio si trova in un'area non accettabile della matrice di rischio, ulteriori mitigazioni vengono introdotte.
Il calcolo dalla probabilità è effettuato usando due metodi, TESEO (Tecnica Empirica Stima Errori Operatori) e THERP (Technique for Human Error Rate Prediction): il primo viene applicato come riportato in letteratura mentre il secondo è applicato usando una formulazione innovativa. Quando questi metodi non sono applicabili l'Expert Judgement (EJ, Giudizio di Esperti) viene usato per stimare la probabilità.
Alla fine, i livelli di rischio calcolati con la matrice di rischio modificata sono confrontati con i livelli di rischio valutati considerando la matrice di rischio dell'ICAO.
I risultati mostrano che quando vengono utilizzati i metodi sopra citati, assieme alle probabilità di errori umani selezionate attentamente, giustificate e conservative, l'uso della matrice di rischio, adattata ai dati della compagnia aerea e ridefinita con intervalli di probabilità più accurati, e delle barriere esistenti permettono di gestire tutti i possibili pericoli (hazards) che derivano dall'introduzione dello strumento EFB. D'altro canto,

quando la generica matrice di rischio proposta dall'ICAO (International Civil Aviation Organization) viene utilizzata, risulta necessario introdurre ulteriori barriere al fine di rispettare i requisiti di sicurezza. Questo mostra che la matrice di rischio proposta dall'ICAO dovrebbe essere utilizzata con attenzione dalle organizzazioni siccome la necessaria generalizzazione mostrata dalla matrice ICAO conduce sempre ad una richiesta di misure di sicurezza estremamente elevate, a volte ingestibile in termini di rapporto costo/beneficio.

Parole chiave: Electronic Flight Bag, THERP, TESEO, Analisi del Rischio, Safety Management System, Fattori Umani.

Chapter 1

Introduction

This work was developed during an internship at Kite Solutions S.r.l. in collaboration with the airline Air Dolomiti. Kite Solutions is an enterprise specialized in study, development and implementation of safety and risk assessment in highly automated systems as the aviation domain: particular attention is given to Human Factor. Moreover, while working for Kite Solutions, it was possible to use their expertises and their dedicated software, as SDS Plus, for the risk assessment performed for this thesis. Air Dolomiti instead is the airline that provided the data and the information to be used as starting point for the analyses executed during the internship.

1.1 Thesis motivation and objectives

When there is a change in any type of organization or airline it has to be analysed because a lot of factors can have effects on the operators and people in the organization and influence the safety of the organization operations. These analyses, called Management of Change, are performed in aviation industries through the implementation of Safety Management System because safety is one of the most important aspects and it must be continuously developed and applied to it for all procedures in the system. Indeed, the reduction of accidents and incidents is the most important point and the employees must be familiar with the concept of safety.
To analyse safety, the definition of risk assessment is necessary because it can help to maintain an high level of workability and it increases the mission efficacy. The classification of risk is usually divided in the classification of severity and likelihood that lead to the concept of risk matrix where the risk is defined by the intersection between severity and likelihood.

This analysis is focused on human factors and a description of the methods developed in the past and still in use is presented in this thesis.

This project is focused on the analysis of changes that the use of Electronic Flight Bag produces in particular during the take-off briefing for the aircraft, Embraer 195, in normal, in stress and increased workload situations. The take-off briefing is the most important phase during the preparation of flight and flight itself because it represents a critical point in all flights and pilots decide the aircraft parameters for the manoeuvre that they should follow during take-off.

In this work the methodology applied for the risk assessment is the RAMCOP which is used for the implementation of prospective and retrospective analyses. In this thesis the methodology focuses on the Human Reliability Analysis (HRA) evaluated through the application of the two methods, Tecnica Empirica Stima Errori Operatori (TESEO) and Technique for Human Error Rate Prediction (THERP); the second one represents an innovative approach to the problem because it is not applied as presented in literature but it was modified in order to consider the choices pilots are required to take during the take-off briefing.

The objectives of this work is to use the methods TESEO and THERP to analyse hazards and consequences and to find the sequence with the higher probability to happen. Then these sequences are presented in a table along with the possible barriers that are applied in order to reduce the value of probability and to take the risk in an acceptable zone in the risk matrix.
At the end, a comparison between the risk matrix developed by ICAO and the risk matrix developed in this thesis is presented.

1.2 Content

This work is divided into six chapters:

- Chapter 1.
  It includes a presentation of the work with the motivations and the objectives of this thesis.

- Chapter 2.
  It includes a description of Safety Management System and risk assessment with the distinction between severity and likelihood and

the definition of risk matrix. There is also a description of the methods used in Human Reliability Analysis (HRA). There are the definitions of retrospective and prospective analyses because they are important for the analysis and their role in the risk assessment.

- Chapter 3.
  The Management of Change is defined and the Risk Assessment Methodology for Company Operational Processes (RAMCOP) methodology used for the implementation of the risk assessment is described.

- Chapter 4.
  There is the description of the take-off briefing and the relative procedures; the Electronic Flight Bag (EFB) is also described in order to introduce its interaction with the case study.

- Chapter 5.
  The analyses are presented for both methods considered. Besides, there is a comparison between the risk matrix used for this work and the risk matrix developed by ICAO. This chapter contains the most relevant and innovative aspects of the work of this thesis.

- Chapter 6.
  The conclusion is presented along with the possible future developments.

In Appendix there is a detailed description of the two methods used for this thesis, TESEO and THERP.

Chapter 2

Risk Analysis: concepts and standard methods

In this chapter an introduction to the Safety Management System and to the risk assessment is presented: both are used for safety valuation. Moreover, the methods and methodologies used in Human Reliability Analysis (HRA) are described. At the end, a description of prospective and retrospective analysis is presented.

2.1 Safety Management System

To introduce the concept of SMS, it is important to discuss about safety in aviation. In these years, the aviation domain has tried to further reduce the accident and the incident rate. In particular the Safety Management System has been developed to help to spread and to familiarise the aviation employees to the concepts of safety.
The concept of safety can be associated to the risk represented by an element to the mission effectiveness and to maintain an high level of workability.
The definition of safety (ICAO - DOC 9859 [1]) adopted in this thesis is the following:

The state in which the risk of harm to persons or environment damage is reduced to, and maintained at or below, an acceptable level through a continuing process of hazard identification and risk management.

Moreover the aviation industries invest a lot of resources trying to reduce the accident and the incident rate because these have a big impact

on the public opinion. The management of safety is a prerequisite for a sustainable aviation business. For these reasons, the aviation international and national authorities, in the last years, have been aiming to change the attitude towards safety introducing SMS to all levels of relevant organizations (airlines, airports, maintenance services, Air Traffic Management, etc.); for example, Ente Nazionale per l'Aviazione Civile (ENAC) with the Informative Note [2] imposes to improve a Safety Management System for Italian companies. Therefore, all employees and operators need to know SMS concepts and purpose, as these involve operations as well as technical and financial activities.
SMS is divided into four major components:

- safety politic and institutional purposes;
- risk analysis and management;
- hazards evaluation;
- safety promotion in the organization.

The second and the third components are the technical application of SMS, while the first and the last are the absolutely necessary dissemination elements to sustain and promote the Safety Management System.
In this thesis the attention is focused on risk analysis and hazard evaluation because these two elements are the essential contributors to the evaluation of probabilities and severity of consequences that eventually define the risk matrix and the acceptability or not of certain hazards.

2.2 Risk assessment

The risk assessment is of fundamental importance for the safety analysis because it allows to increase the mission efficacy and to maintain an high level of workability.
The definition of risk [3] adopted in this thesis is the following:

Risk is the measure of how frequently (ϕ) an hazardous event is likely to occur times the level of severity of that event (C):

$$R = C * \phi \tag{2.1}$$

In order to understand the risk definition, the hazard [3] must be defined as well:

Condition, event, or circumstance that could lead to or contribute to unplanned or undesirable consequences.

Following the ICAO manual [4], the hazard *severity* can be divided into five categories:

- negligible;
- minor;
- major;
- hazardous;
- catastrophic.

Similarly ,the *probability* of occurrence is divided into five levels:

- frequent;
- reasonably probable;
- remote;
- extremely remote;
- extremely improbable.

A detailed description of the five hazard severity categories is presented in table 2.1, while a detailed description of probability classification is presented in table 2.2.

Table 2.1: Severity classification scheme [4].

Severity classification	**Results in one or more of the following effects**
Catastrophic	Loss of one or more aircraft and many fatalities.
Hazardous	Reduction of operational capability of the system or the operators that generate: • important reduction of safety; • increase of the workload and the stress which reduce crew performance; • important passengers indisposition and little fatalities; • fatalities between ground personal.
Major	Reduction of operational capability of the system or the operators that generate: • significant reduction of safety; • increase of the workload; • relevant physical indisposition and/or prevented operative efficiency; • passengers indisposition including injuries, material and environmental damages.
Minor	Minimal reduction of global safety. The required actions are performed by the operators. This severity includes: • little reduction of safety; • little increase of the workload; • minor physical indisposition and/or prevented operative efficiency; • reduced material and environmental damages.
Negligible	No effect on safety of system, operators and passengers.

Table 2.2: Probability classification scheme [4].

Probability of Occurrence Definitions	Qualitative definition	Quantitative definition
Extremely improbable	Should virtually never occur in the whole fleet life.	$< 10^{-9}$ per flight hour.
Extremely remote	Unlikely to occur when considering several systems of the same type, but nevertheless has to be considered as being possible.	10^{-7} to 10^{-9} per flight hour.
Remote	Unlikely to occur during total operational life of each system but may occur several times when considering several systems of the same types.	10^{-5} to 10^{-7} per flight hour.
Reasonably probable	May occur once during total operational life of one system.	10^{-3} to 10^{-5} per flight hour.
Frequent	May occur once or several times during operational life.	1 to 10^{-3} per flight hour.

Through table 2.1 and 2.2, it is possible to define the risk matrix (figure 2.1) where three levels of acceptability options can be envisaged, using the five level of severity and probability:

1. unacceptable;
2. review;
3. acceptable.

In figure 2.1 the unacceptable level is presented as a red box and a recovery action must be applied; in the review level (yellow boxes) a recovery action can be necessary; in the acceptable level, presented as a green box, no further actions are required.
There are many techniques and instruments for risk management and assessment which are used in the aviation field. The most important of the currently utilised methods are described in the §2.3.
When this work was developed, the ICAO risk matrix in DOC 9859 version 2009 was considered; in the last months a new version of this ICAO

document [5] was issued and it includes a new risk matrix where the catastrophic/extremely improbable cell is green. It is important to underline that considering the old version of the risk matrix does not introduce errors in the calculation and in the scientific discussions of this thesis (see figure 2.1); indeed the older risk matrix is more conservative with respect to the new one therefore the calculations are toward the acceptable zone of the risk matrix.

Severity / Likelihood	Negligible 1	Minor 2	Major 3	Hazardous 4	Catastrophic 5
Frequent $\varphi \geq 10^{-3}$ x fl. hour					
Reasonably probable $10^{-5} \leq \varphi \leq 10^{-3}$ x fl. hour					
Remote $10^{-7} \leq \varphi \leq 10^{-5}$ x fl. hour					
Extremely remote $10^{-9} \leq \varphi \leq 10^{-7}$ x fl. hour					
Extremely improbable $\varphi \leq 10^{-9}$ x fl. hour					

Figure 2.1: Safety risk assessment matrix [4] [1].

The risk matrix is used to evaluate the safety efficacy and barrier, both in prospective and retrospective analyses. The risk matrix is a fundamental element in risk analysis because it defines what is acceptable and what is not. To calculate the elements that allow risk assessment, it is necessary to know which causes come from an hazard and its probability. For this reason retrospective analyses are used and they help to calculate the potential future risks thanks to organization history. Both types of analyses are used for risk assessment but in this thesis only prospective analyses will be considered. These two types of analyses are explained in details in §2.4.
Moreover all methods (described in §2.3) can be used in risk analysis because they can be associated to human factors components and they describe the human-machine interaction since human actions are a focal point in risk analysis. Indeed, human factors represent a significant contributor to danger.
Before describing all methods used for risk analysis associated to human

factors, it is necessary to introduce two methodologies that can be used for a first qualitative analysis: Airline Risk Management Solutions (ARMS) and BOWTIE.

2.2.1 Airline Risk Management Solutions

The Airline Risk Management Solutions (ARMS) [6] is a methodology developed by a group of experts in 2007 for the operational risk assessment for airlines and other aviation organizations. This methodology has been developed also to implement SMS and to increase the cooperation between organizations that use it.
This methodology is divided into two parts: Event Risk Classification (ERC) and Safety Issues Risk Assessment (SIRA). ERC classifies the risk with a retrospective analysis of hazards which analyses past events, while SIRA represents the analysis of data concerning the matters of safety with a prospective analysis. The process ends with the verification that all safety actions are identified and it creates a registry with the risks evaluation: these steps are necessary to developed a consistent SMS.

2.2.2 BOWTIE

The BOWTIE methodology [7] represents a qualitative and quantitative analysis to risk assessment, structured with the combination of causes and consequences of a well defined hazard. In figure 2.2 the central "node" represents the hazard under assessment.
The BOWTIE process is divided into:

- Step 1: identify the bow-tie hazard;
- Step 2: assess the threats;
- Step 3: assess the consequences;
- Step 4: control;
- Step 5: recover;
- Step 6: identify threats to the controls;
- Step 7: identify the controls for the threats to the controls.

The origin of the BOWTIE methodology is not completely known but it can be seen as an evolution of the cause-consequences diagrams result by [8].

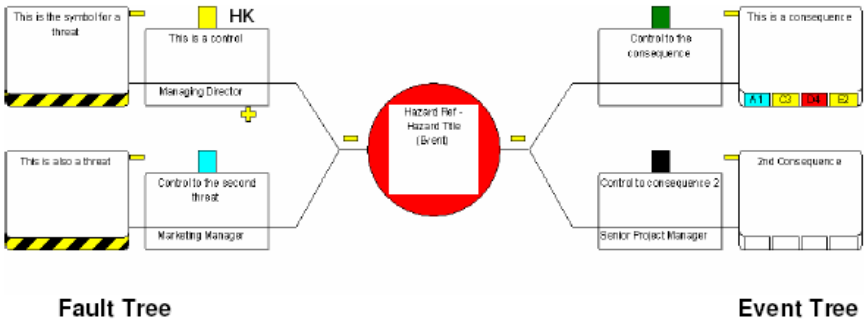


Figure 2.2: BOWTIE methodology [7].

2.3 State of the art in Human Reliability Analysis

A relevant element in risk analysis is the study of human factors which are defined [3] as:

The discipline that deals with human-machine interface and the psychological, social, physical, biological and safety characteristics of a user and the system the user is in.

In literature there are many methods and theories for the implementation of human factors in risk analysis both in prospective and retrospective analyses. In this section a description of the methods most commonly applied in aviation is presented.
Figure 2.3 shows the five different types of Human Reliability Analysis (HRA), each one of them has two options for the method to be used. All methods presented in table 2.3 are defined for HRA and they consider human errors and their contribution to risk.
The methods are divided into two generations: the first one includes methods which quantify errors mainly associated to human behaviour (performance) while the second generation includes methods which aim at assessing more cognitive causes of human erroneous performances.

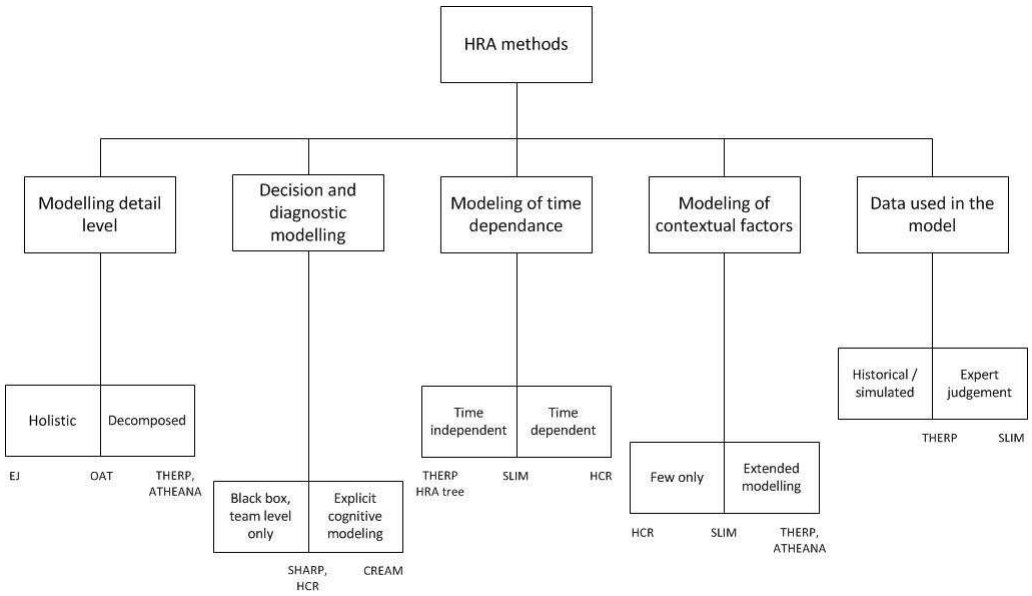


Figure 2.3: Human Reliability Analysis (HRA) readapted from [9].

Table 2.3: Acronym and full title of the tools identified for review readapted from [10].

Tool	In full
APJ	Absolute Probability Judgement
ATHEANA	A Technique for Human Error Analysis
CREAM	Cognitive Reliability and Error Analysis Method
DYLAM-HERA	Dynamic Logical Analytical Method for Human Error Risk Assessment
HCR	Human Cognitive Reliability
OAT	Operator Action Tree
PC	Paired comparisons
SHARP	Systematic Human Action Reliability Procedure
SLIM	Success likelihood index methodology
TESEO	Tecnica Empirica Stima Errori Operatori (Empirical technique to estimate operator errors)
THERP	Technique for Human Error Rate Prediction

2.3.1 The first generation methods

The first generation methods have been developed to help the risk assessor to quantify errors due to human behavioural performances. These methods focus on human action but they consider only superficially the impact of context, errors of commission and organizational factors. Nowadays, they are still used for Quantitative Risk Assessment (QRA).

SHARP

The SHARP methodology, *Systematic Human Action Reliability Procedure* [11], was developed for the nuclear field and it represents the base guide for the human factors in the safety analysis. It is used to analyse systems in which there is a human-machine interaction and it is divided into seven steps:

1. Definition: identification of all human-machine interactions;
2. Screening: identification of the important human actions to be studied in the safety analysis;
3. Break down: each interaction is divided into actions and targets;
4. Representation: representation of the interactions in event or failure trees;
5. Impact assessment: the safety analyst evaluates the impact of the actions identified in the previous step on the event and failure trees;
6. Quantification: the probability of the actions is included in the QRA;
7. Documentation: the analyses results are written in the documentation for future analyses.

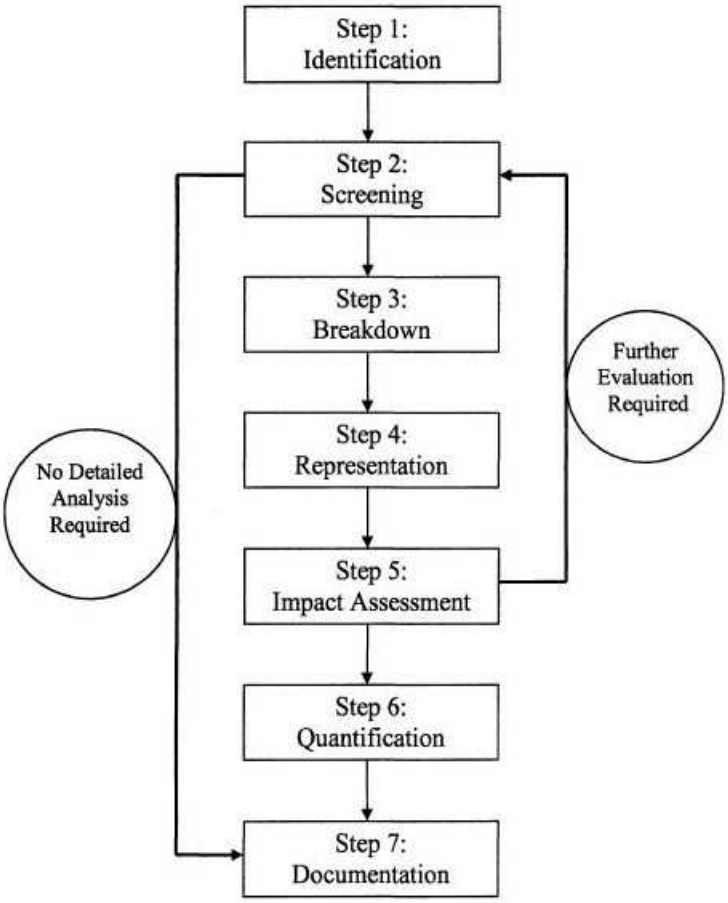


Figure 2.4: Seven steps of SHARP [12].

OAT

The OAT method, *Operator Action Tree*, was developed by Wreathall in 1982 [13] and it is based on the tree graphic representation of the sequence of actions necessary to reach a target. It is focused on the decision-making process due to operator's interpretations.
This method allows to consider alternative procedures and establishes the important decision nodes. As in the SHARP method the concept of "time failure" is used to quantify time-related errors.

APJ

The APJ method, *Absolute Probability Judgement*, was developed by Seaver and Stillwell in 1983 [14] and it is used for human errors quantification or Human Error Probability (HEP).

APJ is based on Expert Judgement in human factors, even if there are only few information on human errors. There are two APJ approaches: "single expert APJ" and "group APJ". The difference between these two approaches consists in the fact that in the first one there is only one expert to estimate the chances of human errors; the second approach is based on a group of people each one of them with its knowledge and opinion and they use these set of skills to estimate HEPs.
Both these approaches are composed of eight steps:

1. selection of the subject-matter experts;
2. identification of mission and the related procedure;
3. preparation of the response booklets;
4. development of the instruction for the experts;
5. judgements of every expert;
6. calculation of the inter-judge consistency;
7. aggregation of the individual estimates;
8. evaluation of the uncertainties.

