A Resilience Engineering approach for the evaluation of performance variability: development and application of the Functional Resonance Analysis Method for air traffic management safety assessment

Luigi Macchi

ParisTech
INSTITUT DES SCIENCES ET TECHNOLOGIES
PARIS INSTITUTE OF TECHNOLOGY

MINES ParisTech

Ecole doctorale n° 432: Sciences et métiers de l'ingénieur

Doctorat ParisTech

T H È S E

pour obtenir le grade de docteur délivré par

l'École nationale supérieure des mines de Paris

Spécialité "Sciences et Génie des Activités à Risques "

présentée et soutenue publiquement par

Luigi MACCHI

le 22 juin 2010

A Resilience Engineering approach to the evaluation of performance variability: development and application of the Functional Resonance Analysis Method for Air Traffic Management safety assessment

Directeur de thèse : **Erik HOLLNAGEL**

Jury

M. Philippe CABON, Maître de Conférences HDR, Unité d'Ergonomie, Université Paris Descartes	Rapporteur
M. Frederic VANDERHAEGEN, Professeur, LAMIH, Université de Valenciennes	Rapporteur
M. Nicholas MC DONALD, Professeur, School of Psychology, Trinity College Dublin	Examinateur
M. Pietro Carlo CACCIABUE, Professeur, Politecnico of Milan	Examinateur
M. Sébastien TRAVADEL, Adjoint au chef du département Investigation, BEA	Examinateur
M. Erik HOLLNAGEL, Professeur, Mines Paristech	Directeur de thèse

T H E S E

MINES ParisTech
Centre de recherche sur les Risques et les Crises
Rue Claude Daunesse, B.P. 207 - 06904 Sophia-Antipolis Cedex - France

ACKNOWLEDGEMENTS

After having written the whole manuscript, it is now due time to give credit to the persons without whom this thesis would have never seen the light. Those I mention (as well as those I forgot to mention) have full credit for what *went right.* I take full responsibility for what *went wrong.*

An heart-felt thank goes to Prof. Erik Hollnagel for the knowledge and experience he always put at disposal. I am grateful to him for the subtle, inspiring and accurate scientific supervision of my thesis.

My gratitude goes to Dr. Denis Besnard and to Dr. Eric Rigaud as well. Merci beaucoup pour votre contribution à ce travail. Discuter avec vous, soit sur des sujets scientifique ou bien sur questionnes personnelles, a été toujours d'aide. Merci.

I (as much as the readers) feel in debt with Elaine Seery for proof-reading the thesis. It was painful, I know. But, thanks a lot!

Un remerciement particulier va à les autres doctorants de la Chaire de Sécurité Industrielle. Eduardo et François qui ont démarré leur thèse au même moment que moi et qui ont été mes compagnons dans cette expérience; Damien et Daniel qui ont rejoint le groupe en cours de route et avec qui a été un plaisir travailler.

Je suis reconnaissant aussi à tout l'équipe du Centre de Recherche sur les Risques et les Crises (CRC), en particulier au secrétariat et au support informatique que bien souvent m'ont donne un coup de main, au delà de leur du.

This thesis offered me the possibility to have a glance into the surprising Air Traffic Management world. For that, I want to acknowledge EUROCONTROL and Deutsche FlugSicherung (DFS) for the generous support offered during the FARANDOLE project. Special credit goes to all DFS Air Traffic Controllers and human factors and safety experts I met and bothered during my study.

In particular, Jörg Leonhardt deserves a mention. It has been a pleasure to meet you as much as to work with you.

Je dis merci à tous les thésards (et pas thésards) que j'ai eu la fortune de rencontre pendant mon séjour sur la Cote. Merci à vous tous pour avoir partage avec moi les pauses café sur la passerelle, les pétanques, les moments de détentes etc.

Thank to my family. Perchè senza il loro supporto le cose sarebbero molto più complicate.