PC

The PC method, *Paired Comparisons*, was developed by Rock in 1964 [15] for nuclear field applications.In this method, as in APJ, EJ is still considered but they compare pairs of procedures used to evaluate human errors. The expert must identify, for each pair, which procedure has the higher human error probability; after this, a classification of the procedures, based on HEP, is written.
PC follows sixteen steps:

1. definition of the tasks;
2. calibration of the tasks;
3. selection of the experts;
4. preparation of the exercise;
5. briefing of the experts;
6. comparison of the pairs of procedures;

7. derivation of the raw frequency matrix;
8. derivation of the proportion matrix;
9. derivation of transformation X-matrix;
10. derivation of the column-difference Z-matrix;
11. calculation of the values;
12. estimation of the calibration points;
13. transformation of the values into probabilities;
14. determination of the within-judge consistency;
15. determination of the inter-judge consistency;
16. estimation of the uncertainties.

TESEO

The TESEO method, *Tecnica Empirica Stima Errori Operatori*, developed by Bello and Colombari in 1980 [16], predicts the human reliability values using five factors:

- K_1, activity's typological factor;
- K_2, temporary stress factor;
- K_3, operator's typological factor;
- K_4, activity's anxiety factor;
- K_5, activity's ergonomic factor.

This method is described in detail in §A.1.

SLIM

The SLIM method was first developed by Embrey in 1983 [17] and it was reviewed in the following years; this method is divided into two modules: SLIM-MAUD and SLIM-SARAH. This method consists in ten steps and it is based on the Performance Shaping Factors (PSF) to estimate HEP. Experts judgement is used for assessing error probabilities.

HCR

The HCR method, *Human Cognitive Reliability* was developed by Hannaman et al. in 1984 [18] and it is based on the mission failure probability evaluation identifying the cognitive behaviour of people with respect to the mean response time and PSF.
The cognitive behaviour is described in (Rasmussen, 1983 [19]) and is based on the well known model Skill, Rule, Knowledge (SRK) which divides the human behaviour into three levels:

- Skill-based behaviour;
- Rule-based behaviour;
- Knowledge-based behaviour.

The mean response time is defined as the time required for an action; PSF include factors as stress, instrumentation and work environment. This method is a compromise between TESEO, OAT and behaviour psychology analyses.

THERP

The THERP method, *Technique for Human Error Rate Prediction*, was developed by Swain and Guttmannn in 1983 [20] and it is the most commonly applied method.
In this method human errors are described by means of probability trees and the Performance Shaping Factors (PSF). THERP is used for reliability analyses with human factors and it is divided into four phases, for a total of twelve steps:

1. Familiarisation: it includes the "Plant Visit" and the "Review Information from System Analyst" steps;
2. Qualitative Assessment: it includes the "Talk or Walk-through", the "Task Analysis" and the "Develop Human Reliability Analysis - Event Tree" steps;
3. Quantitative Assessment: it includes the "Assign NHEP", the "Estimate the Relative Effects of PSF", the "Assess Dependence", the "Determine Success and Failure Probabilities" and the "Determine the Effects of Recovery Factors" steps;
4. Incorporation: it includes the "Perform a Sensitivity Analysis, if Warranted" and the "Supply Information to System Analysts" steps.

This method is described in detail in §A.2.

2.3.2 The second generation methods

The second generation methods [21] have been developed over the last twenty years and they need to be empirically validated in relation to their specific applications. The difference with the first generation methods is that, in this case, the context and errors made at cognitive level lead to the prediction of the actual manifestations of inadequate performances and errors. It must be underlined that the advantages of these second generation methods are yet to be established, as well as the validity of application.

ATHEANA

The ATHEANA method, *A Technique for Human Event Analysis* [22], was developed by a team of experts in HRA to obtain qualitative and quantitative HRA results. This method considers the error-forcing contexts which influence the likelihood of operator errors and it provides structured search schemes to find the error-forcing contexts by integrating the knowledge and the experience of experts from different field of studies.
An advantage of this method is the possibility to be used both for retrospective and prospective analyses.
There are ten main phases:

1. definition of the issues of concern;
2. definition of the scope of the analysis;
3. description of the base case scenario;
4. identification of Human Failure Events (HFE) and Unsafe Actions (UA);
5. identification of the causes;
6. research of deviations from the base case scenario;
7. identification and evaluation of complicating factors;
8. evaluation of the potential for recovery;
9. interpretation of the results (quantification of HFE);
10. inclusion of the results in QRA.

CREAM

The CREAM method, *Cognitive Reliability and Error Analysis Method*, was developed by Erik Hollnagel in 1993 [23] and it is based on the cognitive model called COntextual COntrol Model (COCOM) which includes the operative and social context effects on the human behaviour. This method allows to distinguish the competences from the cognitive control. There are four different control levels and they represent the operator's behaviour towards the event. The levels are: strategic, tactical, opportunistic and impulsive control.
Base on the COCOM model, the CREAM method can be classified with the separation between causes and manifestations; both are influenced by external factors, as the emotional state, the personality, the human-machine interface, the noise, the temperature, the actions made at the wrong time or in the wrong place or at the wrong object.
The CREAM approach has three different major components:

1. "Function Allocation Method", FAME;
2. "Contextual Control Model", COCOM;
3. CREAM.

DYLAM-HERA

The DYLAM-HERA method, *Dynamic Logical Analytical Method for Human Error Risk Assessment*, was developed originally by Cacciabue in 1997 [24] and then expanded. It is applied to the risk evaluation of human errors.
It is based on four main components:

1. evaluation of the human actions integration and the machine responses;
2. development of an inadequate behaviour classification;
3. generation of a database with human errors and system failure;
4. integration of the cognitive model and the system failure data and human errors.

This method allows to identify the operators and systems wrong and correct behaviour based on the human-machine interaction.

2.4 Retrospective and prospective analyses

Retrospective and prospective analyses are the most important steps in the risk assessment process, as they are connected with quantitative and qualitative evaluation of hazards.
In figure 2.5 the elements that characterise retrospective and prospective analyses [25] are represented: common elements and difference between them are showed. The differences are in the fundamental objectives of the two approaches. In retrospective analyses the analyst must find and analyse the most important information from past events through root cause analysis methods, while in prospective analyses the analyst must evaluate possible consequences from given initiating events and boundary conditions, using experience, knowledge and suitable predictive methods.
The common features between them are the theories and models utilised for human-machine interaction assessment and system configuration.

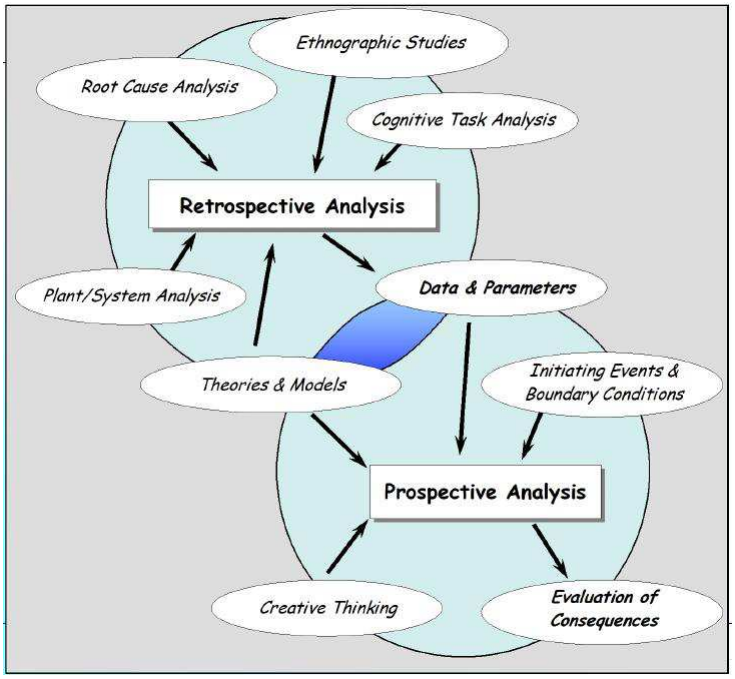


Figure 2.5: Retrospective and prospective analysis [26].

In essence, retrospective analysis [25] can be defined as:

The assessment of events involving human interaction, such as accidents, incidents, or "near-misses", with the objective of detailed search for the fundamental

reason, facts and causes that have promoted and fostered inadequate human behaviour.

Whereas, prospective analysis [25] is defined as:

The assessment and prediction of the consequences of human-machine interaction, given an initiating event and boundary configuration of the system.

These two type of analyses can be applied in the particular context, such as human-machine interaction, and they are strongly interconnected with the qualitative and quantitative evaluation of hazards. The qualitative approach is used to predict human-machine interactions; however, this is not a computational method but it is considered the first step of human-machine interaction analysis. The quantitative simulation, instead, is used to estimate the human behaviour using a computational part. This implies that the interaction of humans with machines and environment (the Human Machine System) is evaluated as a whole.
In essence, as in the case of retrospective and prospective analyses, there are no big differences between qualitative and quantitative simulations because they operate in the same domain and they might be connected to guarantee the desired safety level. Moreover, the two types of analyses are strongly interconnected by the fact that no valid and acceptable quantitative analysis can be performed without an appropriate background of theoretical construct and qualitative assessment of the system under examination.

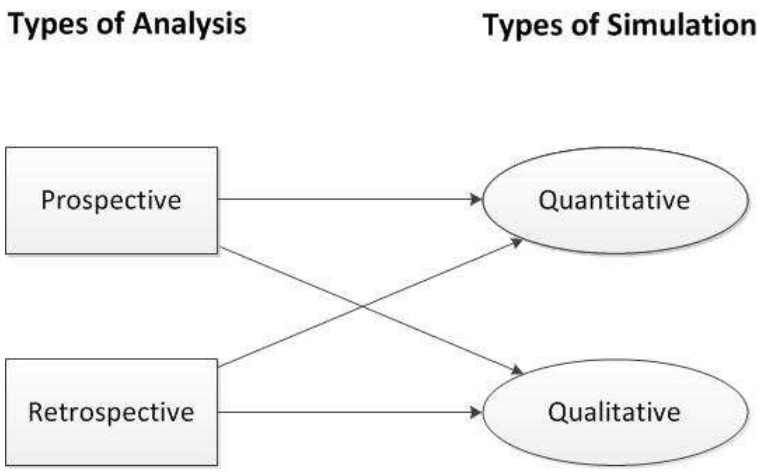


Figure 2.6: Types of simulation and types of analysis readapted from [25].

Chapter 3

Risk Analysis: critical issues and methodology of implementation

In this chapter the definition of Management of Change is provided along with the methodology used in this thesis for its analysis: the methodology described is called Risk Assessment Methodology for Company Operational Processes (RAMCOP).

3.1 Management of Change

The definition of Management of Change is relatively recent but it is not completely clear nor simple as there are many different ideas about its meaning for engineers, business men and psychologists. The Management of Change is an approach that is used to verify the transition between current and future state of a system/organization. Indeed, there can be a change in a company structure and it can be controlled by specialists.
Engineers and psychologists have tried to develop a single thought in order to define a possible definition of Management of Change (MOC) and the result of these studies has led to the following definition [27] of MOC:

Change management is the process, tools and techniques to manage the people-side of business change to achieve the required business outcome, and to realize that business change effectively within the social infrastructure of the workplace.

An example of Management of Change in airline is the introduction of a new instrument on aircraft: the case study considers the use of EFB for the take-off briefing. This case represents an example of Management of Change because the standard procedures are modified.

3.2 Methodology applied for Risk Assessment

The methodology used in this thesis to analyse the Management of Change caused from the introduction of EFB is the Risk Assessment Methodology for Company Operational Processes (RAMCOP). The analysis obtained with this methodology results in the risk assessment of the change. This methodology can be applied by the analyst to many case scenarios since it is not a rigid procedure but it can be adapted to the particular cases. The RAMCOP methodology can be applied both to prospective and retrospective analyses but respectively for the analysis of changes and the analysis of existing procedures. In this thesis, a brief description of this methodology is provided but more details on RAMCOP can be found in Andrea De Col thesis, 2012 [28]. This methodology is composed by three phases and they are described in the following paragraphs.

The first step of the methodology is the identification of the activities (threats) related to the case in exam; for every activity the possible hazards and the consequences are identified. For the identification of activities, hazards and consequences the experts and operators opinion should be taken into account. The activities and the corresponding hazards can be associated also with the left side of the BOWTIE methodology.

The second step of the methodology refers to the identification of the incident sequences of every hazard and the possible barriers for the first mitigation of the risk. Moreover, the probability associated to the hazards and the consequences are estimated along with the value of the barriers. Starting from these data, the likelihood of every incident sequence can be calculated; assigning the severity level to each consequence is possible to evaluate the risk using the selected risk matrix.

The last step starts with the identification of the incident sequence with the higher risk level for every hazard; if more than one sequence has the same risk level, the one with the higher probability or the worst severity is selected. This phase focuses on the additional mitigations for the reduction of the risk.

In figure 3.1 a flow chart of the RAMCOP methodology is presented in order to show the steps of the phases with the relative activities. Figure 3.2 represents the example table for the application of this methodology. The application to the case study of the first two phases is presented in §5.1.5 and §5.2.4, while the last step is applied directly in §5.3.

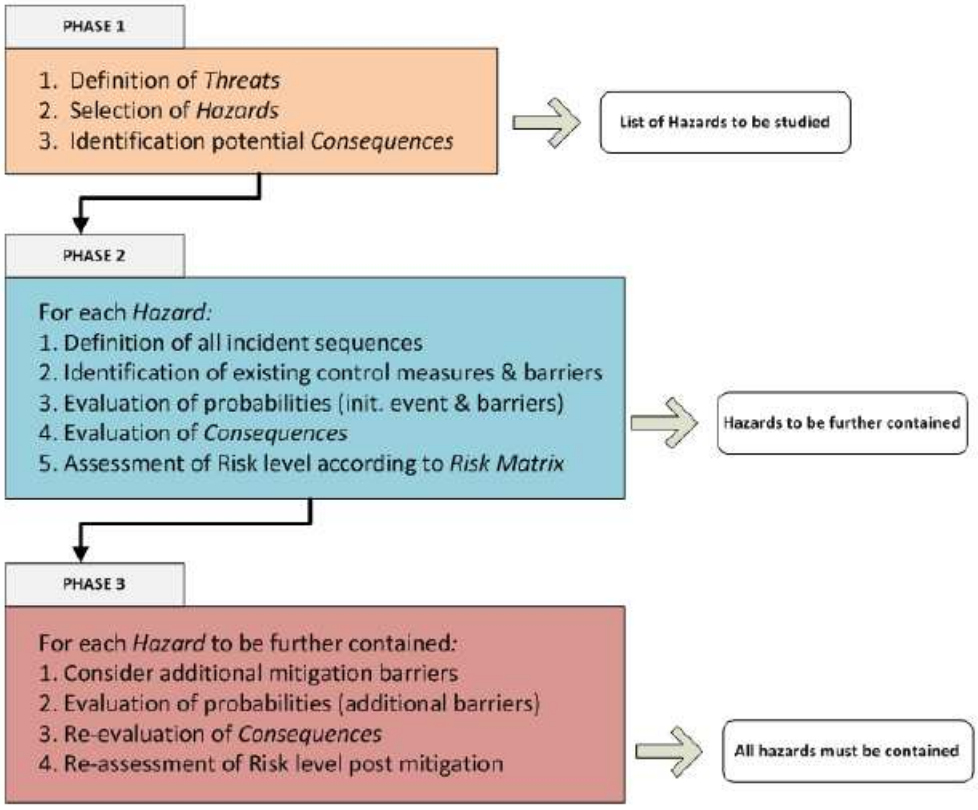
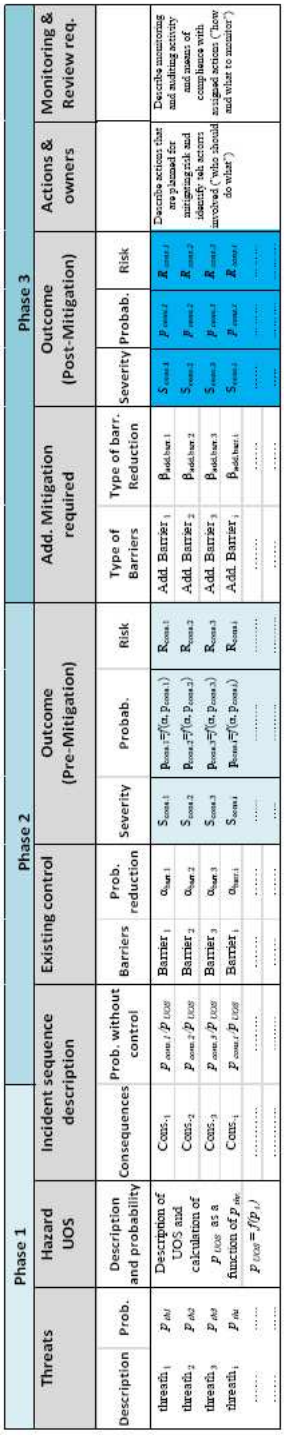


Figure 3.1: RAMCOP flow chart.

It is important to underline that, in this thesis, the RAMCOP methodology is associated to human factors because the purpose of this work is to analyse the reduction of human errors with the introduction of EFB proving that a change in a company can influence human behaviour. For this reason, the methods used for the calculation of the probabilities in phase two are TESEO, THERP and EJ; in particular the THERP method was opportunely modified (see §5.2) in order to develop a innovative approach in probabilities calculation and risk assessment while TESEO and EJ were used as described in literature. The risk level was calculated as a function of likelihood and severity using the modified risk matrix described in §5.1.4.



Phase 1				Phase 2								Phase 3							
Threats		Hazard UOS	Incident sequence description			Existing control			Outcome (Pre-Mitigation)			Add. Mitigation required		Outcome (Post-Mitigation)			Actions & owners	Monitoring & Review req.
Description	Prob.	Description and probability	Consequences	Prob. without control	Barriers	Prob. reduction	Severity	Probab.	Risk	Type of Barriers	Type of barr. Reduction	Severity	Probab.	Risk				
threath.$_1$	P_{Th1}	Description of UOS and calculation of P_{UOS} as a function of $p_{thr.}$	Cons.$_1$	$P_{cons.1} / P_{UOS}$	Barrier$_1$	$\alpha_{barr.1}$	$S_{cons.1}$	$p_{cons.1}=f(\alpha_i p_{cons.1})$	$R_{cons.1}$	Add. Barrier$_1$	$\beta_{add.barr.1}$	$S_{cons.1}$	$P_{cons.1}$	$R_{cons.1}$	Describe actions that are planned for mitigating risk and identify task actors involved ("who should do what")		Describe monitoring and auditing activity and means of compliance with assigned actions ("how and what to monitor")	
threath.$_2$	P_{Th2}		Cons.$_2$	$P_{cons.2} / P_{UOS}$	Barrier$_2$	$\alpha_{barr.2}$	$S_{cons.2}$	$p_{cons.2}=f(\alpha_i p_{cons.2})$	$R_{cons.2}$	Add. Barrier$_2$	$\beta_{add.barr.2}$	$S_{cons.2}$	$P_{cons.2}$	$R_{cons.2}$				
threath.$_3$	P_{Th3}		Cons.$_3$	$P_{cons.3} / P_{UOS}$	Barrier$_3$	$\alpha_{barr.3}$	$S_{cons.3}$	$p_{cons.3}=f(\alpha_i p_{cons.3})$	$R_{cons.3}$	Add. Barrier$_3$	$\beta_{add.barr.3}$	$S_{cons.3}$	$P_{cons.3}$	$R_{cons.3}$				
threath.$_i$	P_{Thi}		Cons.$_i$	$P_{cons.i} / P_{UOS}$	Barrier$_i$	$\alpha_{barr.i}$	$S_{cons.4}$	$p_{cons.4}=f(\alpha_i p_{cons.4})$	$R_{cons.4}$	Add. Barrier$_i$	$\beta_{add.barr.i}$	$S_{cons.4}$	$P_{cons.4}$	$R_{cons.4}$				
.....	.....	$P_{UOS} = f(p_{i,j})$	.....	.....	.....	.....	.....	.....	.....	.....	.....	.....	.....	.....				
.....	.....		.....	.....	.....	.....	.....	.....	.....	.....	.....	.....	.....	.....				

Figure 3.2: RAMCOP example table.

Chapter 4

Case study

In this chapter the case study, the take-off procedure, is analysed in order to develop the risk analysis and find the key aspect and errors in the procedure. The calculation of the hazard probability is performed with two different methods: Tecnica Empirica Stima Errori Operatori (TESEO) and Technique for Human Error Rate Prediction (THERP).
The Electronic Flight Bag (EFB) is also introduced with a short description; it is important to underline that EFB is considered in the case study in order to find the improvement in risk level and in calculated probabilities.

4.1 Take-off procedure

The case study is the take-off procedure for the Air Dolomiti Embraer 195 aircraft. This procedure is composed by the briefing, where the take-off parameters are selected, and the execution of the decisions taken during the briefing, where the parameters are setted in the Flight Management Computer (FMC) which verifies the accuracy of the parameters. After these operations the actual take-off, which was not considered in this thesis, is performed.

4.1.1 Take-off briefing

The briefing is important in the preparation of flight and it must be executed before every flight [29].
During the briefing, Pilot Flying (PF) and Not Pilot Flying (NPF) must cooperate in order to follow every step required in this phase; they must discuss about their disagreements and, at the end, they must reach an understanding on every decision. The cooperation between PF and NPF

should not consider the major experience of the captain. Moreover, the briefing must be short, structured, concise and adapted to the situation that the team is analysing. Pilots need to analyse every occurrence that might happen during the take-off and the emergencies procedures that should be necessary during the relevant contingency manoeuvre.
It is important to underline that the briefing represents a way to visualize actions before they can happen during the take-off manoeuvre and to prepare the pilots to a rapid response.
During the briefing, PF and NPF decide which type of take-off is better: they analyse every parameter necessary to make a correct take-off and, at the end, they study the possible emergency procedures as One Engine Failure (OEF) or other particular situation that can occur [30].
The generic take-off briefing procedure adopted for the analyses in this works is:

Take-off briefing will highlight normal and emergency procedures and any other relevant operational item such as conditional procedure, Minimum Equipment List (MEL), weather, Air Traffic Control (ATC) restrictions, obstacles, etc.
Use the following list as a guide to cover all the major items:

- *type of take-off;*
- *thrust selection;*
- *take-off flaps;*
- *take-off speeds and procedures;*
- *Take-Off Engine Failure Procedure (EFP);*
- *immediate return procedure for non coded emergencies;*
- *diversion to alternate;*
- *overweight landing;*
- *expected departure (Standard Instrument Departure (SID)) and Route;*
- *Minimum Safe Altitude (MSA) and obstacle review.*

In the following the main steps are analysed in order to describe the information needed to perform a correct briefing.
The take-off briefing is made by PF and NPF and they decide and plan the actions for normal and abnormal conditions that can occur during the take-off manoeuvre. In the first step, during the briefing, they need to know

some specific aspects about airport, runway, take-off and SID conditions: all these parameters are given by ATC, Apron Management System and Ground Station. Moreover, they must control QNH (Atmospheric pressure at Nautical Height) and QFE (Atmospheric pressure at Field Pressure), weather, wind and runway conditions and NOtice To AirMen (NOTAM), if available, because these can influence the take-off procedure. For example, NOTAMs inform if the runway, that the aircraft is supposed to use, is in extraordinary repair. PF and NPF must know fuel quantity and weight of the aircraft for the calculation of thrust, flaps configuration and speeds (for example, take-off speed and decision speed), in addition to the previous information.

4.1.2 Take-Off execution

After the take-off briefing, the take-off execution is analysed. In this phase the parameters selected during the briefing are set in FMC and their accuracy is verified. In order to evaluate the errors probability of the actions, in this phase of the procedure, the failure trees of the THERP method is used. In table 4.1, the actions required from PF and NPF and the type of inputs are presented. A correct briefing is necessary in order to perform correctly this phase.

Table 4.1: Take-Off execution

Input	PF Action	NPF Action
Engine value	Read value	Set it on the FMC
Speed values	Read values	Set them on the FMC
Flaps value	Read value	Set it on the FMC

4.2 Electronic Flight Bag

The Electronic Flight Bag (EFB) [31], [32] is:

an electronic display system intended primarily for cockpit/flight-deck or cabin use. EFB devices can display a variety of aviation data or perform basic calculations (for example, performance data, fuel calculations, etc.). The scope of the EFB system functionality may also include various other hosted databases and applications. Physical EFB displays may use various technologies, formats, and forms of

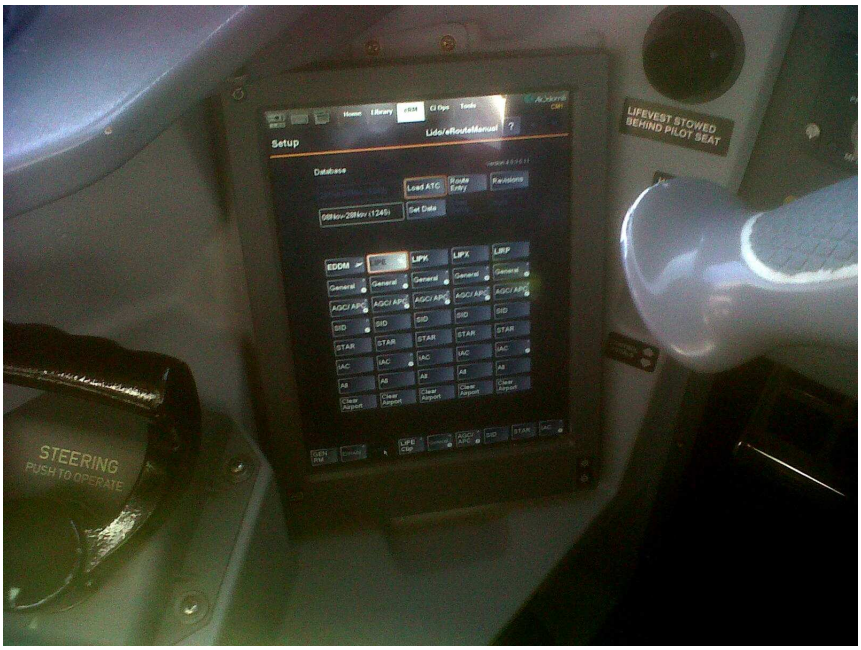
communication. These devices are sometimes referred to as Auxiliary Performance Computers (APC) or Laptop Auxiliary Performance Computers (LAPC).

EFB is an useful instrument in the aircraft for PF and NPF as it can help both during the flight and its preparation, in particular during the take-off briefing and execution.
Before the installation of EFB on an airline fleet, the certification and approval by European Aviation Safety Agency (EASA) or Federal Aviation Administration (FAA) is needed; furthermore, the airline has to decide the type of classification of EFB to be installed on the fleet.
Nowadays, all documentation and information available for the flight are in paper format: they occupy a lot of space on board and they can generate confusion when the pilots need a map or another information during the flight, especially in an emergency situation. With EFB, all documentation and information can be contained in a single laptop and it is not necessary to have all documents and manuals on board.
It is obvious that EFB must be always updated, in particular when there are some changes, for example, in the taxi-way at the airport of destination so NOTAMs must be up to date every time. With this instrument, a lot of information is available in electronic format. An example of EFB representation is shown in figure 4.1.
There are three different classes of EFB systems hardware and their features are compared in table 4.2:

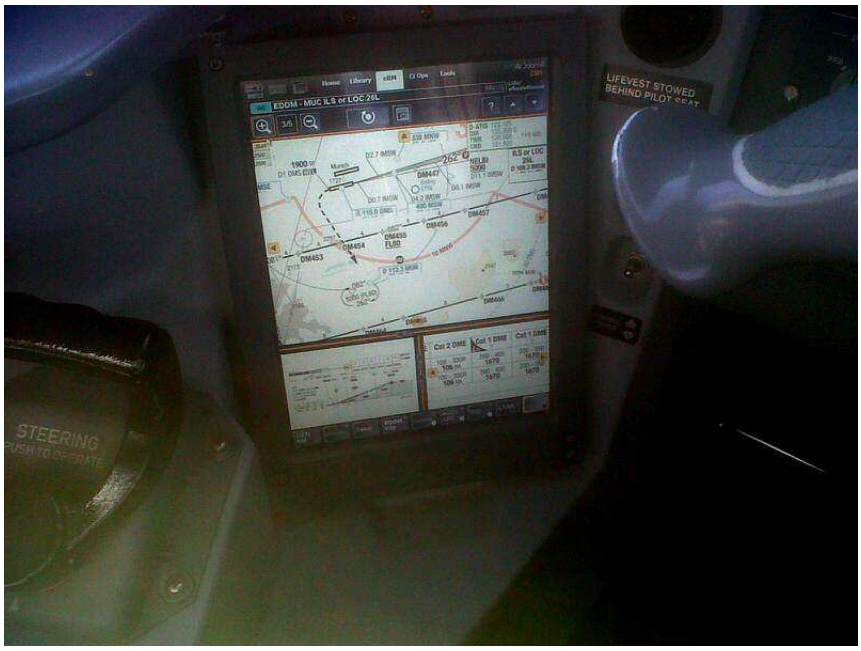
1. class 1;
2. class 2;
3. class 3.

Table 4.2: Electronic Flight Bag: three hardware classes.

Characteristics	Class 1	Class 2	Class 3
COTS-based on computer systems used for aircraft operations	YES	YES	YES
Portable	YES	YES	NO
Connect to aircraft power through a certified power source	YES	YES	YES
Connected to an aircraft mounting device	NO	YES	YES
Connectivity to avionics	Only under specific condition	Possible	YES
Require airworthiness approval	NO	YES	YES
Switch on during all flight phases	Not in taxi, TO and LAND	YES	YES



(a)



(b)

Figure 4.1: Example of EFB representation. Courtesy of Air Dolomiti.

There are also two types of software applications for EFB system as a function of the utilization scope and the approval process required to the client. These two types (A and B) may be hosted on any of the hardware classes and they do not require an airworthiness approval; both types require operational approval but from different authorities: the national authorities for type A and the international authorities for type B.
Type A software includes the documentation currently in paper format and it can display it in a fixed presentation, while type B software includes interactive applications which can modify the data presentation style.
The introduction of EFB in an airline procedure represents a very important change in the management of flights and it should be studied from the viewpoint of safety, as well as return of investment for the entire company.

4.3 Application of EFB to the case study

EFB Class 2 is installed on the Air Dolomiti Embraer 195 aircraft considered for this thesis. Air Dolomiti has the airworthiness approval for this type of class and it is necessary to remember, for this analysis, that EFB is portable and not connected to the avionic system.
The analyses of the take-off procedure presented in §5 consider the possible hazards and their consequences that can emerge during the briefing and its execution with EFB installed in the cockpit.
It is important to underline that the values utilised for this study are not Air Dolomiti real parameters for security reason and for the required level of confidentiality.

Chapter 5

Application of TESEO and THERP method

In this chapter the application of the Tecnica Empirica Stima Errori Operatori (TESEO) and the Technique for Human Error Rate Prediction (THERP) method to the case study analysed is presented.
A presentation of the generic activities, their hazards and the possible consequences is reported along with the values of probability. The resulting risk assessment for each hazard is presented in a table which includes the first and the second phase of the RAMCOP methodology described in §3.2. Moreover, hazards and consequences are analysed in order to identify the sequence with the higher probability. The third phase of the RAMCOP methodology is added in the tables that include the final results (§5.3).
The innovative approach used in this thesis for the development of the THERP tree is also presented.

5.1 Application of TESEO method

The TESEO method is characterized by five coefficients presented in tables 5.1, 5.2, 5.3, 5.4, 5.5. In these tables, there is a definition of the values of the K coefficients for the different factors.

Table 5.1: Activity's typological factor

Type of activity	K_1
Sample, routine	0.001
Requiring attention, routine	0.01
Not routine	0.1

Table 5.2: Temporary stress factor

(a) Routine activities

Time available (s)	K_2 (a)
2	10
10	1
20	0.5

(b) Non-routine activities

Time available (s)	K_2 (b)
3	10
30	1
45	0.3
60	0.1

Table 5.3: Operator's typological factor

Operator's qualities	K_3
Carefully selected, expert, well trained	0.5
Average knowledge and training	1
Little knowledge, poorly trained	3

Table 5.4: Activity's anxiety factor

State of anxiety	K_4
Situation of grave emergency	3
Situation of potential emergency	2
Normal situation	1

Table 5.5: Activity's ergonomic factor

Environmental ergonomic factor	K_5
Excellent microclimate, excellent interface with plant	0.7
Good microclimate, good interface with plant	1
Discrete microclimate, discrete interface with plant	3
Discrete microclimate, poor interface with plant	7
Worse microclimate, poor interface with plant	10

The hazards in which the TESEO method is applied to risk evaluation are:

- hazard No.1: software initialization not completed;
- hazard No.3: improper selection of portrait;
- hazard No.4: improper storage of pc;
- hazard No.5: pilots unable to locate maps;
- hazard No.8: flying with wrong maps or without maps;
- hazard No.12: missing information in the case of emergency.

The calculation of the probability for these hazards is presented in §5.1.5. For every hazard the particular context was considered during the selection of the K coefficients. Assuming that the operator, which has to react to the hazards, is always the same and the level of training in each condition is similar, the K_3 value considered in each hazard was the same. For the environmental ergonomic factor (K_5) a discrete microclimate and a discrete interface with the plant was considered in every hazard except for hazard No.12, where a poor human-machine interface was taken into account.

5.1.1 Generic hazards

The activities, the hazards and the possible consequences are presented in table 5.6. A distinction was made between the cockpit preparation activities and the final crew preparation in the cockpit.
The identification of the activities takes into account the use of EFB and the procedures to be followed for the preparation of the take-off phase. Considering EFB, the possible hazards and consequences were identified. The hazards are evaluated along with the possible consequences in order

to highlight the sequence with the highest probability. This sequence was evaluated considering the severity and the risk matrix.

Activity 1
Excessive workload of CM 2 due to number of task to carry out during cockpit preparation.

This activity concerns the excessive workload of NPF during the flight preparation, in particular during the take-off procedure; in this phase a first external inspection of the aircraft is performed from the captain followed from the cockpit preparation. The excessive workload can contribute to the development of dangerous situation as an incomplete software initialization or the unavailability of the correct maps in EFB. These hazards can potentially lead to consequences as the flight cancellation or delay.

Activity 2
Improper or inadequate loading of software.

The improper or inadequate loading of the software in EFB can lead to hazards as the incorrect selection of the file or the unavailability of the maps. The improper loading of the software can be due to an erroneous switching on from the pilots or the wrong selection of the needed data as the choice of the maps or of the screen for the correct execution of the procedure.
Three possible consequences can generate from these hazards and they are flight cancellation or delay, loss of separation between aircraft or from ground (since the maps are missing PF can not recognize the reference points for the take-off) and Control Flight Into Terrain (CFIT) which can be considered as a consequence of the loss of separation since it represents the aircraft crashing to the ground, against a mountain, in the sea or against any other obstacle.

Activity 3
Lack of adjournment of software.

This activity is similar to the previous one and it concerns the lack of software updating; this can be caused by the omission of the operator in updating the available data. The possible hazards are, as in the previous activity, the improper selection of the file and the unavailability of the maps and the consequences are the flight cancellation or delay, the loss of separation and CFIT.

Activity 4
Lack of familiarity with PC handling, time pressure on CM2.

This activity represents the lack of familiarity of the NPF with the use of a computer or the short time available and the pressure on the NPF. This can lead to an improper EFB storage and, as a consequence, at the unavailability of the maps. The possible consequences of this hazard are the damaging of cables or EFB and smoke or fire in the cockpit; the damaging of cables or EFB causes the cancellation or the delay of the flight.

Activity 5
Pilot workload.

The workload of PF can be excessive and stressful in situations which require high attention (for example during critical situations as take-off, approach and landing) and the utilization of a new instrument installed on the aircraft can increase this workload. As a consequence two very different hazards can be generate: the impossibility to locate the maps in EFB and the loss of Situational Awareness (SA). These hazards are studied separately but they can lead to two possible consequences: the loss of separation and CFIT. As mentioned above, these consequences are connected since CFIT is a possible consequence of the loss of separation.

Activity 6
Out of charge batteries.

The possibility that the batteries run out of charge after a long use is a common characteristic of electronic devices as laptops and tablets. The EFB batteries can be recharged by plugging the instrument into the electrical system of the aircraft. If the batteries are out of charge, EFB cannot be used, for example, to read the maps; this can lead to hazards as no charts on show and loss of SA. The possible consequences are deviation or delay of flight, loss of separation and CFIT.

Activity 7
No updated paper maps or missing paper maps.

For this activity the paper maps are needed but they are not updated or missing on board. The possible hazards are the loss of SA and flying with wrong or without maps and the consequences are deviation or delay of flight, loss of separation and CFIT.

Activity 8
No airfield sketch. Lack of familiarity with airfield, worsened by visibility problems. No ground facilities (radar, light guidance system, etc.).

This activity analyses the lack of familiarity with the airfield, worsened by low visibility and the lack of ground facilities as radar or light guidance system that can reduce the orientation capability of PF on the airfield. In this case PF might not have the coordinates to perform a cross-check with the on board computer, Flight Management System (FMS), and PF can feel lost on the airfield not knowing where the aircraft is. The possible consequences are an incursion on take-off runway, cancellation of flight or ground collision with other aircraft, ground vehicles or airfield infrastructures.

Activity 9
No SID. No or wrong SID, bad weather.

The flight procedures for an aircraft during take-off and climb are included in SID; the use of the SID makes possible the separation of the aircraft with natural obstacles surrounding the airfield. This activity analyses a situation where SID is missing or the pilots use the wrong one along with bad weather that can lead to the following hazards: lack of information on the surrounding obstacles, loss of SA, lack of information on the performances of the aircraft (as the correct value of power and speed for take-off) and the possibility to start the take-off from the wrong runway. The consequences of these hazards can be collision with another aircraft, loss of separation, CFIT and wrong take-off runway.

Activity 10
No approach chart in the case of emergency (bad weather, difficult environment, for examples mountains).

The emergency situations require different procedures that must be analysed considering the working environment, the time available and the workload. This activity analyses the lack of maps in the case of emergency, such as bad weather and difficult environment, which can lead to an increased workload and stress level for the pilots, since the information needed to exit the emergency status is not available; another hazard generated from this activity can be the loss of SA. The possible consequences are loss of control during the flight and CFIT which, in this case, does not depend on the loss of separation.

Table 5.6: Generic hazards.

Activity or issues	Hazard	Potential outcome
Phase Cockpit Preparation: - Cockpit Power up - Walk Around (external inspection) - Cockpit Preparation CM 1 - Cockpit Preparation CM 2		
Excessive workload of CM 2 due to number of task to carry out during cockpit preparation	- Software initialization not completed - Maps not available	- Flight cancellation or delay
Improper/inadequate loading of software	- Improper selection of portrait - Maps not available	- Flight cancellation or delay - Loss of separation - CFIT
Lack of adjournment of software	- Improper selection of portrait - Maps not available	- Flight cancellation or delay - Loss of separation - CFIT
Lack of familiarity with PC handling, time pressure on CM 2	- Improper selection of PC - Maps not available	- Damage to cables or PC - Fire/smoke in the cabin - Flight cancellation or delay
Phase Cockpit Crew: - Final Cockpit Preparation		
Pilot workload	- Pilots unable to locate maps - Loss of SA	- Loss of separation - CFIT
Out of charge batteries	- No charts on show - Loss of SA	- Diversion - Delay - Loss of separation - CFIT
No updated paper maps or missing paper maps	- Flying with wrong maps or without maps - Loss of SA	- Diversion - Delay - Loss of separation - CFIT
No Airfield Sketch. Lack of familiarity with airfield, worsened by visibility problems → No Ground facilities (radar, light guidance system, etc.)	- No coordinates for Xcheck with FMS (impossible to see taxiway) - Getting lost on airfield	- Runway incursion - Flight cancellation - Ground collision (aircraft, infrastructures and vehicles)
No SID (Standard Instrumental Departure) → No/Wrong SID, bad weather	- No info/news on obstacles - Loss of SA - Missing performance - Flying wrong departure	- Mid air collision - Loss of separation (ground and flight) - CFIT - Wrong runway take-off

Table 5.6: Continues on next page

Table 5.6: Continues from previous page

No approach chart in the case of emergency (bad weather, difficult environment, for example mountains)	- Missing information in the case of emergency (increase of WL of crew) - Loss of SA	- Loss of control in flight - CFIT

5.1.2 Hazards and consequences

The hazards related to every activity are presented in table 5.7 along with the possible consequences which are ordered from the most probable. In the last column of the table, the existing controls for every sequence, as described in the following paragraphs, are presented; the controls were evaluated considering the particular hazard and the possible consequence for the calculation of the probability to be used as an input, along with the severity, for the risk matrix.
The calculation of the probabilities presented in the next paragraphs is obtained multiplying the probability of the single hazard by the consequences considered; this result is afterwards multiplied by the values of the barriers considered. It is important to underline that the value of probability of the consequences is called "probability without control" (see for example 5.12) because it represents a weight assigned to the incident sequence considered, for example loss of separation or CFIT.

Table 5.7: Hazards and consequences.

Hazard No.	Description	Incident sequence description	Existing control
1	Software initialisation not completed	- Flight cancellation/delay - Loss of separation - CFIT	Maintenance Quality Control TCAS EGPWS
2	Maps not available	- Flight cancellation/delay - Loss of separation - CFIT	Maintenance Quality Control TCAS EGPWS
3	Improper selection of portrait	- Flight cancellation/delay - Loss of separation - CFIT	Training SOP - EOP TCAS EGPWS

Table 5.7: Continues on next page

Table 5.7: Continues from previous page

4	Improper storage of computer	- Damage to cables/PC - Fire/smoke in the cabin - Flight cancellation/delay	Maintenance Quality Control SOP
5	Pilots unable to locate maps	- Loss of separation - CFIT	Training EOP TCAS EGPWS
6	Loss of SA	- Diversion / Delay - Loss of separation - CFIT	Training SOP - EOP TCAS EGPWS
7	No charts on show	- Diversion / Delay - Loss of separation - CFIT	Maintenance TCAS EGPWS
8	Flying with wrong maps or without maps	- Diversion / Delay - Loss of separation - CFIT	Training SOP - EOP TCAS EGPWS
9	No coordinates for Xcheck with FMS (impossible to see taxiway)	- Runway incursion - Ground collision (aircraft, infrastructures and vehicles) - Wrong runway take-off	ATC communication SOP Training
10	Getting lost on airfield	- Runway incursion - Ground collision (aircraft, infrastructures and vehicles) - Wrong runway take-off	ATC communication EOP Training
11	Missing performance	- Mid air collision - Loss of separation (ground) - CFIT	EOP Training EGPWS
12	Missing information in the case of emergency (increase of WL of crew)	- Loss of control in flight - CFIT	ATC communication EOP Training EGPWS
13	No info/news on obstacles	- Loss of separation (ground) - CFIT	ATC communication EOP EGPWS
14	Flying wrong departure	- Mid air collision - Loss of separation (ground and flight) - CFIT	ATC communication EOP TCAS EGPWS

5.1.3 Barriers values: human and technological factors

The barriers considered to calculate the values of probability are the following:

- TCAS:
  Terrain Control Avoidance System is a system of traffic alert and traffic collision; it warns the pilots about the presence of other aircraft and it suggests the manoeuvre to follow. It represents a good barrier to avoid the loss of separation.

- EGPWS:
  Enhanced Ground Proximity Warning System is an instrument that is useful to determine the position of aircraft and their proximity to terrain thanks to a bright and a sound signal; this is an advanced version of the GPWS. This instrument represents an important barrier to avoid a type of incident called CFIT, Controlled Flight Into Terrain, that is characterized by collision with terrain.

- Training:
  crew training is an important step to guarantee safety. The training teaches to react to the situation respecting the procedure defined and it helps the crew during the flight and its preparation.

- SOP:
  Standard Operating Procedures is a manual with the procedures for standard operations.

- EOP:
  Emergency Operating Procedures is a manual that includes the procedures for emergency situations.

- ATC Communication:
  Air Traffic Control represents a very important barrier because the traffic flow must be ordered and safe on ground and on sky with some instruments as radar and communication system.

- maintenance and processes (MQ):
  this barrier includes maintenance and quality control intended as control of the processes based on quality.

The barriers considered are divided into technological and human barriers with a different value assigned to each category:

- human barriers: 0.4;

- technological barriers: 0.3.

This distinction is possible because there is human influence in every action and the operator acts in order to improve a well-defined situation or because there are a lot of instruments that help the operator to recover a situation that could become critical. In fact, analysing the two values, it is possible to notice that the value of the human barriers is higher than the value of the technological barriers because the human part is the most important while technology always depends on the human answer.
The technological barriers are:

- TCAS;
- EGPWS.

The human barriers are:

- Training;
- SOP;
- EOP;
- ATC Communication;
- maintenance and processes (MQ).

It is important to underline that communication with ATC is considered as a human barrier because it represents the trained elements made by men but it represents also the technological part because the communication is created with opportune instruments.
The choice of the values for different barriers was made with the comparison of two sector experts [33], Alberto Ottomaniello and Italo Oddone, who work for Air Dolomiti.