The last line is dedicated to Delphine. Je te remercie pour beaucoup plus de choses que ton aide dans cette thèse.

Table of Content

List of Figures

List of Tables

List of Tables - Annex

Page intentionally left blank

SUMMARY

This thesis demonstrates the need to develop and apply systemic safety assessment methods to account for the effect of performance variability on Air Traffic Management safety.

Traditionally, safety assessments have been focused on the identification and estimation of failures, breakdowns and human errors. Thus, they required the identification and description of system's components, their functioning modes and their interdependencies. As the underlying assumption of safety assessment was that the system's components - including humans - have a bimodal functioning, i.e. they function or they fail, it was possible to warrant safety by making sure that the prescribed components' performance was reliable and no deviations occurred.

For Air Traffic Management, this assumption is inadequate. Like most modern socio-technical systems, it is so complex and it changes so rapidly that, in practice, it is impossible for it to be completely described and specified. As direct consequence, performance cannot be completely specified because it must vary to meet actual conditions and demands. Resilience Engineering acknowledges that performance variability is, in the context of complex socio-technical systems, an inevitable asset to ensure the functioning of an organisation and at the same time can be harmful for system safety when it combines in an unexpected and undesired manner.

This argument clearly indicates the need for safety assessment methods that can deal with performance variability. Several applications (e.g. Woltjer & Hollnagel, 2007; Lundblad et al., 2008, Rome, 2009) illustrate that the Functional Resonance Analysis Method (FRAM) (Hollnagel, 2004) has the ability to model socio-technical systems and to account for performance variability, both in accident analysis and safety assessment. However parts of the FRAM can be improved to expand its capabilities to evaluate and manage performance variability.

This thesis addresses this weakness and develops and illustrates a methodology for the evaluation of performance variability that accounts for:

1. The heterogeneity of functions performed in a socio-technical system;
2. The performance variability due to local adjustments made to meet performance demands;
3. An aggregate representation for performance variability during safety assessment.

The evaluation of the the methodology has been based on a safety assessment case study for a ground based safety net in the German Air Traffic Management domain. The results have been compared with the official results obtained during a traditional safety assessment process. The comparison shows the added valued of the proposed methodology. In particular it illustrates the possibility to identify emergent risks and human contribution to system safety.

The concluding section of this thesis explores the integration of the proposed methodology into current safety assessment and potential guidelines for future improvements to the Resilience Engineering approach to system safety are outlined.

References

Hollnagel, E. (2004). *Barriers and accident prevention.* Aldershot: Ashgate.

Lundblad, K., Speziali, J., Woltjer, R., & Lundberg, J. (2008). FRAM as a risk assessment method for nuclear fuel transportation. In *Proceedings of the 4*th *International Conference Working on Safety*. Crete, Greece.

Rome, F. (2009). De l'analyse de l'accident à l'analyse du travail: Application à deux cas d'étude dans la sécurité aérienne. PhD Thesis: Ecole Doctorale "Cognition, Comportament, Conduites Humaines". Universitè Paris Descartes.

Woltjer, R. & Hollnagel, E. (2007). *The Alaska Airlines Flight 261 accident: A systemic analysis of functional resonance*. Proceedings of the 2007 (14th) International Symposium on Aviation Psychology (ISAP), 763-768, Dayton, OH.

Because things are the way they are,
things will not stay the way they are

Bertolt Brecht

Ah, this is obviously some strange usage of the word 'safe'
that I wasn't previously aware of.

Douglas Adams

Page intentionally left blank

Chapter 1: Safety Challenges for Air Traffic Management

Page intentionally left blank

Résumé du Chapitre 1

Dans un proche avenir, le système européen de gestion du trafic aérien sera révolutionné par de grands changements structurels, fonctionnels et organisationnels, afin d'accroître son efficacité. Tous ces changements doivent se soumettre à un processus d'évaluation des risques, de manière à identifier et éliminer tous les risques considérés inacceptables.

La gestion du trafic aérien a besoin de modèles et de méthodes pour assurer et améliorer la sécurité; l'objectif de cette thèse est de démontrer la nécessité d'appliquer des méthodes systémiques pour évaluer la variabilité de la performance et ses effets sur la sécurité du système.

La pertinence de cet objectif est examinée à partir d'une analyse de l'évolution historique des stratégies de sécurité. La complexité du système de gestion du trafic aérien requiert l'application de méthodes capables de saisir la dynamique de système réels ainsi que leur performance. Traditionnellement, les modèles et méthodes étaient axés sur les accidents, les incidents évités de justesse, tandis que le fonctionnement normal du système était généralement exclu de l'analyse. Ce chapitre, sur la base de Normal Accident Theory, Théorie des accidents normaux (Perrow, 1984) et de Resilience Engineering, Ingénierie de la Résilience (Hollnagel, Woods, Leveson, 2006; Hollnagel, Nemeth, Dekker, 2008), présente les raisons pour lesquelles le fonctionnement normal doit être au centre de l'étude de l'estimation de la sécurité et la raison pour laquelle la variabilité de la performance doit être correctement gérée.

Introduction

In the near future European Air Traffic Management system will be revolutionised by major structural, functional and organisational changes to increase its efficiency. All these changes have to undergo a safety assessment process to identify and eliminate all unacceptable risks.

Air Traffic Management needs models and methods to ensure and improve safety; the objective of this thesis is to demonstrate the need for applying systemic methods to evaluate performance variability and its effect on system safety.

The relevance of this objective is discussed, starting from a review of the historical evolution of safety approaches. The complexity of Air Traffic Management systems requires the application of methods able to capture real system's dynamics and performance. Traditionally, models and methods have been focused on accidents, incidents, near-misses while the normal system functioning was normally excluded from the analysis. This chapter, on the basis of Normal Accident Theory (Perrow, 1984) and of Resilience Engineering (Hollnagel, Woods, Leveson, 2006; Hollnagel, Nemeth, Dekker, 2008), presents the reasons why normal functioning has to be the focus of safety assessment and why performance variability has to be correctly managed.

1 Research context: Air Traffic Management

Safety is aviation's top priority. Air Traffic Management (ATM) plays a major role in ensuring safe aircraft departures, flights, landings and ground manoeuvres. Air Navigation Service Providers (ANSPs) produce safety by providing safe separation margins to aircraft both in the air and on the ground. At the same time, economic and operational conditions have to be maintained efficiently.

European citizens increased mobility, for business and leisure, has led to a growing demand for safe, high-quality air transport. By the year 2020, air traffic is predicted to grow by about 5% a year which means that the traffic flow in Europe will double with respect to what it was ten years ago. Hence, in the near future, European ATM will have to meet the increased traffic flow while simultaneously improving safety levels and reducing environmental impact in a cost-effective way.

These requirements are going to be satisfied by the development of a new ATM concept implying a structural revision of the ATM system. The Single European Sky (SESAR) Joint Undertaking, launched by the European Community and by the European Organisation for the Safety of Air Navigation (EUROCONTROL), aims at

the implementation of the first necessary step in the direction of a reorganisation of European ATM system: the *achievement of one airspace continuum for ATM purposes in Europe which encompasses the airspace at and around airports as well as en-route* (EUROCONTROL, 2003. p.16).

1.1 Air Traffic Management: a complex socio-technical system

Air Traffic Management is a socio-technical system where technology is embedded in a social context that designs, tests, runs and maintains it. The term socio-technical system refers to the coupling between social and technical aspects in an organisation (Trist, 1978). From the interaction between the two set of aspects stems the successful (or unsuccessful) performance of the organisation.