5.1.4 Severity levels and risk matrix

Starting from the analysis of the case study and the severity natures in table 5.8, the four most appropriate natures were selected for this work: non-routine incidents, customer impact, equipment and compliance (see table 5.9).
The risk matrix used was adapted starting from the one in figure 5.1 in which the probability ranges were modified in order to be applied to the case study. Indeed, the new matrix and the new probability boundaries

are reported in figure 5.3; it is possible to notice that it was necessary to consider the number of flights made by Air Dolomiti in order to define the new values and ranges of the probabilities. For this reason it is not possible to consider the same ranges and values for every airline but it is necessary to adjust them.
In figure 5.2 the risk levels and their mitigation considered for this thesis are reported.

In §5.4 the risk calculation with the range of probability considered in ICAO risk matrix are reported: it is possible to notice that some sequences have a higher risk than the case analysed in §5.1.5 and they can be in the unacceptable zone of the risk matrix.

In table 5.10 the possible number of flights of a medium airline, as Air Dolomiti, are reported along with the original and the new value of probability considered; the new values were evaluated taking into account the possible number of daily, weekly and monthly flights.

Table 5.8: Starting nature severity level [34].

Severity level	S5	S4	S3	S2	S1	S0
NATURE	Extreme	High	Medium	Low	Minor	None
Injury	Multiple fatalities and/or permanent disabilities with serious illness or health impairments.	Fatalities and/or permanent disability with serious illness or health impairment.	Serious but non-permanent injuries (e.g. loss time injury).	Injuries requiring medical first aid treatment only.	No or minor injuries (First aid treatment).	None.
Non-Routine Incidents (modified ICAO definition)	Total loss or hull loss	Accident with serious injuries or fatalities, or significant damage to aircraft.	Serious incident with injuries and/or substantial damage to aircraft.	Incident with minor injury and or minor aircraft damage.	Incident with discomfort and/or less than minor system damage.	None.
Property or A/C Damage Cost	>20 Mio EUR	400.000 EUR to 20 Mio. EUR	10.000 EUR to 400.000 EUR	300 EUR to 10.000 EUR	<300 EUR	None
Reputation and Public Confidence	Fundamental change in the public perception of quality airline.	Extended national or international negative media coverage.	Short-term nation-wide negative media coverage.	Negative local media coverage.	None.	None.
Customer Impact	Extensive shut down of services for an extended period. All customers affected.	More than 40 flights cancelled, rescheduled or delayed. Thousands of customers affected.	Between 1 and 40 flights cancelled, rescheduled or delayed. Hundreds of customers affected.	Between 2 and 5 flights rescheduled or delayed. Dozens of customers affected.	1 flight rescheduled or delayed. Small number of customers affected.	None.

Table 5.8: Continues on next page

Table 5.8: Continues from previous page

Operational Impact	Fleet grounding for extended period.	Brief fleet grounding up to 2 days.	Aircraft grounding more than 2 days.	Aircraft grounding 4 to 48 hours.	Aircraft delay less than 4 hrs.	None.
Equipment	Loss of critical equipment, shutdown of organization.	Major damage, results in major slowdown and/or downtime.	Minor damage, leads to organizational slowdown and/or minor downtime.	Minor damage, potential organizational slowdown and/or downtime.	No adverse consequences.	None.
Compliance	Significant disruption to scheduled services over an extended period of time.	Substantial fine and disruption to scheduled services.	Substantial fine but no disruption to scheduled services.	No fine and no disruption to scheduled services.	Minor breaches by individual staff members.	None.
Process Breach	Several steps of flight critical process not followed or flight critical process non-existent.	No steps of documented process followed or process non-existent.	Majority of steps of documented process not followed or process unknown.	Contiguous steps of documented process not followed or process partly unclear.	Some single steps of documented process not followed.	None.
Know-How Loss	Dramatic loss resulting in fully new build-up requiring more than 2 years.	Heavy loss resulting in substantial build-up and/or renewal requiring 1-2 years.	Worrying loss resulting in substantial build-up and/or renewal requiring up to 1 year.	Loss resulting in noticeable build-up and/or renewal requiring 3-6 months.	Slight loss that can be easily absorbed within the existing organization within 3 months.	None.

Table 5.8: Continues on next page

Table 5.8: Continues from previous page

Safety Awareness Ignorance	Intolerable total absence of safety awareness demanding immediate dismissal.	Unusually high level of safety awareness ignorance needing immediate correction or dismissal.	Unacceptable attitude toward safety awareness needing immediate correction or dismissal warning.	Generally acceptable attitude toward safety awareness with occasional blackouts needing pronounced and lasting correction.	Sound attitude toward safety awareness with occasional and isolated misjudgment needing clarification and lasting educational influence.	None.

Table 5.9: Nature severity level selected. [34]

Severity level	S5	S4	S3	S2	S1	S0
NATURE	Extreme	High	Medium	Low	Minor	None
Non-Routine Incidents (modified ICAO definition)	Total loss or hull loss.	Accident with serious injuries or fatalities, or significant damage to aircraft.	Serious incident with injuries and/or substantial damage to aircraft.	Incident with minor injury and or minor aircraft damage	Incident with discomfort and/or less than minor system damage.	None.
Customer Impact	Extensive shut down of services for an extended period. All customers affected.	More than 40 flights cancelled, rescheduled or delayed. Thousands of customers affected.	Between 1 and 40 flights cancelled, rescheduled or delayed. Hundreds of customers affected.	Between 2 and 5 flights rescheduled or delayed. Dozens of customers affected.	1 flight rescheduled or delayed. Small number of customers affected.	None.
Equipment	Loss of critical equipment, shutdown of organization.	Major damage, results in major slowdown and/or downtime.	Minor damage, leads to organizational slowdown and/or minor downtime.	Minor damage, potential organizational slowdown and/or downtime.	No adverse consequences.	None.
Compliance	Significant disruption to scheduled services over an extended period of time.	Substantial fine and disruption to scheduled services.	Substantial fine but no disruption to scheduled services.	No fine and no disruption to scheduled services.	Minor breaches by individual staff members.	None.

	Severity Level					
Probability Level	S5 Extreme	S4 High	S3 Medium	S2 Low	S1 Minor	S0 None
P5 Frequent 9.0E-04 < P ≤ 1	A	A	B	C	D	E
P4 Likely 1.0E-04 < P ≤ 9.0E-04	A	A	B	C	D	E
P3 Possible 1.0E-05 < P ≤ 1.0E-04	A	B	C	D	E	E
P2 Low 2.0E-06 < P ≤ 1.0E-05	A	B	C	D	E	E
P1 Unlikely 2.0E-07 < P ≤ 2.0E-06	B	C	D	E	E	E
P0 Remote 2.0E-08 < P ≤ 2.0E-07	C	C	D	E	E	E
Pe Extr. Remote P ≤ 2.0E-08	C	D	E	E	E	E

Figure 5.1: Initial risk matrix. [34] [35]

Risk Level	Risk	Risk mitigation
A	Estreme	Immediate mitigation required
B	High	Short term improvement
C	Acceptable with mitigation	Long term improvement required
D	Low	Monitor
E	Negligible	Collect data

Figure 5.2: Risk level and mitigation.

Table 5.10: Choice probability level. [34]

Probability level	One out of flights	Probability	New values probability
P5	140	7.3E-03	1
P4	1.100	9.0E-04	3.2E-03
P3	10.000	1.0E-04	2.9E-04
P2	100.000	1.0E-05	2.6E-05
P1	500.000	2.0E-06	4.4E-06
P0	5.000.000	2.0E-07	6.25E-07
Pe	50.000.000	2.0E-08	6.25E-08

	Severity Level					
Probability Level	S5 Extreme	S4 High	S3 Medium	S2 Low	S1 Minor	S0 None
P5 Frequent $3.2E\text{-}03 < P \leq 1$	A	A	B	C	D	E
P4 Likely $2.9E\text{-}04 < P \leq 3.2E\text{-}03$	A	A	B	C	D	E
P3 Possible $2.6E\text{-}05 < P \leq 2.9E\text{-}04$	A	B	C	D	E	E
P2 Low $4.4E\text{-}06 < P \leq 2.6E\text{-}05$	A	B	C	D	E	E
P1 Unlikely $6.25E\text{-}07 < P \leq 4.4E\text{-}06$	B	C	D	E	E	E
P0 Remote $6.25E\text{-}08 < P \leq 6.25E\text{-}07$	C	C	D	E	E	E
Pe Extr. Remote $P \leq 6.25E\text{-}08$	C	D	E	E	E	E

Figure 5.3: Final risk matrix.

5.1.5 Hazards and risk matrix

Hazard No.1
Software initialization not completed

In table 5.12 the initial event, the incident consequences and the final value of the probabilities are presented. The value of probability and the severity level give the risk associated to the sequence; the probability of the hazard was evaluated with the TESEO method while the consequences were evaluated with the EJ method. The values of the barriers and the incident sequences considered are also reported.
The values of the TESEO method coefficients (K) for the HU calculation of the hazard are presented in table 5.11.

Table 5.11: Software initialization not completed

K_1	Requiring attention, routine	0.01
K_2 (a)	20 (s)	0.5
K_3	Average knowledge and training	1
K_4	Normal situation	1
K_5	Discrete microclimate, discrete interface with plant	3

The expression to calculate HU is:

$$HU = K_1 \cdot K_{2_a} \cdot K_3 \cdot K_4 \cdot K_5 = 0.01 \cdot 0.5 \cdot 1 \cdot 1 \cdot 3 = 0.015 \tag{5.1}$$

This hazard is considered as a routine activity requiring some attention, with a long reaction time from the operator; the work environment resulting from this hazard can be associated with a normal working situation.
The barriers considered are maintenance and processes (MQ), TCAS and EGPWS: TCAS is used to reduce the loss of separation while EGPWS is used for CFIT. This statement is applied to all hazards that consider loss of separation and CFIT as incident sequence.
In this hazard the possible sequences with the relative barriers are:

1. Software initialization not completed + Flight cancellation or delay.
   The barrier is maintenance and processes (MQ).

2. Software initialization not completed + Loss of separation.
   The barriers are maintenance and processes (MQ) and TCAS.

3. Software initialization not completed + Loss of separation + CFIT.
   The barriers are maintenance and processes (MQ), TCAS and EGPWS.

The values considered for the barriers are:

- maintenance and processes: $MQ = 0.4$;
- Terrain Control Avoidance System: $TCAS = 0.3$;
- Enhanced Ground Proximity Warning System: $EGPWS = 0.3$;

The expressions used to estimate the values of probability are the following:

$$\begin{cases} P_{1a} = MQ \cdot P_{Software} \cdot P_{Flight} \\ P_{1b} = MQ \cdot P_{Software} \cdot P_{Loss} \\ P_{1c} = MQ \cdot P_{Software} \cdot [P_{Loss} \cdot P_{CFIT}] \end{cases} \tag{5.2}$$

The results obtained with the expressions are:

$$\begin{cases} P_{1a} = 3.0E-04 \\ P_{1b} = 1.8E-09 \\ P_{1c} = 5.4E-13 \end{cases} \tag{5.3}$$

This subdivision is possible because CFIT is the consequence of loss separation, therefore the probability of the last sequence depends on the previous one, while flight cancellation is considered as a consequence only of the initial event.
Starting from these results it was possible to evaluate which sequence has the higher probability and, through the severity, to find the cell in the risk matrix.

Table 5.12: Hazard No.1 - Software initialization not completed

Hazard	Incident sequence description		Existing control				
No. 1	Consequences	Probab. without control		Probab. reduction	Severity	Probab.	Risk
Software initialization not completed	Flight cancellation or delay	0.5E-01	MQ	0.4	Low	3.0E-04	C
	Loss of separation	1.0E-06	MQ TCAS	0.4 0.3	High	1.8E-09	D
TESEO: 0.015	CFIT	1.0E-03	MQ TCAS EGPWS	0.4 0.3 0.3	Extreme	5.4E-13	C

Hazard No.2
Maps not available. Cockpit preparation

This hazard can be generated from two activities: wrong loading of the EFB software and lack of software update; moreover the maps are not available on EFB.
The probabilities of the initial event was estimated with the EJ method and there is a distinction between phase of cockpit preparation and phase of taxiing. The phase of taxiing has an higher probability than the phase of cockpit preparation because the time available to recover missing information during the phase taxiing is lower.

Phase of cockpit preparation

In table 5.13 the values of probability of the hazard and the possible consequences are reported; the values were all evaluated with the EJ method, based on previous experiences.
For this hazard the barrier considered is maintenance and processes (MQ) and the only possible sequence is:

1. Maps not available + Flight cancellation or delay.
   The barrier is maintenance and processes (MQ).

The value considered for the barrier is:

- maintenance and processes: $MQ = 0.4$;

The expression used to estimate the value of probability is:

$$P_2 = MQ \cdot P_{Maps} \cdot P_{FlightDiversion} \tag{5.4}$$

The result obtained is:

$$P_2 = 2.0E - 05 \tag{5.5}$$

The risk level was then evaluated considering the probability and the severity associated in the risk matrix.

Table 5.13: Hazard No.2 - Maps not available. Cockpit preparation phase.

Hazard	Incident sequence description		Existing control				
No. 2	Consequences	Probab. without control		Probab. reduction	Severity	Probab.	Risk
Maps not available EJ: 1.0E-03	Flight cancellation or delay	0.5E-01	M Q	0.4	Low	2.0E-05	D

Phase taxiing

In this phase, the initial event is the same that in the previous case but it is different for the value of probability defined with the EJ method. The value of the hazard probability is higher than the one for the phase of cockpit preparation.
The probabilities of the consequences were evaluated with the EJ method and the possible sequences are reported in the following list:

1. Maps not available + Flight cancellation or delay.
   The barrier is maintenance and processes (MQ).
2. Maps not available + Loss of separation.
   The barriers are maintenance and processes (MQ) and TCAS.
3. Maps not available + Loss of separation + CFIT.
   The barriers are maintenance and processes (MQ), TCAS and EGPWS.

The values considered for the barriers are:

- maintenance and processes control: $MQ = 0.4$;
- Terrain Control Avoidance System: $TCAS = 0.3$;
- Enhanced Ground Proximity Warning System: $EGPWS = 0.3$;

The expressions utilised to estimate the values of probability are the following:

$$\begin{cases} P_{2a} = MQ \cdot P_{Maps} \cdot P_{FlightDiversion} \\ P_{2b} = MQ \cdot TCAS \cdot P_{Maps} \cdot P_{Loss} \\ P_{2c} = MQ \cdot TCAS \cdot EGPWS \cdot P_{Maps} \cdot [P_{Loss} \cdot P_{CFIT}] \end{cases} \tag{5.6}$$

The results obtained with the expressions are:

$$\begin{cases} P_{2a} = 2.0E-04 \\ P_{2b} = 1.2E-07 \\ P_{2c} = 3.6E-11 \end{cases} \tag{5.7}$$

Considering the selected severity levels and the values of probability calculated the cell in the risk matrix was determined.

Table 5.14: Hazard No.2 - Maps not available. Taxiing phase.

Hazard	Incident sequence description		Existing control				
No. 2	Consequences	Probab. without control		Probab. reduction	Severity	Probab.	Risk
Maps not available	Flight cancellation or delay	0.5E-01	M Q	0.4	Low	2.0E-04	D
	Loss of separation	1.0E-04	MQ TCAS	0.4 0.3	High	1.2E-07	C
EJ: 1.0E-02	CFIT	1.0E-03	M Q TCAS EGPWS	0.4 0.3 0.3	Extreme	3.6E-11	C

Hazard No.3
Improper selection of portrait

The value of probability of this hazard was evaluated with the TESEO method; the consequences, instead, were evaluated with the EJ method. The values of the TESEO method coefficients (K) for the HU calculation are presented in table 5.15.

Table 5.15: Improper selection of portrait

K_1	Requiring attention, routine	0.01
K_2 (a)	10 (s)	1
K_3	Average knowledge and training	1
K_4	Situation of potential emergency	2
K_5	Discrete microclimate, discrete interface with plant	3

The expression to evaluate HU is:

$$HU = K_1 \cdot K_{2_a} \cdot K_3 \cdot K_4 \cdot K_5 = 0.01 \cdot 1 \cdot 1 \cdot 2 \cdot 3 = 0.06 \tag{5.8}$$

As in the hazard No.1, a routine activity requiring attention from the operator is considered but the response time is shorter since the hazard can show consequences in a shorter period of time. For the same reason a potential emergency situation is considered in the anxiety factor.

The barriers considered for this hazard are training, SOP or EOP, TCAS and EGPWS. It is important to underline that the application of SOP and EOP is not considered together for the calculation of probability but one of them is selected for each sequence based on the type of consequence (standard or emergency) in the sequence analysed. In the following the list of sequences used for the calculation of the probabilities and the barriers considered are reported:

1. Improper selection of portrait + Flight cancellation or delay.
   The barriers are training and SOP.
2. Improper selection of portrait + Loss of separation.
   The barriers are training, EOP and TCAS.
3. Improper selection of portrait + Loss of separation + CFIT.
   The barriers are training, EOP, TCAS and EGPWS.

The values for the barriers are:

- training: $Training = 0.4$;
- Standard Operating Procedures: $SOP = 0.4$;
- Emergency Operating Procedures: $EOP = 0.4$;
- Terrain Control Avoidance System: $TCAS = 0.3$;
- Enhanced Ground Proximity Warning System: $EGPWS = 0.3$;

The expressions used to evaluate the probabilities are:

$$\begin{cases} P_{3a} = Training \cdot SOP \cdot P_{Portrait} \cdot P_{FlightDiversion} \\ P_{3b} = Training \cdot EOP \cdot TCAS \cdot P_{Portrait} \cdot P_{Loss} \\ P_{3c} = Training \cdot EOP \cdot TCAS \cdot EGPWS \cdot P_{Portrait} \cdot [P_{Loss} \cdot P_{CFIT}] \end{cases} \tag{5.9}$$

The results are:

$$\begin{cases} P_{3a} = 4.8E-04 \\ P_{3b} = 2.88E-06 \\ P_{3c} = 8.64E-10 \end{cases} \tag{5.10}$$

It was possible to find the values of probability of the first and the second incident sequence multiplying the probability of initial event by the probability of the first and the second consequence; however the probability of the third incident sequence (CFIT) was calculated multiplying the relative value of probability by the probability of the second sequence.
The severity of every event allowed, along with the probability values, to obtain the risk level in risk matrix.

Table 5.16: Hazard No.3 - Improper selection of portrait.

Hazard	Incident sequence description		Existing control				
No. 3	Consequences	Probab. without control		Probab. reduction	Severity	Probab.	Risk
Improper selection of portrait TESEO: 0.06	Flight cancellation or delay	0.5E-01	Training SOP	0.4 0.4	Low	4.8E-04	C
	Loss of separation	1.0E-03	Training EOP TCAS	0.4 0.4 0.3	High	2.88E-06	C
	CFIT	1.0E-03	Training EOP TCAS EGPWS	0.4 0.4 0.3 0.3	Extreme	8.64E-10	C

Hazard No.4
Improper storage of PC

In table 5.18 the initial event and the possible consequences are reported; each sequence includes both the relative consequences, therefore the probability of the hazard was multiplied by the probability of the consequences. The probability of initial event was calculated with the TESEO method for both possible sequences.
The values of the TESEO method coefficients K for the HU calculation are presented in table 5.17.

Table 5.17: Improper storage of PC

K_1	Requiring attention, routine	0.01
K_2 (a)	10 (s)	1
K_3	Average knowledge and training	1
K_4	Situation of potential emergency	2
K_5	Discrete microclimate, discrete interface with plant	3

$$HU = K_1 \cdot K_{2_a} \cdot K_3 \cdot K_4 \cdot K_5 = 0.01 \cdot 1 \cdot 1 \cdot 2 \cdot 3 = 0.06 \tag{5.11}$$

This hazard is catalogued, based on the possible consequences, as a routine action requiring attention in an average period of time; the value of K_2 was therefore selected from table 5.2a. The anxiety factor was selected considering a potential emergency situation.

Table 5.18: Hazard No.4 - Improper storage of PC.

Hazard	Incident sequence description		Existing control				
No. 4	Consequences	Probab. without control		Probab. reduction	Severity	Probab.	Risk
Improper storage of PC TESEO: 0.06	Damage to cables/PC Fire/smoke in the cabin	1.0E-03 1.0E-03	M Q SOP	0.4 0.4	High High	9.6E-09	D
	Damage to cables/PC Flight cancellation or delay	1.0E-03 0.5E-01	MQ SOP	0.4 0.4	High Low	4.8E-07	C

The barriers considered for this hazard are maintenance and processes (MQ) and SOP (Standard Operating Procedures).
The possible sequences with their relative barriers are:

1. Improper storage of PC + Damage to cables / PC + Fire / smoke in the cabin.
   The barriers are maintenance and processes (MQ) and SOP .
2. Improper storage of PC + Damage to cables / PC + Flight cancellation or delay.
   The barriers are maintenance and processes (MQ) and SOP .

The values considered for the barriers are:

- maintenance and processes: $MQ = 0.4$;
- Standard Operating Procedures: $SOP = 0.4$.

The expressions used to estimate the values of probability are the following:

$$\begin{cases} P_{4a} = MQ \cdot SOP \cdot P_{PC} \cdot [P_{Damage} \cdot P_{Fire}] \\ P_{4b} = MQ \cdot SOP \cdot P_{PC} \cdot [P_{Damage} \cdot P_{Flight}] \end{cases} \tag{5.12}$$

The results obtained are:

$$\begin{cases} P_{4a} = 9.6E-09 \\ P_{4b} = 4.8E-07 \end{cases} \tag{5.13}$$

Through the value of probability and severity level considered it was possible to identify in which cell of the risk matrix the risk is.

Hazard No.5
Pilots unable to locate maps

For this hazard the TESEO method was used for the calculation of the probability while the consequences were estimated with the EJ method. The values of the TESEO method coefficients (K) for the HU calculation are presented in table 5.19.

Table 5.19: Pilots unable to locate maps

K_1	Requiring attention, routine	0.01
K_2 (a)	20 (s)	0.5
K_3	Average knowledge and training	1
K_4	Situation of potential emergency	2
K_5	Discrete microclimate, discrete interface with plant	3

The expression to calculate the HU is:

$$HU = K_1 \cdot K_{2_a} \cdot K_3 \cdot K_4 \cdot K_5 = 0.01 \cdot 0.5 \cdot 1 \cdot 2 \cdot 3 = 0.03 \tag{5.14}$$

The features considered for this hazard are similar to the ones described in the previous cases; indeed, the inability of the pilots to locate the necessary maps is a routine event which requires attention. This can lead to a potential emergency situation and, consequently, to an increased anxiety. The reaction time selected for this hazard is the maximum for this type of situation: 20 seconds.

Table 5.20: Hazard No.5 - Pilots unable to locate maps.

Hazard	Incident sequence description		Existing control				
No. 5	Consequences	Probab. without control		Probab. reduction	Severity	Probab.	Risk
Pilots unable to locate maps TESEO: 0.03	Loss of separation	1.0E-03	Training EOP TCAS	0.4 0.4 0.3	High	1.44E-06	C
	CFIT	1.0E-03	Training EOP TCAS EGPWS	0.4 0.4 0.3 0.3	Extreme	4.32E-10	C

In this case only two sequences are possible and the barriers are training, EOP, TCAS and EGPWS. In the following the list of possible sequences and their barriers are reported:

1. Pilots unable to locate maps + Loss of separation.
   The barriers considered are training, EOP and TCAS.

2. Pilots unable to locate maps + Loss of separation + CFIT.
   The barriers are training, EOP, TCAS and EGPWS.

The values for the barriers are:

- training: $Training = 0.4$;
- Emergency Operating Procedures: $EOP = 0.4$;
- Terrain Control Avoidance System: $TCAS = 0.3$;
- Enhanced Ground Proximity Warning System: $EGPWS = 0.3$.

The expressions used to evaluate the values of probability are the following:

$$\begin{cases} P_{5a} = Training \cdot EOP \cdot TCAS \cdot P_{Pilots} \cdot P_{Loss} \\ P_{5b} = Training \cdot EOP \cdot TCAS \cdot EGPWS \cdot P_{Pilots} \cdot [P_{Loss} \cdot P_{CFIT}] \end{cases} \tag{5.15}$$

The results obtained with the previous expressions are:

$$\begin{cases} P_{5a} = 1.44E-06 \\ P_{5b} = 4.32E-10 \end{cases} \tag{5.16}$$

After these calculations it was possible to locate the intersection cell in the risk matrix considering the value of the probability and the severity level decided for the sequence.

Hazard No.6
Loss of SA

The risk evaluation for this hazard was particular because it was necessary to consider that this situation depends on the crew who can be careless or that can be exposed to an high workload. Therefore, it was advisable to calculate the value of probability through the EJ method.
A distinction between three different conditions of loss of SA is necessary: known airport condition, new destination (different airport from usual) and emergency situation. The values of the probability were estimated for every sequence in each case. From tables 5.21, 5.22 and 5.23 it is possible to notice that the hazard probability in case of emergency situation is the highest while for the case of known airport the probability of loss of awareness is the lowest. The probability of the initial event was decided

considering the three different cases: this is higher in the emergency situation.
In these three different conditions it is possible to underline that CFIT consequence, as in other hazards described, depends on the loss of separation while the flight diversion or delay incident sequence is a separated one.
The barriers for this hazard are training, SOP and/or EOP, TCAS and EGPWS. The choice between SOP or EOP depends on the particular sequence considered.
The possible sequences with their barrier are:

1. Loss of SA + Flight diversion or delay.
   The barriers for this sequence are training and SOP.
2. Loss of SA + Loss of separation.
   The barriers are training, EOP and TCAS.
3. Loss of SA + Loss of separation + CFIT.
   The barrier are training, EOP, TCAS and EGPWS.

The values of the barriers are:

- training: $Training = 0.4$;
- Standard Operating Procedures: $SOP = 0.4$;
- Emergency Operating Procedures: $EOP = 0.4$;
- Terrain Control Avoidance System: $TCAS = 0.3$;
- Enhanced Ground Proximity Warning System $EGPWS = 0.3$.

These sequences and the relative barriers are the same for the three cases reported below; the difference is on the probability of the hazard.

Known airport

The expressions used to evaluate the values of the probability are:

$$\begin{cases} P_{6a} = Training \cdot SOP \cdot P_{SA} \cdot P_{Flight} \\ P_{6b} = Training \cdot EOP \cdot TCAS \cdot P_{SA} \cdot P_{Loss} \\ P_{6c} = Training \cdot EOP \cdot TCAS \cdot EGPWS \cdot P_{SA} \cdot [P_{Loss} \cdot P_{CFIT}] \end{cases} \tag{5.17}$$

The results obtained with these expressions are:

$$\begin{cases} P_{6a} = 8.0E-07 \\ P_{6b} = 4.8E-09 \\ P_{6c} = 1.44E-12 \end{cases} \tag{5.18}$$

The risk level associated to each sequence was then determined.

Table 5.21: Hazard No.6 - Loss of SA. Known airport.

Hazard	Incident sequence description		Existing control				
No. 6	Consequences	Probab. without control		Probab. reduction	Severity	Probab.	Risk
Loss of SA EJ: 1.0E-04	Flight diversion or delay	0.5E-01	Training SOP	0.4 0.4	Low	8.0E-07	E
	Loss of separation	1.0E-03	Training EOP TCAS	0.4 0.4 0.3	High	4.8E-09	D
	CFIT	1.0E-03	Training EOP TCAS EGPWS	0.4 0.4 0.3 0.3	Extreme	1.44E-12	C

New destination (new airport)

The expressions used to estimate the values of the probability are:

$$\begin{cases} P_{6a} = Training \cdot SOP \cdot P_{SA} \cdot P_{Flight} \\ P_{6b} = Training \cdot EOP \cdot TCAS \cdot P_{SA} \cdot P_{Loss} \\ P_{6c} = Training \cdot EOP \cdot TCAS \cdot EGPWS \cdot P_{SA} \cdot [P_{Loss} \cdot P_{CFIT}] \end{cases} \tag{5.19}$$

The results obtained are:

$$\begin{cases} P_{6a} = 8.0E-06 \\ P_{6b} = 2.4E-07 \\ P_{6c} = 7.2E-11 \end{cases} \tag{5.20}$$

In this case there are three possible sequences: in table 5.22 their probability values of the probability and their severity levels are reported. It was therefore possible to identify the risk level in the risk matrix.

Table 5.22: Hazard No.6 - Loss of SA. New destination (new airport).

Hazard	Incident sequence description		Existing control				
No. 6	Consequences	Probab. without control		Probab. reduction	Severity	Probab.	Risk
Loss of SA EJ: 1.01E-03	Flight diversion or delay	0.5E-01	Training SOP	0.4 0.4	Low	8.0E-06	D
	Loss of separation	5.0E-03	Training EOP TCAS	0.4 0.4 0.3	High	2.4E-07	C
	CFIT	1.0E-03	Training EOP TCAS EGPWS	0.4 0.4 0.3 0.3	Extreme	7.2E-11	C

Emergency situation

The expressions used to estimate the values of the probability are the following:

$$\begin{cases} P_{6a} = Training \cdot SOP \cdot P_{SA} \cdot P_{Flight} \\ P_{6b} = Training \cdot EOP \cdot TCAS \cdot P_{SA} \cdot P_{Loss} \\ P_{6c} = Training \cdot EOP \cdot TCAS \cdot EGPWS \cdot P_{SA} \cdot [P_{Loss} \cdot P_{CFIT}] \end{cases} \tag{5.21}$$

The results are:

$$\begin{cases} P_{6a} = 8.0E-05 \\ P_{6b} = 4.8e-06 \\ P_{6c} = 1.44e-09 \end{cases} \tag{5.22}$$

In this case, as in the previous ones, it was possible to evaluate the risk considering the intersection cell between the value of probability and the severity level in the risk matrix.

Table 5.23: Hazard No.6 - Loss of SA. Emergency situation.

Hazard	Incident sequence description		Existing control				
No. 6	Consequences	Probab. without control		Probab. reduction	Severity	Probab.	Risk
Loss of SA EJ: 1.0E-02	Flight diversion or delay	0.5E-01	Training SOP	0.4 0.4	Low	8.0E-05	D
	Loss of separation	1.0E-02	Training EOP TCAS	0.4 0.4 0.3	High	4.8E-06	B
	CFIT	1.0E-03	Training EOP TCAS EGPWS	0.4 0.4 0.3 0.3	Extreme	1.44E-09	C

Hazard No.7
No charts on show

This hazard can be caused by maps not updated on EFB or maps showed on EFB display: it is therefore necessary to use the paper maps. The appropriate method for the calculation of probability was EJ. It is necessary to divide this hazard into two phases: cockpit preparation phase and taxiing phase; the first phase is characterized by lower value of the probability of the initial event.

Cockpit preparation phase

The barrier considered for this phase is maintenance and processes (MQ) and its value is 0.4; the sequence allowed is:

1. No charts on show + Flight diversion or delay.

The expression used to estimate the value of the probability is:

$$P_7 = MQ \cdot P_{Charts} \cdot P_{Flight} \tag{5.23}$$

The result obtained is:

$$P_7 = 2.0E - 04 \tag{5.24}$$

Table 5.24: Hazard No.7 - No charts on show - Cockpit preparation phase.

Hazard	Incident sequence description		Existing control				
No. 7	Consequences	Probab. without control		Probab. reduction	Severity	Probab.	Risk
No charts on show EJ: 1.0E-02	Flight delay	0.5E-01	MQ	0.4	Low	2.0E-04	D

Taxiing phase

The barriers considered are maintenance and processes (MQ), TCAS and EGPWS and the possible sequences are:

1. No charts on show + Flight diversion or delay.
   The barriers allowed is maintenance and processes (MQ).
2. No charts on show + Loss of separation.
   The barriers are maintenance and processes (MQ) and TCAS.
3. No charts on show + Loss of separation + CFIT.
   The barriers considered are maintenance and processes (MQ) and TCAS and EGPWS.

The values of the barriers are:

- maintenance and processes: $MQ = 0.4$;
- Terrain Control Avoidance System: $TCAS = 0.3$;
- Enhanced Ground Proximity Warning System: $EGPWS = 0.3$.

The expressions used to estimate the values of the probability are:

$$\begin{cases} P_{7a} = MQ \cdot P_{Charts} \cdot P_{Flight} \\ P_{7b} = MQ \cdot TCAS \cdot P_{Charts} \cdot P_{Loss} \\ P_{7c} = MQ \cdot TCAS \cdot EGPWS \cdot P_{Charts} \cdot [P_{Loss} \cdot P_{CFIT}] \end{cases} \tag{5.25}$$

The results obtained with the expressions are:

$$\begin{cases} P_{7a} = 2.0E-05 \\ P_{7b} = 1.2E-08 \\ P_{7c} = 3.6E-12 \end{cases} \tag{5.26}$$

The risk level was then evaluated, knowing the severity level.

Table 5.25: Hazard No.7 - No charts on show - Taxiing phase.

Hazard	Incident sequence description		Existing control				
No. 7	Consequences	Probab. without control		Probab. reduction	Severity	Probab.	Risk
No charts on show	Flight diversion or delay	0.5E-01	MQ	0.4	Low	2.0E-05	D
	Loss of separation	1.0E-03	M Q TCAS	0.4 0.3	High	1.2E-08	D
EJ: 1.0E-04	CFIT	1.0E-03	M Q TCAS EGPWS	0.4 0.3 0.3	Extreme	3.6E-12	C

Hazard No.8
Flying with wrong maps or without maps

This hazard occurs when EFB does not work so it is necessary to use the paper maps which are not present on board (see table 5.6 and in particular the Activities or Issues column). So, it is necessary to remember that EFB does not work and the paper maps are absent.
The probability of the initial event was calculated with the TESEO method and the values of the coefficients (K) for the HU calculation are presented in table 5.26.

Table 5.26: Flying with wrong maps or without maps

K_1	Requiring attention, routine	0.01
K_2 (a)	20 (s)	0.5
K_3	Average knowledge and training	1
K_4	Situation of potential emergency	2
K_5	Discrete microclimate, discrete interface with plant	3

The expression of the calculation of HU is:

$$HU = K_1 \cdot K_{2_a} \cdot K_3 \cdot K_4 \cdot K_5 = 0.01 \cdot 0.5 \cdot 1 \cdot 2 \cdot 3 = 0.03 \qquad (5.27)$$

Flying with the wrong maps or without them is considered a routine activity that requires attention and an immediate reaction is not required. Since the activity is a routine type, the K_2 factor shall be selected from table 5.2a. The resulting situation is of potential emergency and the anxiety factor is higher than in a normal situation.

Table 5.27: Hazard No.8 - Flying with wrong maps or without maps.

Hazard	Incident sequence description		Existing control				
No. 8	Consequences	Probab. without control		Probab. reductio n	Severity	Probab.	Risk
Flying with wrong maps or without maps	Flight diversion or delay	0.5E-01	Training SOP	0.4 0.4	Low	2.4E-04	D
	Loss of separation	1.0E-03	Training EOP TCAS	0.4 0.4 0.3	High	1.44E-06	C
TESEO: 0.03	CFIT	1.0E-03	Training EOP TCAS EGPWS	0.4 0.4 0.3 0.3	Extreme	4.32E-10	C

The barriers considered for this hazard are training, SOP or EOP, TCAS and EGPWS. The possible sequences are three and they are divided into:

1. Flying with wrong maps or without maps + Flight diversion or delay.
   The barriers are training and SOP.

2. Flying with wrong maps or without maps + Loss of separation.
   The barriers are training, EOP, TCAS.

3. Flying with wrong maps or without maps + Loss of separation + CFIT.
   The barriers are training, EOP, TCAS and EGPWS.

The values of the barriers are:

- Standard Operating Procedures: $SOP = 0.4$;
- Emergency Operating Procedures: $EOP = 0.4$;
- Terrain Control Avoidance System: $TCAS = 0.3$;
- Enhanced Ground Proximity Warning System: $EGPWS = 0.3$.

The expressions used for the calculation of probability are the following:

$$\begin{cases} P_{8a} = Training \cdot SOP \cdot P_{Flying} \cdot P_{Flightdiversion} \\ P_{8b} = Training \cdot EOP \cdot TCAS \cdot P_{Flying} \cdot P_{Loss} \\ P_{8c} = Training \cdot EOP \cdot TCAS \cdot EGPWS \cdot P_{Flying} \cdot [P_{Loss} \cdot P_{CFIT}] \end{cases} \tag{5.28}$$

The results obtained are:

$$\begin{cases} P_{8a} = 2.4E-04 \\ P_{8b} = 1.44E-06 \\ P_{8c} = 4.32E-10 \end{cases} \tag{5.29}$$

At the end, the values of the probability obtained with the calculation were used, along with the severity level, to enter the risk matrix and obtain an assessment of the risk.

Hazard No.9
No coordinates for cross-check with FMS (impossible to see taxiway)

In this hazard EFB is not coordinated with the on-board computer GPS so there is no correspondence between coordinates. The initial event was evaluated through the EJ method and the runway incursion incident sequence is directly connected with ground collision since the last one depends on the first one. Moreover the ground collision consequence includes the collisions with other aircraft or with infrastructures and vehicles in movement on the airfield.
It is important to remind that the necessary coordinates are available from FMS even if EFB does not provide the correct coordinates.
The possible barriers for these sequences are ATC communication, training and SOP. The sequences are:

1. No coordinates for cross-check with FMS + Runway incursion.
   The barriers are ATC communication, training and SOP.

2. No coordinates for cross-check with FMS + Runway incursion + Ground collision.
   The barriers are ATC communication, training and SOP.

3. No coordinates for cross-check with FMS + Wrong runway take-off.
   The barriers evaluated are ATC communication, training and SOP.

The values considered for the barriers are:

- training: $Training = 0.4$;
- Standard Operating Procedures: $SOP = 0.4$;
- Air Traffic Control communication: $ATC = 0.4$.

The expressions used to estimate the values of probability are the following:

$$\begin{cases} P_{9a} = ATC \cdot Training \cdot SOP \cdot P_{FMS} \cdot P_{Runway} \\ P_{9b} = ATC \cdot Training \cdot SOP \cdot P_{FMS} \cdot [P_{Runway} \cdot P_{Collisoion}] \\ P_{9c} = ATC \cdot Training \cdot SOP \cdot P_{FMS} \cdot P_{WrongRunway} \end{cases} \quad (5.30)$$

The results obtained are:

$$\begin{cases} P_{9a} = 6.4E-07 \\ P_{9b} = 6.4E-10 \\ P_{9c} = 6.4E-08 \end{cases} \quad (5.31)$$

The hazard, impossible to see taxiway, is included in this hazard because they are connected and they have the same consequences in the incident sequence. Moreover, this is possible because the impossibility to see the taxiway is not connected directly with the use of EFB but with the coordinates for the crossed control.

Table 5.28: Hazard No.9 - No coordinates for Xcheck with FMS (impossible to see taxiway.

Hazard	Incident sequence description		Existing control				
No. 9	Consequences	Probab. without control		Probab. reduction	Severity	Probab.	Risk
No coordinates for Xcheck with FMS (impossible to see taxiway)	Runway incursion	1.0E-02	ATC Training SOP	0.4 0.4 0.4	Medium	6.4E-07	D
	Ground collision (aircraft, infrastructures and vehicles)	1.0E-03	ATC Training SOP	0.4 0.4 0.4	Extreme	6.4E-10	C
EJ: 1.0E-03	Wrong runway take-off	1.0E-03	ATC Training SOP	0.4 0.4 0.4	Medium	6.4E-08	D

Hazard No.10
Getting lost on airfield

This hazard origins from the lack of familiarity with the airport and the surrounding zone combined with bad visibility: all of this can be connected to missing, for example, radar on ground or lighting system in the airfield. The initial event was evaluated through the EJ method and its probability was multiplied by three possible sequences, reported in the following list:

1. Getting lost on airfield + Runway incursion.
   The barriers are ATC communication, training and EOP.

2. Getting lost on airfield + Runway incursion + Ground collision.
   The barriers are ATC communication, training and EOP.

3. Getting lost on airfield + Wrong runway take-off.
   The barriers are ATC communication, training and EOP.

It is important to underline that the ground collision incident sequence depends on runway incursion so the probability of the two sequences was multiplied one by the other.
The barriers considered are ATC communication, training and EOP because in this hazard the pilots feel "lost" in the airport.
The values choice for the barriers are:

- Air Traffic Control communication: $ATC = 0.4$;
- training: $Training = 0.4$;
- Emergency Operating Procedures: $EOP = 0.4$.

The expressions utilised to evaluate the probability are the following:

$$\begin{cases} P_{10a} = ATC \cdot Training \cdot EOP \cdot P_{Lost} \cdot P_{Runway} \\ P_{10b} = ATC \cdot Training \cdot EOP \cdot P_{Lost} \cdot [P_{Runway} \cdot P_{Collisoion}] \\ P_{10c} = ATC \cdot Training \cdot EOP \cdot P_{Lost} \cdot P_{Wrong} \end{cases} \tag{5.32}$$

The results obtained with the expressions are:

$$\begin{cases} P_{10a} = 6.4E-07 \\ P_{10b} = 6.4E-10 \\ P_{10c} = 6.4E-8 \end{cases} \tag{5.33}$$

Table 5.29: Hazard No.10 - Getting lost on airfield.

Hazard	Incident sequence description		Existing control				
No. 10	Consequences	Probab. without control		Probab. reduction	Severity	Probab.	Risk
Getting lost on airfield EJ : 1.0E-03	Runway incursion	1.0E-02	ATC Training EOP	0.4 0.4 0.4	Medium	6.4E-07	D
	Ground collision (aircraft, Infrastructures and vehicles)	1.0E-03	ATC Training EOP	0.4 0.4 0.4	High	6.4E-10	D
	Wrong runway take-off	1.0E-03	ATC Training EOP	0.4 0.4 0.4	Medium	6.4E-08	D

Hazard No.11
Missing performance

This hazard comes from the lack of SID or from the possession of wrong SID because a lot of SID exist and they require some types of aircraft performances. The use of wrong performance values can lead to collision with other aircraft or to loss of separation and at the possible CFIT.
The hazard value of probability and the possible consequences was evaluated through the EJ method; moreover, there are three possible sequences in order to evaluate three values of probability and to find which is the sequence with the higher risk.
The possible sequences are:

1. Missing performance + Mid air collision.
   The barriers are training and EOP.

2. Missing performance + Loss of separation (ground and flight).
   The barriers are training, EOP and TCAS.

3. Missing performance + Loss of separation (flight) + CFIT.
   The barriers are training, EOP, TCAS and EGPWS.

The barriers considered are the training, EOP, TCAS and EGPWS and their values are:

- training: $Training = 0.4$;
- Emergency Operating Procedures: $EOP = 0.4$;

- Terrain Control Avoidance System: $TCAS = 0.3$;
- Enhanced Ground Proximity Warning System: $EGPWS = 0.3$.

The expressions used to evaluate the values of probability are the following:

$$\begin{cases} P_{11a} = Training \cdot EOP \cdot P_{Performance} \cdot P_{Mid} \\ P_{11b} = Training \cdot EOP \cdot TCAS \cdot P_{Performance} \cdot P_{Loss} \\ P_{11c} = Training \cdot EOP \cdot TCAS \cdot P_{Performance} \cdot [P_{Loss} \cdot P_{CFIT}] \end{cases} \tag{5.34}$$

The results obtained with the expressions are:

$$\begin{cases} P_{11a} = 1.6E-07 \\ P_{11b} = 4.8E-08 \\ P_{11c} = 1.44E-11 \end{cases} \tag{5.35}$$

Table 5.30: Hazard No.11 - Missing performance.

Hazard	Incident sequence description		Existing control				
No. 11	Consequences	Probab. without control		Probab. reduction	Severity	Probab.	Risk
Missing performance EJ : 1.0E-03	Mid air collision	1.0E-03	Training EOP	0.4 0.4	High	1.6E-07	C
	Loss of separation (ground and flight)	1.0E-03	Training EOP TCAS	0.4 0.4 0.3	High	4.8E-08	D
	CFIT	1.0E-03	Training EOP TCAS EGPWS	0.4 0.4 0.3 0.3	Extreme	1.44E-11	C

Hazard No.12
Missing information in the case of emergency

In this hazard, the value of the probability of the initial event was initially calculated with the TESEO method but it was not the appropriate choice in this case. The calculation with the TESEO method is reported and the values of the coefficients (K) for the HU calculation are presented in tables 5.31a and 5.31b.

The expressions to calculate the HU in two cases are:

$$HU = K_1 \cdot K_{2_b} \cdot K_3 \cdot K_4 \cdot K_5 = 0.1 \cdot 10 \cdot 1 \cdot 3 \cdot 7 = 21 \tag{5.36}$$

$$HU = K_1 \cdot K_{2_b} \cdot K_3 \cdot K_4 \cdot K_5 = 0.1 \cdot 1 \cdot 1 \cdot 3 \cdot 7 = 2.1 \tag{5.37}$$

Missing information in the case of emergency is a different type of event with respect to the previous ones since it requires an immediate reaction from the operator and the resulting anxiety, which influences the pilot actions, is related to a serious emergency situation. TESEO, with the coefficients considered for this hazard, results in $HU > 1$; therefore a mitigation must be adopted in order to reduce the probability of this event to a value lower than 1. The second HU calculation for this hazard considers a longer reaction time (30s): the probability resulting in this case is still greater than 1, even if it is an order of magnitude lower than in the first calculation, therefore a mitigation must be applied.

Table 5.31: Missing information in the case of emergency

(a) Case 1

K_1	Not routine	0.1
K_2 (b)	3 (s)	10
K_3	Average knowledge and training	1
K_4	Situation of grave emergency	3
K_5	Discrete microclimate, poor interface with plant	7

(b) Case 2

K_1	Not routine	0.1
K_2 (b)	30 (s)	1
K_3	Average knowledge and training	1
K_4	Situation of grave emergency	3
K_5	Discrete microclimate, poor interface with plant	7

It is necessary to underline that the type of emergency considered in this hazard is unknown; it will be therefore necessary to specify or to distinguish between the different emergency types that can occur. Based on this distinction, a low or high value for the temporal response (see the value $HU = 21$) must be considered; it is also possible to consider an intermediate value for the response time but, in this case, a new table for the K_2 factor must be created for the calculation with TESEO.
In this hazard ATC presence and training of the operators lead to an extreme value for the severity; the probability of the initial event was calculated with TESEO while the incident sequence probability was evaluated

through EJ. There is a sequence composed by loss of control in flight and CFIT; in this sequence the calculation of the probability of loss of control in flight and CFIT are multiplied for the probability of initial event.
It was decided not to consider the increase of workload of the crew as a consequence but to connect it directly to the initial event because the workload depends on the emergency type.
To follow this concept, it is important to underline that TESEO is not the best method to calculate the probability of the initial event but it is necessary to use the EJ method that results the most appropriate method to define the hazard value of the probability and the incident sequences values.
The possible sequences are:

1. Missing information in the case of emergency + Loss of control in flight.
   The barriers are ATC, training and EOP.

2. Missing information in the case of emergency + Loss of control in flight + CFIT.
   The barriers are ATC, training, EOP and EGPWS.

The barriers considered are ATC communication, training, EOP and Enhanced Ground Proximity Warning System; their values are:

- Air Traffic Control communication: $ATC = 0.4$;
- Emergency Operating Procedures: $EOP = 0.4$;
- training: $Training = 0.4$;
- Enhanced Ground Proximity Warning System: 0.3.

The expressions used to evaluate the values of the probability are:

$$\begin{cases} P_{12a} = ATC \cdot EOP \cdot Training \cdot P_{Info} \cdot P_{Loss} \\ P_{12b} = ATC \cdot EOP \cdot Training \cdot EGPWS \cdot P_{Info} \cdot [P_{Loss} \cdot P_{CFIT}] \end{cases} \tag{5.38}$$

The results obtained with the expressions are:

$$\begin{cases} P_{12a} = 3.2E-06 \\ P_{12b} = 9.6E-10 \end{cases} \tag{5.39}$$

Table 5.32: Hazard No.12 - Missing information in the case of emergency.

Hazard	Incident sequence description		Existing control				
No. 12	Conseq.	Probab. without control		Probab. reduction	Severity	Probab.	Risk
Missing information in the case of emergency (increase of WL of crew) EJ: 5.0E-02	Loss of control in flight	1.0E-03	ATC Training EOP	0.4 0.4 0.4	High	3.2E-06	C
	CFIT	1.0E-03	ATC Training EOP EGPWS	0.4 0.4 0.4 0.3	Extreme	9.6E-10	C

Hazard No.13
No info/news on obstacles

This hazard, no info/news on obstacles, is connected to lack of SID or to have the wrong SID; moreover, this hazard is influenced by bad weather. It is important to underline that, in this case, there is little communication with ATC which cannot signal the presence of obstacles around the airport, like mountains or buildings. These can lead to a possible loss of separation (on ground) and CFIT: in this case CFIT does not depend on loss of separation.
The barriers considered for this hazard are ATC communication, EOP and EGPWS.
The possible sequences with their barrier are:

1. No info / news on obstacles + loss of separation (on ground).
   The barriers are ATC communication and EOP.

2. No info / news on obstacles + CFIT.
   The barriers are ATC communication, EOP and EGPWS.

The barriers values are:

- Air Traffic Control communication: $ATC = 0.4$;
- Emergency Operating Procedures: $EOP = 0.4$;
- Enhanced Ground Proximity Warning System: $EGPWS = 0.3$.

The expressions to evaluate the values of the probability are the following:

$$\begin{cases} P_{13a} = ATC \cdot EOP \cdot P_{No} \cdot P_{Loss} \\ P_{13b} = ATC \cdot EOP \cdot EGPWS \cdot P_{No} \cdot P_{CFIT} \end{cases} \tag{5.40}$$

The results obtained with the expressions are:

$$\begin{cases} P_{13a} = 4.8E-08 \\ P_{13b} = 4.8E-10 \end{cases} \tag{5.41}$$

Table 5.33: Hazard No.13 - No info/news on obstacles.

Hazard	Incident sequence description		Existing control				
No. 13	Consequences	Probab. without control		Probab. reduction	Severity	Probab.	Risk
No info/news on obstacles	Loss of separation (ground)	1.0E-03	ATC EOP	0.4 0.4	High	4.8E-08	D
EJ: 1.0E-03	CFIT	1.0E-05	ATC EOP EGPWS	0.4 0.4 0.3	Extreme	4.8E-10	C

Hazard No.14
Flying wrong departure

This hazard considers the aircraft take-off wrong departure so it is possible that the detachment from the ground is in another point with respect to the estimated one.
The possible consequences are mid air collision, loss of separation (on ground or in flight) and CFIT.
The following barriers are appropriate: ATC communication, EOP, TCAS for loss of separation and EGPWS for CFIT.
The sequences and the corresponding barriers are reported:

1. Flying wrong departure + Mid air collision.
   The barriers are ATC communication and EOP.

2. Flying wrong departure + Loss of separation (ground or flight).
   The barriers are ATC communication, EOP and TCAS.

3. Flying wrong departure + Loss of separation (ground or flight) + CFIT.
   The barriers are ATC communication, EOP, TCAS, EGPWS.

The barriers values are:

- Air Traffic Control communication: $ATC = 0.4$;
- Emergency Operating Procedures: $EOP = 0.4$;
- Terrain Control Avoidance System: $TCAS = 0.3$;
- Enhanced Ground Proximity Warning System: $EGPWS = 0.3$.

The expressions to evaluate the values of probability are the following:

$$\begin{cases} P_{14a} = ATC \cdot EOP \cdot P_{Wrong} \cdot P_{Mid} \\ P_{14b} = ATC \cdot EOP \cdot TCAS \cdot P_{Wrong} \cdot P_{Loss} \\ P_{14c} = ATC \cdot EOP \cdot TCAS \cdot EGPWS \cdot P_{Wrong} \cdot [P_{Loss} \cdot P_{CFIT}] \end{cases} \tag{5.42}$$

The results obtained with the expressions are:

$$\begin{cases} P_{14a} = 1.6E-08 \\ P_{14b} = 4.8E-09 \\ P_{14c} = 1.44E-12 \end{cases} \tag{5.43}$$

Table 5.34: Hazard No.14 - Flying wrong departure.

Hazard	Incident sequence description		Existing control				
No. 14	Consequences	Probab. without control		Probab. reduction	Severity	Probab.	Risk
Flying wrong departure EJ: 1E-04	Mid air collision	1E-03	ATC EOP	0.4 0.4	High	1.6E-08	D
	Loss of separation (ground and flight)	1E-03	ATC EOP TCAS	0.4 0.4 0.3	High	4.8E-09	D
	CFIT	1E-03	ATC EOP TCAS EGPWS	0.4 0.4 0.3 0.3	Extreme	1.44E-12	C

5.2 Application of THERP method

In this paragraph the use of the THERP method for the case study and the risk assessment are presented.
The generic hazards are described along with their possible consequences and the incident sequences. Afterwards the probabilities of each sequence are determined using the failure trees and the risk level associated is obtained through the severity levels and the risk matrix.
It is important to underline that the values of hazards probability are calculated from the THERP with the development of the THERP tree since in it is possible to distinguish the failures and the successes (see §5.2.2).

5.2.1 Hazards and consequences

In table 5.35 the two hazard considered for this case study and their possible incident sequences are presented. The only barrier used is the same for both hazards: training.
In §5.2.4 the hazards considered for the analysis with the THERP method are described and the calculation of the probability is presented; the consequences and their barriers for the risk mitigation are reported.

Table 5.35: Hazards, incident sequence description and existing control.

Hazard No.	Description	Incident sequence description	Existing control
1	Speed not adequate to take-off (over speed)	- Tail strike - Loss of control - Runway overrun	Training
2	Aborted take-off	- Runway excursion	Training

5.2.2 Development of THERP tree

The THERP tree developed is presented in figure 5.4: this is different from the theory because the first (*THRUST Calculation and reading*) is a three ways node and it represents the innovative approach while the other nodes (*SPEED and TAKE-OFF CONFIGURATION*) are binary, as in the classic method.
Referring to figure 5.4, the first node represents the *THRUST Calculation and reading*: the choice of this parameter depends on other factors evaluated in advance, as the aircraft weight or length and the condition of runway,

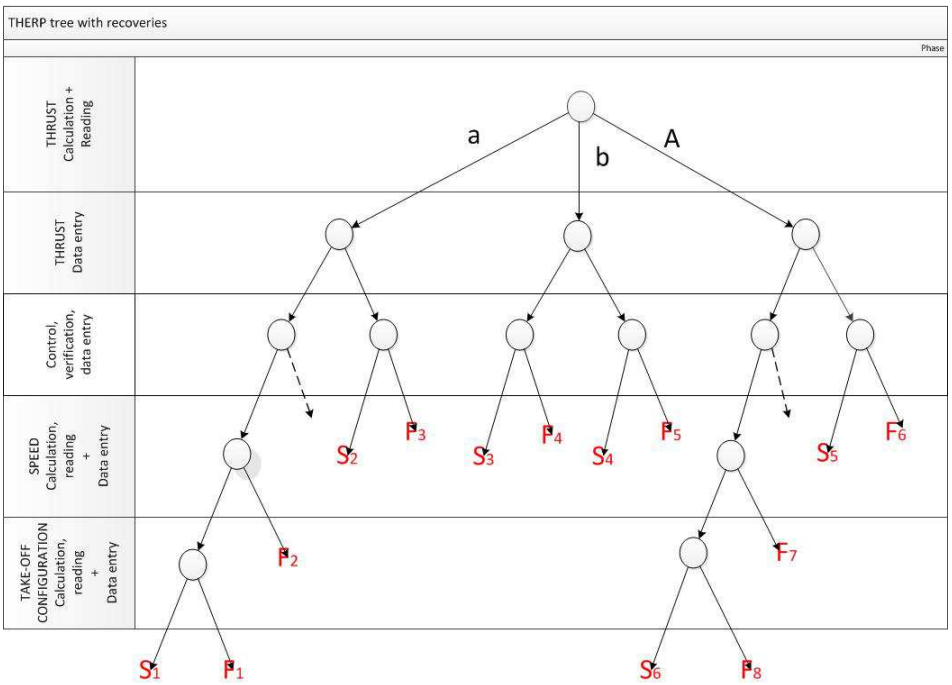


Figure 5.4: THERP tree.

outside temperature, pressure (QNH - Atmospheric pressure at Nautical Height), wind and present MEL. The only parameters that can be modified in order to obtain the optimal thrust are temperature and pressure. It is important to underline that the modification of this parameter from the pilots does not represent a violation because this behaviour is allowed. However it is important not to abuse of this possibility introducing a thrust value too different from the calculated one to avoid other possible problems during the flight. In figure 5.4 it is possible to distinguish three arms and they represent:

- *a* is the correct calculation of the value and the following correct insertion of the parameter;
- *b* is the wrong calculation of the value and the following insertion of wrong parameter;
- *A* is the voluntary wrong calculation of the value and the following correct insertion of parameter but with the voluntary wrong value.

When EFB gives the thrust values, the set of speeds and the optimal take-off configuration are automatically known.
The other nodes are binary so it is possible to insert only correct on wrong

values.

Another node, called *Control, verification, data entry*, must be included in the analysis because, after the calculation of thrust through EFB the value is inserted on a computer (FMS) and two possibilities are available: the pilots notice the error or the computer gives a warning about the value entered. This node represents a check point to help the pilot.

It is important to underline that it is possible to apply the recovery from the central line (letter *b*) to the right or to the left nodes of the *Speed calculation, reading and data entry* step: this is possible because the pilot or the on board system have the possibility to identify the error.

5.2.3 Probability tree calculation

As described above, in figure 5.4 it is possible to distinguish three directions and they represent three different actions:

- *a* is the correct calculation of the value and the following correct insertion of the parameter;
- *b* is the wrong calculation of the value and the following insertion of wrong parameter;
- *A* is the voluntary wrong calculation of the value and the following correct insertion of parameter but with the voluntary wrong value.

The speed and take-off configuration nodes include the reading and the insertion of the parameters; therefore, in figure 5.5 these nodes and the values associated to each side are represented.
The same probability value of reading and insertion are considered so the same value of success and failure is obtained; this value was used to calculate the final probability of the THERP tree. The expressions are the following:

$$F_s = 0.001 + (0.001 \cdot 0.999) = 0.002 \tag{5.44}$$

$$S_v = 0.999 \cdot 0.999 = 0.998 \tag{5.45}$$

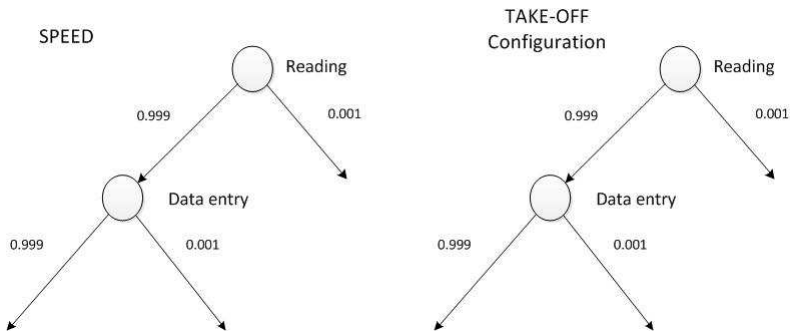


Figure 5.5: Speed and take-off configuration trees.

Success and Failure calculation

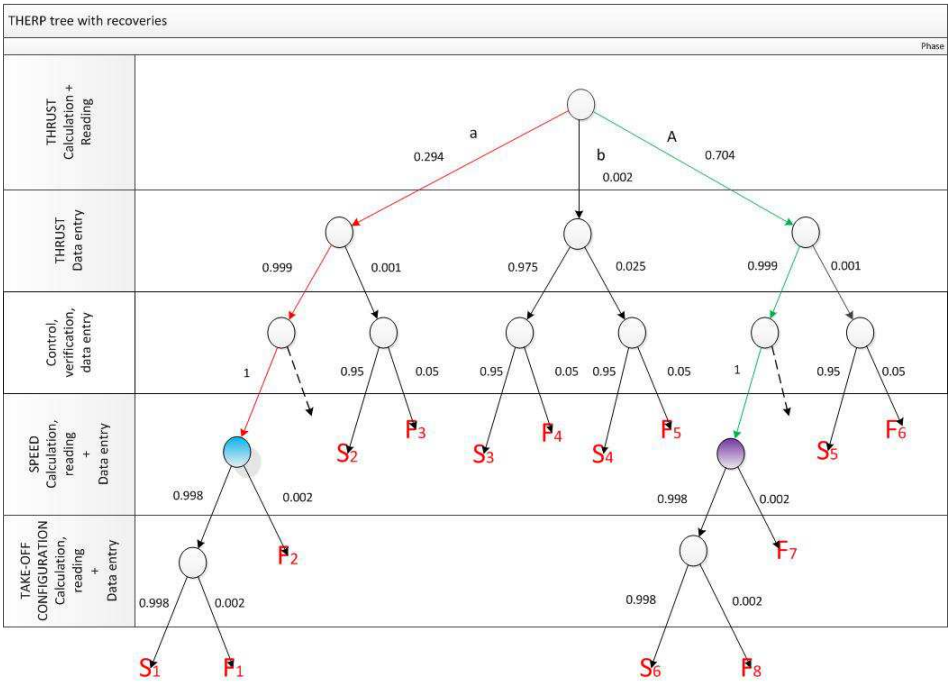


Figure 5.6: THERP tree with probabilities.

In figure 5.6 the tree, along with the values of the success and failure of each node, are reported.
The expressions of the different failures (F) are the following:

$$F_3 = 0.294 \cdot 0.001 \cdot 0.05 = 0.0000147 \tag{5.46}$$

$$F_4 = 0.002 \cdot 0.975 \cdot 0.05 = 0.0000975 \tag{5.47}$$

$$F_5 = 0.002 \cdot 0.025 \cdot 0.05 = 0.00000250 \tag{5.48}$$

$$F_6 = 0.704 \cdot 0.001 \cdot 0.05 = 0.0000352 \tag{5.49}$$

In order to apply the recovery it is necessary to consider two different cases; in this way, it is possible to choose the direction, left or right, of the recovery and in which check node the operator can correct the parameters inserted.
In the following paragraphs, the two cases are analysed separately and the numerical values obtained are reported along with the sequences considered.

Case One

In this case, the recovery is applied to the left sequence of the tree (the line *a* in red in figure 5.6) and in particular to the speed insertion node (the light blue node in figure 5.6). The value of the probability in this node is calculated as the sum of the success of the sequence on the line *a*, S_2, S_3 and S_4.

$$\begin{aligned} R_{left} &= S_{line_a} + S_2 + S_3 + S_4 = \\ &= (0.294 \cdot 0.999 \cdot 1) + (0.294 \cdot 0.001 \cdot 0.95) + \\ &+ (0.002 \cdot 0.975 \cdot 0.95) + (0.002 \cdot 0.025 \cdot 0.95) = 0.296 \end{aligned} \tag{5.50}$$

On the *A* side of the tree, the recovery is calculated as the sum of S_5 and the probability of the green sequence highlighted in figure 5.6. The resulting value is reported in the speed insertion node, the violet node in figure 5.6).

$$S_5 = (0.704 \cdot 0.001 \cdot 0.95) = 0.000669 \tag{5.51}$$

$$S_{recovery_{left}} = S_5 + (0.704 \cdot 0.999 \cdot 1) = 0.704 \tag{5.52}$$

The expressions of the failures (F_2, F_1, F_7 e F_8) and the successes (S_1 and S_2) are reported:

$$F_1 = R_{left} \cdot 0.998 \cdot 0.002 = 0.000591 \tag{5.53}$$

$$F_2 = R_{left} \cdot 0.002 = 0.000592 \tag{5.54}$$

$$S_1 = R_{left} \cdot 0.998 \cdot 0.998 = 0.295 \tag{5.55}$$

$$F_7 = S_{reovery_{left}} \cdot 0.002 = 0.00141 \tag{5.56}$$

$$F_8 = S_{recovery_{left}} \cdot 0.998 \cdot 0.002 = 0.00141 \tag{5.57}$$

$$S_6 = S_{recovery_{left}} \cdot 0.998 \cdot 0.998 = 0.701 \tag{5.58}$$

The total probability of success and failure of the procedure is obtained by adding the final probability of the different sequences that end with

success and failure.
The following expressions represent the value of total probability of success and failure and they are:

$$S = S_1 + S_6 = 0.996 \tag{5.59}$$

$$F = F_1 + F_2 + F_3 + F_4 + F_5 + F_6 + F_7 + F_8 = 0.00415 \tag{5.60}$$

The addition of success S and failure F must be equal one and in this case the result is:

$$Somma = S + F = 0.996 + 0.00415 = 1.0000 \tag{5.61}$$

Case Two

In this case, the recovery is always applied to the speed insertion node but to the right sequence of the tree (highlighted in green in figure 5.6). The value of the probability in this node (the violet node in figure 5.6) is calculated as the sum of the success of the sequence on the line A, S_3, S_4 and S_5.

$$\begin{aligned} R_{right} &= S_{line_A} + S_5 + S_3 + S_4 = \\ &= (0.704 \cdot 0.001 \cdot 0.95) + (0.704 \cdot 0.999 \cdot 1) + \\ &+ (0.002 \cdot 0.025 \cdot 0.95) + (0.002 \cdot 0.975 \cdot 0.95) = 0.706 \end{aligned} \tag{5.62}$$

On the a side of the tree, the recovery is instead calculated as the sum of S_2 and the probability of the red sequence highlighted in figure 5.6. The resulting value is reported in the speed insertion node coloured in light blue in figure 5.6.

$$S_2 = (0.294 \cdot 0.001 \cdot 0.95) = 0.000279 \tag{5.63}$$

$$S_{recovery_{left}} = S_2 + (0.294 \cdot 0.999 \cdot 1) = 0.294 \tag{5.64}$$

These are the expressions of the failures (F_2, F_1, F_7 e F_8) and the successes (S_1 and S_2):

$$F_1 = S_{recovery_{left}} \cdot 0.998 \cdot 0.002 = 0.000588 \tag{5.65}$$

$$F_2 = S_{recovery_{left}} \cdot 0.002 = 0.000588 \tag{5.66}$$

$$S_1 = S_{recovery_{left}} \cdot 0.998 \cdot 0.998 = 0.293 \tag{5.67}$$

$$F_7 = R_{right} \cdot 0.002 = 0.00141 \tag{5.68}$$

$$F_8 = R_{right} \cdot 0.998 \cdot 0.002 = 0.00141 \tag{5.69}$$

$$S_6 = R_{right} \cdot 0.998 \cdot 0.998 = 0.703 \tag{5.70}$$

The total probability of success and failure of the procedure is obtained by adding the final probability of the different sequences that end with success and failure.
The following expressions represent the value of total probability of success and failure and they are:

$$S = S_1 + S_6 = 0.996 \tag{5.71}$$

$$F = F_1 + F_2 + F_3 + F_4 + F_5 + F_6 + F_7 + F_8 = 0.00415 \tag{5.72}$$

The addition of the probability of success S and failure F must be equal one:

$$Somma = S + F = 0.996 + 0.00415 = 1.0000 \tag{5.73}$$

Choice probability value to insert in THERP tree

The probability of the sides of every node was selected analysing the chapter 20 of the THERP manual of Swain and Guttman, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant applications* [20].
This manual was developed for nuclear field but it was possible to find a correspondence with the case in exam.
In tables 5.36, 5.37 and 5.38 are respectively reported the insertion, the reading and the check of the parameters; moreover, in every table the cases selected are highlighted.

Table 5.36: Lecture. THERP, chapter 20, table 20-9. [20]

Table 20-9:
Estimated probabilities of errors in selecting unannunciated displays for quantitative or qualitative readings

Item	Selection of wrong display	HEP	EF
(1)	When it is dissimilar to adjacent displays	Negligible	
(2)	From similar-appearing displays when they are on a panel with clearly drawn mimic lines that include the displays	0.0005	10
(3)	From similar-appearing displays that are part of well-delineated functional groups on a panel	0.001	3
(4)	From an array of similar-appearing displays identified by labels only	0.003	3

Table 5.37: Data entry. THERP, chapter 20, table 20-10. [20]

Table 20-10:
Estimated HEPs for errors of commission in reading and recording quantitative information from unannunciated displays

Item	Display or Task	HEP	EF
(1)	Analog meter	0.003	3
(2)	Digital readout (≤ 4 digits)	0.001	3
(3)	Chart recorder	0.006	3
(4)	Printing recorder with large number of parameters	0.05	5
(5)	Graphs	0.01	3
(6)	Values from indicator lamps that are used as quantitative display	0.001	3
(7)	Recognize that an instrument being red is jammed, if there are no indicators to alert the user	0.1	5
	Recording task: number of digits or letters to be recorded:		
(8)	≤ 3	Negligible	-
(9)	> 3	0.001 (per symbol)	3
(10)	Simple arithmetic calculations with or without calculators	0.01	3
(11)	Detect out-of-range arithmetic calculations	0.05	5

Table 5.38: Check parameter. THERP, chapter 20, table 20-22. [20]

Table 20-22:
Estimated probabilities that a checker will fail to detect errors made by others

Item	Checking Operation	HEP	EF
(1)	Checking routine tasks, checker using written materials (includes over-the-shoulder inspections, verifying position of locally operated valves, switches, circuit breakers, connectors, etc., and checking written lists, tags, or procedures for accuracy)	0.1	5
(2)	Same as above, but without written materials	0.2	5
(3)	Special short-term, one-of-kind checking with alerting factors	0.05	5
(4)	Checking that involves active participation, such as special measurements	0.01	5
	Given that the position of a locally operated valve is checked (items 1 above), noticing that it is not completely opened or closed:	0.5	5
(5)	- Position indicator only	0.1	5
(6)	- Position indicator and a rising stem	0.5	5
(7)	- Neither a position indicator nor a rising team	0.9	5
(8)	Checking by reader/checker of the task performer in to-man team, or checking by a second checker, routine task (no credit for more than two checkers)	0.5	5
(9)	Checking the status of equipment if that status affects one's safety when performing his tasks	0.001	5
(10)	An operator checks change or restoration tasks performed by a maintainer	Above HEPs ÷ 2	5

For the central sequence of the tree, a different table was considered (table 5.39) for the data entry node because the required recovery from the central sequence can be applied.
In addition, table 5.40 could be considered because it includes multiplicative factors based on stress level and experience. For the case in exam, the take-off briefing, the stress level factor is one.

Table 5.39: THERP, chapter 20, table 20-2. [20]

Table 20-2:
Initial-screening model of estimated HEPs and EFs for rule-based actions by control room personnel after diagnosis of an abnormal event

Item	Potential Errors	HEP	EF
	Failure to perform rule-based actions correctly when written procedures are available and used:		
(1)	Errors per critical step without recovery factors	0.05	10
(2)	Errors per critical step with recovery factors	0.025	10

Table 5.40: THERP, chapter 20, table 20-16. [20]

Table 20-16:
Modification of estimated HEPs for effects of stress and experience levels

	Stress Level	Modifiers for Nominal HEPs Skilled	Novice
Item		**(a)**	**(b)**
(1)	Very low (Very low task load)	x2	x2
	Optimum (Optimum task load):		
(2)	- Step-by-step	x1	x1
(3)	- Dynamic	x1	x2
	Moderately high (Heavy task load):		
(4)	- Step-by-step	x2	x4
(5)	- Dynamic	x5	x10
	Extremely high (Threat stress):		
(6)	- Step-by-step	x5	x10
(7)	- Dynamic diagnosis	0.25 (EF=5)	0.50 (EF=5)
		These are the actual HEPs to use with dynamic tasks or diagnosis – they are NOT modifiers.	

5.2.4 Hazards and risk matrix

Hazard No.1
Speed not adequate to take-off

This hazard is characterized by an insufficient speed to take-off and the pilot acts on the aircraft thrust in order to increase the speed and execute the take-off. For this hazard the aircraft is after the point of the decision speed and it is not possible to abort the take-off; the possible consequences are tail strike, loss of control and runway overrun while the barriers considered for this hazard are training and Standard Operating Procedures (SOP).
The possible sequences and their barriers are:

1. Speed not adequate to take-off + Tail strike.
   The barriers are training and SOP.

2. Speed not adequate to take-off + Loss of control.
   The barriers are training and SOP.

3. Speed not adequate to take-off + Runway overrun.
   The barriers considered are training and SOP.

The values considered for the barriers are:

- training: $Training = 0.4$;
- Standard Operating Procedures: $SOP = 0.4$.

The expressions used to estimate the values of the probability are:

$$\begin{cases} P_{1a} = Taining \cdot SOP \cdot P_{Speed} \cdot P_{Tail} \\ P_{1b} = Taining \cdot SOP \cdot P_{Speed} \cdot P_{Loss} \\ P_{1c} = Taining \cdot SOP \cdot P_{Speed} \cdot P_{Runway} \end{cases} \tag{5.74}$$

The results obtained with the expressions are:

$$\begin{cases} P_{1a} = 6.64E-05 \\ P_{1b} = 6.64E-07 \\ P_{1c} = 3.32E-06 \end{cases} \tag{5.75}$$

Using the probability values calculated and the severity levels it was possible to individuate the corresponding risk in the risk matrix.

Table 5.41: Hazard No.1 - Speed not adequate to take-off.

Hazard	Incident sequence description		Existing control				
No. 1	Consequences	Probab. without control		Probab. reduction	Severity	Probab.	Risk
Speed not adequate to take-off THERP: 4.15E-03	Tail strike	1E-01	Training SOP	0.4 0.4	Medium	6.64E-05	C
	Loss of control	1E-03	Training SOP	0.4 0.4	High	6.64E-07	C
	Runway overrun	5E-03	Training SOP	0.4 0.4	Medium	3.32E-06	D

Hazard No.2
Aborted take-off

This hazard, reported in table 5.42, is characterised by a speed on the runway lower than the decision speed before the aircraft reaches the

decision speed point; in this case the pilot can decide to stop the aircraft and to abort the take-off. The possible consequence is runway excursion and the barriers are training and Standard Operating Procedures (SOP). The sequence and their barriers are:

1. Aborted take-off + Runway excursion.
   The barriers are training and SOP.

The values considered for the barriers are:

- training: $Training = 0.4$;
- Standard Operating Procedures: $SOP = 0.4$.

The expression used to estimate the value of probability is the following:

$$P_2 = Taining \cdot SOP \cdot P_{Aborted} \cdot P_{Runway} \tag{5.76}$$

The result obtained is:

$$P_2 = 6.64E - 05 \tag{5.77}$$

Through the value of probability and the severity level considered it was possible to identify in which cell of the risk matrix the risk is.

Table 5.42: Hazard No.2 - Aborted take-off.

Hazard	Incident sequence description		Existing Control				
No. 2	Consequences	Probab. without control		Probab. Reduction	Severity	Probab.	Risk
Aborted take-off THERP: 4.15E-03	Runway excursion	5E-03	Training SOP	0.4 0.4	High	3.32E-06	C

5.3 TESEO and THERP results

In tables 5.43, 5.44 and 5.45, the risk assessment for the take-off briefing is presented. Both hazards analysed with TESEO and THERP along with their consequences are reported; moreover, the corresponding barriers and the value of probability for every incident sequence are included. These tables were completed using as a reference the based table (figure 3.2) of

the RAMCOP methodology; all the steps described in §3.2 are included in these tables. The value of probability presented refers to the sequence with the higher probability and the most important parameter is the level of risk. If two or more incident sequences of the same hazard had the same risk level, the sequence with the higher value of probability was considered. Moreover, in tables 5.43, 5.44 and 5.45 the severity level associated and the risk level obtained from the risk matrix are reported.
Further mitigations, aiming to reduce the probability values of the sequences that have not a risk level in the acceptable area (the green cells in the risk matrix), are also presented. These mitigations are the presence of kit paper (maps) and the necessity of further specific training. For both mitigations the value considered is 0.1.
Since many of the hazards require the additional training mitigation in order to reduce the risk level, a solution could be to give to the pilots additional training on the use of EFB in advance to let them familiarize with the instrument before its actual use.
After the application of the additional mitigation all probabilities are reduced and none of the risk levels are in the high or extreme zone in the risk matrix.
For the hazards evaluated with the TESEO method the risks indicated with *C* are related to *extreme* level of severity: in these cases a further reduction of the probability could be necessary through the application of other mitigations.
Hazard No.10 is the only one that does not require any further mitigation since its risk level is within the acceptable area (level *D* in the risk matrix).

Table 5.43: TESEO risk assessment for take-off briefing. 1 of 2

Hazard		Incident sequence description	Existing Control	Outcome (Pre-Mitigation)			Additional mitigation required	Outcome (Post-Mitigation)			Actions and owners	Monitoring and Review requirements
No.	Description			Severity	Likelihood	Risk		Severity	Likelihood	Risk		
1	Software initialisation not completed	- Flight cancellation or delay - Loss of separation - CFIT	MQ TCAS EGPWS	Low	3.0E-04	C	Paper maps	Low	3.0E-05	D		
2	Maps not available	- Flight cancellation or delay - Loss of separation - CFIT	MQ TCAS EGPWS	High	1.2E-07	C	Paper maps	High	1.2E-08	D		
3	Improper selection of portrait	- Flight cancellation or delay - Loss of separation - CFIT	Training SOP - EOP TCAS EGPWS	Low	4.8E-04	C	Paper maps	Low	4.8E-05	D		
4	Improper storage of PC	- Damage to cables/PC + Fire/smoke in the cabin - Damage to cables/PC + Flight cancellation or delay	MQ SOP	High	4.8E-07	C	Paper maps Training	High	4.8E-09	D		
5	Pilots unable to locate maps	- Loss of separation - CFIT	Training EOP TCAS EGPWS	High	1.4E-06	C	Paper maps Training	High	1.4E-08	D		
6	Loss of SA	- Flight diversion or delay - Loss of separation - CFIT	Training SOP - EOP TCAS EGPWS	High	4.8E-06	C	Paper maps Training	High	4.8E-08	D		
7	No charts on show	- Flight diversion or delay - Loss of separation - CFIT	MQ TCAS EGPWS	Extreme	3.6E-12	C	Paper maps	Extreme	3.6E-13	C		

Table 5.44: TESEO risk assessment for take-off briefing. 2 of 2

Hazard		Incident sequence description	Existing Control	Outcome (Pre-Mitigation)			Additional mitigation required	Outcome (Post-Mitigation)			Actions and owners	Monitoring and Review requirements
No.	Description			Severity	Likelihood	Risk		Severity	Likelihood	Risk		
8	Flying with wrong maps or without maps	- Flight diversion or delay - Loss of separation - CFIT	Training SOP - EOP TCAS EGPWS	High	1.4E-06	C	Paper maps Training	High	1.4E-08	D		
9	No coordinates for Xcheck with FMS (impossible to see taxiway)	- Runway incursion - Ground collision (aircrafts, vehicles and infrastructures) - Wrong runway take-off	ATC SOP Training	Extreme	6.4E-10	C	Training	Extreme	6.4E-11	C		
10	Getting lost on airfield	- Runway incursion - Ground collision (aircrafts, vehicles and infrastructures) - Wrong runway take-off	ATC EOP Training	Medium	6.4E-07	D						
11	Missing performance	- Mid air collision - Loss of separation (ground) - CFIT	EOP Training EGPWS	High	1.6E-07	C	Training	High	1.6E-08	D		
12	Missing information in the case of emergency (increase of WL of crew)	- Loss of control in flight - CFIT	ATC EOP Training EGPWS	High	3.2E-06	C	Paper maps Training	High	3.2E-08	D		
13	No info/news on obstacles	- Loss of separation (ground) - CFIT	ATC EOP EGPWS	Extreme	4.8E-10	C	Training	Extreme	4.8E-11	C		
14	Flying wrong departure	- Mid air collision - Loss of separation (ground and flight) - CFIT	ATC EOP TCAS EGPWS	Extreme	1.4E-12	C	Paper maps Training	Extreme	1.4E-14	C		

Table 5.45: THERP risk assessment for take-off briefing.

Hazard		Incident sequence description	Existing Control	Outcome (Pre-Mitigation)			Additional mitigation required	Outcome (Post-Mitigation)			Actions and owners	Monitoring and Review requirements
No.	Description			Severity	Likelihood	Risk		Severity	Likelihood	Risk		
1	Speed not adequate to take-off	- Tail strike - Loss of control - Runway overrun	Training SOP	Medium	6.64E-05	C	Training	Medium	6.64E-06	C		
2	Aborted take-off	- Runway excursion	Training SOP	High	3.32E-06	C	Training	High	3.32E-07	C		

5.4 Comparison with ICAO risk matrix

In this paragraph ICAO risk matrix is presented in order to compare the risk assessment performed with the modified risk matrix used in this thesis with ICAO risk levels.
ICAO risk matrix is represented in figure 5.7 while the risk levels and the mitigations are presented in figure 5.8.

	Severity Level				
Probability Level	S5 Catastrophic	S4 Dangerous	S3 Major	S2 Minor	S1 Negligeable
P5 Frequent P > 1.0E-04	A	A	A	C	E
P4 Reasonably probable 2.0E-05 < P ≤ 1.0E-04	A	A	A	C	E
P3 Remote 2.0E-06 < P ≤ 2.0E-05	A	A	C	E	E
P2 Extremely remote 2.0E-08 < P ≤ 2.0E-06	A	C	E	E	E
P1 Extremely improbable P ≤ 2.0E-08	C	E	E	E	E

Figure 5.7: ICAO risk matrix [1].

Risk Level	Risk	Risk mitigation
A	Estreme	Immediate mitigation required
C	Acceptable with mitigation	Long term improvement required
E	Negligible	Collect data

Figure 5.8: ICAO Risk level and mitigation [1].

In table 5.46 there is a comparison between the severity levels used by ICAO and for this thesis. In ICAO severity classification the low and minor levels considered for this work are joined in one level.

Table 5.46: Comparison between ICAO severity level and severity level by the case study.

Severity level of ICAO risk matrix	Severity level for the case study
Catastrophic	Extreme
Dangerous	High
Major	Medium
Minor	Low
	Minor
Negligible	None

In order to compare the results obtained between the TESEO and the THERP methods and ICAO risk matrix, all the risk levels were re-evaluated entering ICAO risk matrix with the probabilities calculated and the severity estimated: this risk assessment is reported in tables 5.47, 5.48 and 5.49. As described above only the sequences with the higher risk for each hazards are included in this table. It is important to notice that, for some of the hazards, the sequence with the higher risk level is not the same as in TESEO and THERP risk assessment. Moreover, prior to the additional mitigations application some sequences result in the unacceptable zone of the risk matrix while after the mitigations they are in the yellow zone and further mitigations are still necessary.

Table 5.47: TESEO risk assessment with ICAO risk matrix. 1 of 2

Hazard		Incident sequence description	Existing Control	Outcome (Pre-Mitigation)			Additional mitigation required	Outcome (Post-Mitigation)			Actions and owners	Monitoring and Review requirements
No.	Description			Severity	Likelihood	Risk		Severity	Likelihood	Risk		
1	Software initialisation not completed	- Flight cancellation or delay - Loss of separation - CFIT	MQ TCAS EGPWS	Minor	3.0E-04	C	Paper maps	Minor	3.0E-05	C		
2	Maps not available	- Flight cancellation or delay - Loss of separation - CFIT	MQ TCAS EGPWS	Minor	2.0E-04	C	Paper maps	Minor	2.0E-05	E		
3	Improper selection of portrait	- Flight cancellation or delay - Loss of separation - CFIT	Training SOP - EOP TCAS EGPWS	Dangerous	2.9E-06	A	Paper maps	Dangerous	2.9E-07	C		
4	Improper storage of PC	- Damage to cables/PC + Fire/smoke in the cabin - Damage to cables/PC + Flight cancellation or delay	MQ SOP	Dangerous	4.8E-07	C	Paper maps Training	Dangerous	4.8E-09	E		
5	Pilots unable to locate maps	- Loss of separation - CFIT	Training EOP TCAS EGPWS	Dangerous	1.4E-06	C	Paper maps Training	Dangerous	1.4E-08	E		
6	Loss of SA	- Flight diversion or delay - Loss of separation - CFIT	Training SOP - EOP TCAS EGPWS	Dangerous	4.8E-06	A	Paper maps Training	Dangerous	4.8E-08	C		
7	No charts on show	- Flight diversion or delay - Loss of separation - CFIT	MQ TCAS EGPWS	Minor	2.0E-04	C	Paper maps	Minor	2.0E-05	E		

Table 5.48: TESEO risk assessment with ICAO risk matrix. 2 of 2

Hazard		Incident sequence description	Existing Control	Outcome (Pre-Mitigation)			Additional mitigation required	Outcome (Post-Mitigation)			Actions and owners	Monitoring and Review requirements
No.	Description			Severity	Likelihood	Risk		Severity	Likelihood	Risk		
8	Flying with wrong maps or without maps	- Flight diversion or delay - Loss of separation - CFIT	Training SOP - EOP TCAS EGPWS	Minor	2.4E-04	C	Paper maps Training	Minor	2.4E-06	E		
9	No coordinates for Xcheck with FMS (impossible to see taxiway)	- Runway incursion - Ground collision (aircrafts, vehicles and infrastructures) - Wrong runway take-off	ATC SOP Training	Catastrophic	6.4E-10	C	Training	Catastrophic	6.4E-11	C		
10	Getting lost on airfield	- Runway incursion - Ground collision (aircrafts, vehicles and infrastructures) - Wrong runway take-off	ATC EOP Training	Major	6.4E-07	E						
11	Missing performance	- Mid air collision - Loss of separation (ground) - CFIT	EOP Training EGPWS	Dangerous	1.6E-07	C	Training	Dangerous	1.6E-08	E		
12	Missing information in the case of emergency (increase of WL of crew)	- Loss of control in flight - CFIT	ATC EOP Training EGPWS	Dangerous	3.2E-06	A	Paper maps Training	Dangerous	3.2E-08	C		
13	No info/news on obstacles	- Loss of separation (ground) - CFIT	ATC EOP EGPWS	Dangerous	4.8E-10	C	Training	Dangerous	4.8E-11	E		
14	Flying wrong departure	- Mid air collision - Loss of separation (ground and flight) - CFIT	ATC EOP TCAS EGPWS	Catastrophic	1.4E-12	C	Paper maps Training	Catastrophic	1.4E-14	C		

Table 5.49: THERP risk assessment with ICAO risk matrix.

Hazard		Incident sequence description	Existing Control	Outcome (Pre-Mitigation)			Additional mitigation required	Outcome (Post-Mitigation)			Actions and owners	Monitoring and Review requirements
No.	Description			Severity	Likelihood	Risk		Severity	Likelihood	Risk		
1	Speed not adequate to take-off	- Tail strike - Loss of control - Runway overrun	Training SOP	Major	6.64E-05	A	Training	Major	6.64E-06	C		
2	Aborted take-off	- Runway excursion	Training SOP	Dangerous	3.32E-06	A	Training	Dangerous	3.32E-07	C		

Chapter 6

Conclusion

The methodology applied in this thesis for qualitative and quantitative risk analyses represents a useful instrument for the implementation of Safety Management System because it can be adapted to the particular case in exam; this methodology is the Risk Assessment Methodology for Company Operational Processes (RAMCOP) applied to the prospective analysis in order to analyse the Management of Change due to the introduction of a new instrument, the Electronic Flight Bag, in the take-off briefing procedure. The activities related to the use of EFB are identified considering human factors; starting from the activities required from the procedure, hazards and consequences were identified and the probabilities of every possible incident sequence were calculated using Tecnica Empirica Stima Errori Operatori (TESEO) and Technique for Human Error Rate Prediction (THERP). When these methods were not applicable the Expert Judgement (EJ) method was used for probability estimation. The risk assessment was performed by means of a risk matrix modified with respect to the ICAO risk matrix: probability ranges and severity levels were adapted in order to be applicable to the case study. It is important to notice that the case study is based on human factors.

The TESEO method was used as described in literature while the THERP method developed for this work represents an innovative approach because it does not use only binary nodes but it includes a three ways node in the first step; this approach could be considered in future studies and compared to the classical binary approach. Moreover, a different application of the recovery with respect to the binary approach is implemented.
The Expert Judgement method is particularly exposed to fluctuations and uncertainties when it comes to Human Factors. To improve the objective-

ness of the results, the analyst should use one of the methods described in literature for the evaluation of probabilities.

Starting from the results presented in §5, it is possible to notice that, after the final mitigations, the risk levels are within the acceptable zone and they comply with the requirements of international regulations. However, analysing the results, in terms of risk levels, using the ICAO risk matrix it can be noticed that further additional barriers are needed in order to reduce the risk to acceptable areas.
The EFB considered in this thesis belongs to the second class, as the one used by Air Dolomiti; the results obtained in this thesis are in agreement with the company expectations. It can be concluded that EFB is an useful instrument during the preparation of a flight and the risk levels and the probability values are acceptable.

In the future the risk assessment of the use of EFB can be expanded to all the phases of the flight in order to verify if it can be useful in every phase and to define when its use is critical. Air Dolomiti uses EFB classified as second category that are separated from the avionic system but it was demonstrated that pilots can benefit from the use of EFB during take-off briefing; moreover it occupies less space with respect to maps and paper on board. If the company will decide to install the third category EFB, which is integrated with the avionic system, all the studies of probabilities and analyses of risk developed in this thesis can be extended to other phases of the flight in order to verify that the risks are within an acceptable area of the risk matrix or if other barriers are needed.

The implementation of this work in a dedicated software can speed up future calculation since the analyst would have to modify only the parameters in order to obtain the results. A first implementation of TESEO was performed using SQL, Microsoft Visual Studio and SDS Plus that is a Safety Database System (see §A.1.2 for further information).

Appendix A

Methods used in case study analysed

In this thesis the attention is focused on prospective analyses for the evaluation of human factors effects on the risk assessment. Moreover, this analysis does not consider the entire aircraft system but only the take-off briefing and its execution.
The methods used for the case study are TESEO and THERP and they are described in the following paragraphs. It was decided to use this methods because they belong to the first generation and they do not need an empirical validation. Moreover, among the first generation methods this two are the most suitable for the Human Reliability Analysis (HRA) including the errors recovery possibility.
Furthermore, the implementation of the TESEO method is presented.

A.1 TESEO

A.1.1 Description

TESEO, *Tecnica Empirica Stima Errori Operatori*, is a method used for the HRA and it was developed in 1980 by Bello and Colombari [16]. This method is very simple to use but it can be applied to limited fields and applications.
The Human Reliability (HR) calculates the probability that an operator fulfils successfully the action the system requested. HR is calculated as:

$$HR = 1 - HU \tag{A.1}$$

where HU stands for Human Unreliability.
It is important to say that, in HU and HR estimations, only successes are

considered, while errors are neglected. One of the operator characteristics is the possibility to correct the errors with a recovery. An unsuccessfully result occurs only when there is an uncorrected error.
Other two elements are considered in this method: Human Error (HE) and Probability of Recovery (PR). HE is the probability that the operator makes mistakes, while PR is the probability to correct the mistake. HE and PR are connected to HU by the following equation:

$$HU = HE(1 - PR) \tag{A.2}$$

To define the TESEO method, many different types of data are considered; they can be divided into four categories:

1. data from experience of operation in real plants;
2. data from plant simulator;
3. data from laboratory studies;
4. data collected by interviewing "experts".

The first type is the best one, even if these data are very difficult to find; the second and the third types are more easy to manage even if these data must be corrected with some coefficients; the last type requires some expert analysts and every single data is analysed by the experts.
These different types of data are used to built a model, TESEO, and to evaluate the probability of failure or success of the particular task performed by the operator. Even when the data described above are available, it is difficult to estimate HE and PR needed to calculate HU. Using the hypothesis that HE and PR can be represented as a function of the operator skills, the type of operation and the time available for the execution, a set of parameters can be defined:

- K_1, the type of task to be executed;
- K_2, the time available to the operator to complete the task;
- K_3, the operator's level of experience/characteristics;
- K_4, the operator's state of mind;
- K_5, the environmental and ergonomic conditions prevalent.

The calculation of HU presented in equation A.2 becomes a multiplicative function of these five parameters:

$$HU = K_1 \cdot K_2 \cdot K_3 \cdot K_4 \cdot K_5 \tag{A.3}$$

Table A.1: Activity's typological factor [16].

Type of activity	K_1
Simple, routine	0.001
Requiring attention, routine	0.01
Not routine	0.1

Table A.2: Temporary stress factor [16].

(a) Routine activities

Time available (s)	K_2 (a)
2	10
10	1
20	0.5

(b) Non-routine activities

Time available (s)	K_2 (b)
3	10
30	1
45	0.3
60	0.1

Table A.3: Operator's typological factor [16].

Operator's qualities	K_3
Carefully selected, expert, well trained	0.5
Average knowledge and training	1
Little knowledge, poorly trained	3

Table A.4: Activity's anxiety factor [16].

State of anxiety	K_4
Situation of grave emergency	3
Situation of potential emergency	2
Normal situation	1

Table A.5: Activity's ergonomic factor [16].

Environmental ergonomic factor	K_5
Excellent microclimate, excellent interface with plant	0.7
Good microclimate, good interface with plant	1
Discrete microclimate, discrete interface with plant	3
Discrete microclimate, poor interface with plant	7
Worst microclimate, poor interface with plant	10

A.1.2 Implementation

The implementation of TESEO was included in the existing software SDS Plus belonging to Kite Solution. SDS Plus is a web application which extends the concept of a Safety Database System to support the activities for the Safety Management System. This tool has the objective to be an adequate and simple support system, not only in the gathering, but also in the analysis of data relative to events regarding the security of the operations. SDS Plus is developed to favour a process of continuous increase of the understanding level of potentially dangerous situations and to constantly improve the technical, organizational and economic operation conditions.

With the purpose of integration and standardisation of the levels of security in the European and world scenario, SDS Plus adopts the ADREP (Accident/Incident Data Reporting) which is an instrument of management and classification of the data proposed by ICAO recognised at an international level.

The TESEO method, reported in literature (§A.1.1), was implemented in SDS Plus using SQL Server database as a source for the required data. The first step is the implementation of the coefficient tables of TESEO introducing the values and the definitions of the parameters. These tables, in SQL, are identified by a code used to a uniquely identify the name and

the corresponding factor; this code is also used to connect the parameters to Microsoft Visual Studio where the user can modify them if necessary. It is important to underline that Microsoft Visual Studio supports different programming languages such as C# and ASP.NET used for the implementation of TESEO. In order to correctly implemented the method, the user should have a basic knowledge of these languages.

In the following some figures of the TESEO application are presented. In figure A.1 the implementation of K_2 table in SDS Plus is presented. The TESEO method considers different values for this parameter based on the option selected for the K_1 coefficient; this option is presented with the R, routine activity, and the N, non-routine activity, option in the last column of the selection window. In figure A.2 the selection of the K_5 coefficient is reported; the other coefficients of the method are implemented in the same way. Figure A.3 shows the result of the HU calculation as presented from SDS Plus.

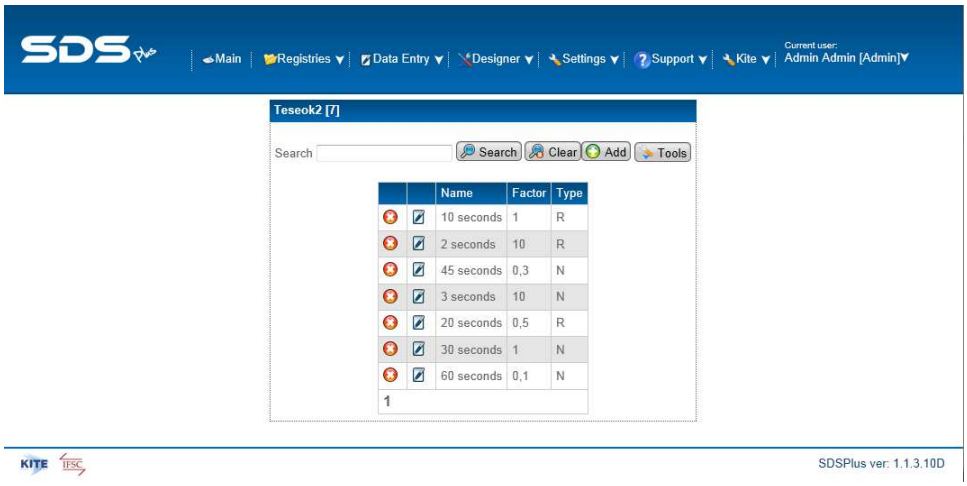


Figure A.1: Rappresentation of K_2 table in SDS Plus.

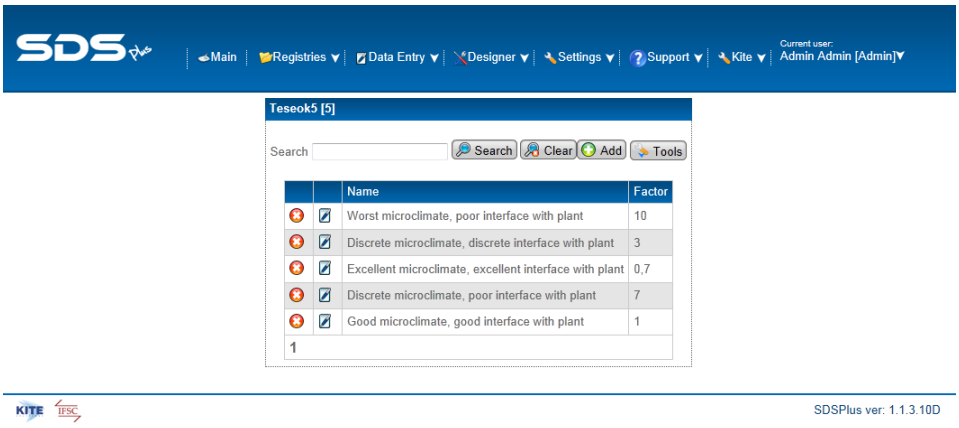


Figure A.2: Rappresentation of K_5 table in SDS Plus.

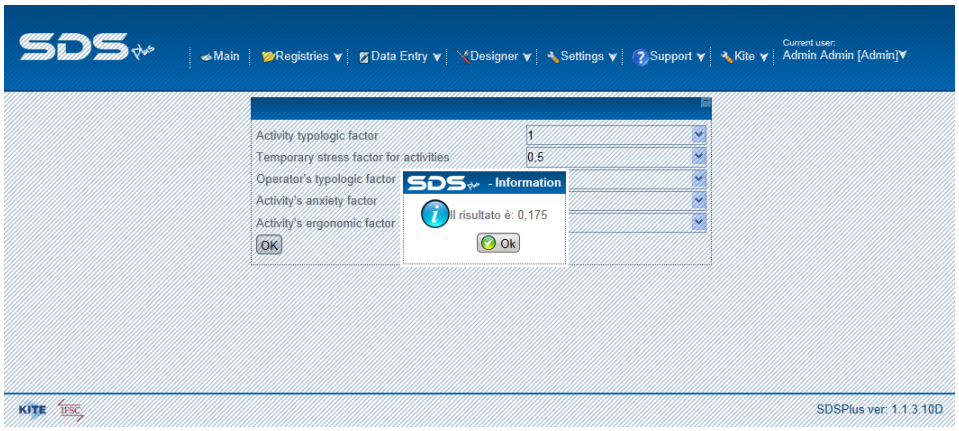


Figure A.3: Rappresentation of *HU* result in SDS Plus.

A.2 THERP

The THERP method, *Technique for Human Error Rate Prediction* [20], is used in HRA and it composed by four phases divided into twelve steps and they are:

1. Familiarisation;
2. Qualitative Assessment;
3. Quantitative Assessment;
4. Incorporation.

THERP organises all possible errors and operator's mishaps in two general types:

- error of omission;
- error of commission.

The first type of error concerns the omission of one or more steps during the execution of the operation; the second type of error concerns the lack of knowledge and wrong interpretation of the information.
In order to describe and analyse errors and human behaviour, THERP uses the Event Trees concept (binary alternative possibility of success or failure of a step/activity in a procedure) and this is called HRA-ETs, *Human Reliability Analysis - Event Trees*. As showed in figure A.4, the trees are developed in a vertical way and each action is represented by a decision point. Each decision point is binary and, in general, the right side of the tree represents the failure while the left side represents the success of every action.
The probability of success and failure of a procedure is assigned to every decision point and then the evaluation of the probability is made with the Quantitative Risk Assessment (QRA) expressions.

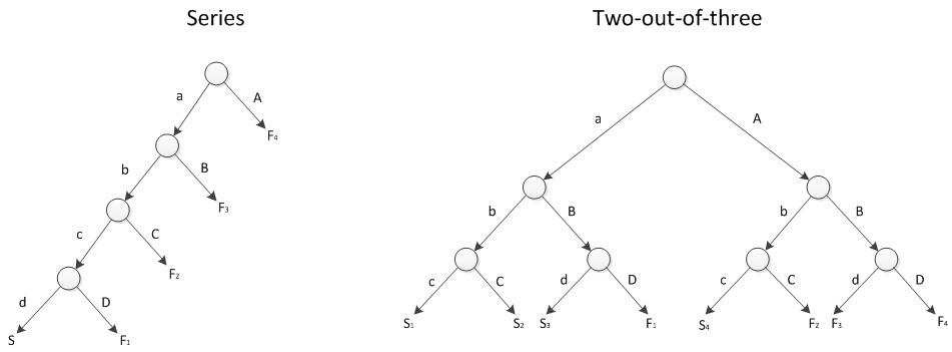


Figure A.4: Types of event trees [3].

The twelve steps are described in detailed:

- Step 1: Plant Visit:
  the analyst studies the aspects of the control systems and the elements that can affect PSF;
- Step 2: Review Information from System Analyst:
  the system analyst finds the critical human actions, identified in the previous step, and these are analysed by the reliability analyst again;

- Step 3: Talk- or Walk- Through:
  the reliability analyst discusses the procedures with the system operators and defines the requirements for the operators performance;
- Step 4: Task Analysis:
  the reliability analyst divides the procedures into different tasks and and he finds the most significant for the safety and reliability system. Moreover, the analyst identifies the possible operators errors;
- Step 5: Develop HRA Event Trees:
  in this step the possible errors are described by event trees but in this phase the recoveries are not introduced;
- Step 6: Assign Nominal Human Error Probabilities:
  this step estimates NHEP of every action in the HRA-ETs; the values of NHEP come from simulation tests and experts judgements;
- Step 7: Estimate the Relative Effects of PSFs:
  in this step HEPs are modified in order to take into account the actual features of the case study;
- Step 8: Assess Dependence:
  the dependence between the actions, in which the procedure is divided, is taken into account. The type of dependence considered is the positive one, where the success (error) of an action increases the success (error) probability of another action; for the other types of dependences a conservative probability calculation can be obtained by considering the two actions independent from each other;
- Step 9: Determine Success and Failure Probabilities:
  in this step the analyst calculates the value of the probability of the mission success and failure;
- Step 10: Determine the Effects of Recovery:
  the evaluation of the possible recoveries is performed in order to estimate their effect;
- Step 11: Perform a Sensitivity Analysis, if Warranted:
  a sensitivity analysis on a single parameter is performed;
- Step 12: Supply Information to System Analyst:
  the results of the analyses are presented to the system analyst and a review of the results is made in order to assure the correct progress of the analyses.

Acronym

APC	Auxiliary Performance Computers
APJ	Absolute Probability Judgement
ARMS	Airline Risk Management Solutions
ATC	Air Traffic Control
ATHEANA	A Technique for Human Error Analysis
CFIT	Control Flight Into Terrain
CM	Crew Member
COCOM	COntextual COntrol Model
COTS	Commercial-Off-The-Shelf
CREAM	Cognitive Reliability and Error Analysis Method
DYLAM-HERA	Dynamic Logical Analytical Method for Human Error Risk Assessment
EASA	European Aviation Safety Agency
EFB	Electronic Flight Bag
EFP	Engine Failure Procedure
EGPWS	Enhanced Ground Proximity Warning System
EJ	Expert Judgement
ENAC	Ente Nazionale per l'Aviazione Civile
EOP	Emergency Operating Procedures
ERC	Event Risk Classification

FAA	Federal Aviation Administration
FAME	Function Allocation Method
FMC	Flight Management Computer
FMS	Flight Management System
GPS	Global Positioning System
HCR	Human Cognitive Reliability
HE	Human Error
HEP	Human Error Probability
HFE	Human Failure Events
HR	Human Reliability
HRA	Human Reliability Analysis
HU	Human Unreliability
ICAO	International Civil Aviation Organization
LAPC	Laptop Auxiliary Performance Computers
MEL	Minimum Equipment List
MOC	Management of Change
MSA	Minimum Safe Altitude
NHEP	Nominal Human Error Probabilities
NOTAM	NOtice To AirMen
NPF	Not Pilot Flying
OAT	Operator Action Tree
OEF	One Engine Failure
PC	Paired comparisons
PF	Pilot Flying
PR	Probability of Recovery

PSF	Performance Shaping Factors
QRA	Quantitative Risk Assessment
RAMCOP	Risk Assessment Methodology for Company Operational Processes
SA	Situational Awareness
SHARP	Systematic Human Action Reliability Procedure
SID	Standard Instrument Departure
SIRA	Safety Issues Risk Assessment
SLIM	Success likelihood index methodology
SMS	Safety Management System
SOP	Standard Operating Procedures
SRK	Skill, Rule, Knowledge
TCAS	Terrain Control Avoidance System
TESEO	Tecnica Empirica Stima Errori Operatori
THERP	Technique for Human Error Rate Prediction
TO	Take-Off
UA	Unsafe Actions
WL	Workload

Bibliography

[1] International Civil Aviation Organization ICAO. *DOC 9859 - Safety Management Manual (SMM)*, 2009.

[2] ENAC. *Informative Note NI-2012-14 of October 31*, 2012. `http://www.enac.gov.it/La_Regolazione_per_la_Sicurezza/Note_Informative/info-1014002619.html`.

[3] P.C. Cacciabue. *Sicurezza del Trasporto Aereo*. Springer-Verlag Italia, Milano, 2010.

[4] International Civil Aviation Organization ICAO. *DOC 9859 - Safety Management Manual (SMM)*, 2006.

[5] International Civil Aviation Organization ICAO. *DOC 9859 - Safety Management Manual (SMM)*, 2012.

[6] ARMS Working Group. *The ARMS Methodology for Operational Risk Assessment in Aviation Organization*, 2010.

[7] BowTie Pro. http://www.bowtiepro.com/, May 2012.

[8] D.S. Nielsen. *The Cause/Consequence Diagram Method as a Basis for Quantitative Accident Analysis*, 1971. Danish Atomic Energy Commission, RISO-M-1374.

[9] S. Kurniawan. Cmpe 233: Human Factors, Human Reliability. `http://users.soe.ucsc.edu/~srikur/files/Lecture8a.pdf`, 2008. Jack Baskin School of Engineering, University of California, Santa Cruz.

[10] J. Bell and J. Holroyd. *Review of human reliability assessment methods*, 2009. Health and Safety Laboratory.

[11] G.W. Hannaman and A.J. Spurgin. *Systematic Human Action Reliability Procedure (SHARP)*. EPRI NP-3583, Project 2170-3, Interim Report, NUS Corporation, 1984. San Diego, CA, US.

[12] P.E. Dawson. *Evaluation of the Economic Simplified Boiling Water Reactor Human Reliability Analysis Using the SHARP Framework*. Bachelor of Science in Mechanical Engineering, MIT, US, 2007.

[13] J.W. Wreathall. *Operator Action Action Tree, An Approach to Quantifying Operator Error Probability During Accident Sequences*. NUS Report 4159, NUS Corporation, 1982. Gaithersberg, Maryland, US.

[14] D.A. Seaver and W.G. Stillwell. *Procedures for using Expert Judgement to Estimate Human Error Probabilities in Nuclear Power Plant Operations*. NUREG/CR-2743, USNRC, 1982.

[15] L.L. Thurstone. *A Low of Comparative Judgement*. Psychological Review 34:273-286, 1980.

[16] G. C. Bello and V. Colombari. *The human factors in risk analyses of process plants: the control room operator model TESEO*, 1980. RE&SS, 1:3-14.

[17] D.E Embrey, P.C. Humphreys, E.A. Rosa, B. Kirwan, and K. Rea. *SLIM-MAUD: An Approach to Assessing Human Error Probabilities Using Structured Expert Judgement*. NUREG/CR-3518, USNRC, 1984. Washington, US.

[18] G.W. Hannaman, A.J. Spurgin, and Y.D. Lukic. *Human Cognitive Reliability Model for PRA Analysis*. NUS-4531, NUS Corporation, 1984. San Diego, CA, US.

[19] J. Rasmussen. *Skills, Rules and Knowledge: signals, signs and symbols; and other distinctions in human performance model*. IEEE-SMC 13-3:257-267, 1983.

[20] A.D. Swain and H.E. Guttmann. *Handbook on Human Reliability Analysis with Emphasis on Nuclear Power Plant Application*, 1983. Draft Report NUREG/CR-1278 SAND 80-0200 RX, AN Final Report.

[21] E. Hollnagel and P.C. Cacciabue. *Reliability of Cognition, Context, and Data for a Second Generation HRA*. Proceedings of International Conference on Probabilistic Safety Assessment and Management, 1994, March 20-25. San Diego, California.

[22] M.T. Barriere, D.C. Bley, S.E. Cooper, J. Forester, A. Kolaczkowski, W.J. Luckas, G.W. Parry, A. Ramey-Smith, C. Thompson, D.W. Whitehead, and J. Wreathall. *Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA)*, 2000. NUREG - 1624, US-NRC, Washington DC.

[23] E. Hollnagel. *Cognitive Reliability and Error Analysis Method*. Elsevier, 1998. London.

[24] P.C. Cacciabue. *A Methodology for Human Factors Analysis for System Engineering: Theory and applications*. IEEE-System Man and Cybernetics. IEEE-SMC 27-3:325-339, 1997.

[25] P.C. Cacciabue. *Modelling and Simulation of Human Behaviour in System Control*. Springer-Verlag, London, UK, 1998.

[26] P.C. Cacciabue. *Guide to Applying Human Factors Methods*. Springer-Verlag, London, UK, 2004.

[27] Prosci Inc. Welcome to the change management tutorial series. http://www.change-management.com/tutorial-definition-history.htm, Visited in January 2012.

[28] A. De Col. Un approccio pratico alla valutazione del rischio per il Safety Management System in campo aeronautico: il caso studio delle perdite di separazione in volo. Master Degree, Politecnico di Milano, 2012.

[29] Airbus. Flight Operations Briefing Notes - Standard Operating Procedures - Conducting Effective Briefings. `http://www.airbus.com/fileadmin/media_gallery/files/safety_library_items/AirbusSafetyLib_-FLT_OPS-SOP-SEQ06.pdf`, 2004.

[30] Air Dolomiti. *Standard Operating Procedures, Normal Procedure for Embraer 195*, 2011.

[31] Teledyne controls. `http://www.teledynecontrols.com/productsolution/efb`, Visited in January 2012.

[32] JAA Administrative and Guidance Material. Leaflet no. 36: Approval of electronic flight bags (efbs). `http://www.dac.public.lu/documentation/procedures_ops/`, 2004.

[33] I. Oddone and A. Ottomaniello. Personal communication, 2011-2012.

[34] A. Ottomaniello and I. Oddone. *Risk Assessement - Flights in Airspace contaminated by Volcanic Ash*, 2011.

[35] E. De Grandis, I. Oddone, A. Ottomaniello, and P.C. Cacciabue. *Managing risk in real contexts with scarcity of data and high potential hazards: the case of flights in airspace contaminated by volcanic ash*. Proceedings of PSAM-11 - ESREL 2012, 2012, June 25-29. Helsinki, Finland.