Modern and future Air Traffic Management, as socio-technical system, holds prominent features which increase the challenges to ensure its safe functioning. Safety assessment has to be performed for a system where Air Traffic Controllers (ATCOs) have to continually interact and control a dynamic environment to produce an efficient and safe traffic flow in the sky. Air Traffic Controllers learn rules and procedures, as well as how to best use the available technology to accomplish their tasks. To be successful, besides reliable technology and appropriate procedures, ATM requires another important element: the controllers' activity that continuously combines their procedural knowledge with the requests and constraints from their working environment and from the on-going situations.

The ATM domain can be characterised by four features which challenge safety and thus have to be considered when performing safety assessment:

Complexity

ATM is indeed complex. The central aspect of complexity is related to the number of elements and the nature of the interactions taking place within the system. Complex socio-technical systems are as well characterised by large problem space, distributed dynamic, potentially high hazards, many coupled subsystems, automated uncertain data and mediated interaction via computers (Vincente, 1999). The enormous amount of technology, required to meet ATM performance demands, leads to a high

level of system complexity. The envisaged revision of ATM structure, to increase performance capacity, is likely to result in a general ATM system increase in complexity even if, locally, there will be improvements. The increased complexity is also likely to result in an increased level of unpredictability of system behaviour where actions have unexpected and potentially adverse consequences (Hollnagel & Woods., 2005).

Uncertainty

The uncertainty characteristic of ATM relates to the knowledge about the environment and its future states. To deal with regular environment, Air Traffic Controllers develop patterns of behaviour appropriate to solve recurrent situations. But for out-of-the ordinary situations, they are obliged to build a hypothesis with the available information and knowledge and to make judgements on how to best cope with the demands.

Dynamic

The ATM environment is intrinsically dynamic. The control of a dynamic process is affected by four aspects: 1) the rate of change in the process to be controlled; 2) the relation between the process to be controlled and the control process; 3) possible delays in the system; 4) the quality of the feedback information. Controllers have three possibilities to control a dynamic process: 1) develop a mental model of the task; 2) develop heuristic rules; 3) rely on feedback and modification of behaviour (Brehmer & Allard., 1991).

Underspecification

The three above mentioned features of ATM domain leads straight to a fourth one: underspecification. No matter the amount of effort, it is utopian to claim to achieve a complete description of an ATM system, a description accounting for every possible scenario, every possible situation's development, every possible interaction between system components etc. The underspecification of ATM requires ATCOs fundamental contribution to system functioning and safety. This situation is extremely clear to controllers, who pride themselves on their skills, and their

understanding of rules and procedures, that enable them to deliver the best service to their clients (EUROCONTROL, 2009).

2 Research objectives

Safety for modern Air Traffic Management is a big challenge since it has to be assessed and ensured for any change in the ATM system and accidents are unacceptable. Safety assessment tradition is long and honoured. But modern socio-technical systems question the power of available safety assessment methods. The underspecification of ATM creates the needs for controllers to perform local adjustments of their activities. These adjustments are, not only constant, but necessary for the the organisation to effectively pursue its objective (Bourrier, 1996). Local adjustments make performance variable and this has to be considered during safety assessment.

The objective of this thesis is to demonstrate the need for developing and applying systemic safety assessment methods to account for the effect of performance variability on Air Traffic Management safety. In contributing to the development of the Functional Resonance Analysis Method this thesis aims at demonstrating the necessity to acknowledge that performance is – and has to be – variable, to maintain the functioning of modern socio-technical system. The acknowledgement of sources and reasons for performance variability is the precondition for its management and for safety improvements.

3 Safety assessment: identifying and eliminating unacceptable risks

To ensure an acceptable safety level for such a complex and distinctive socio-technical system it is necessary for any change in ATM to undergo a thorough safety assessment process. EUROCONTROL (2001) defines safety assessment as the systematic and comprehensive process to establish safety requirements and to demonstrate that these requirements are met.

While accident analysis is a reactive process, safety assessment is a proactive one. The proactivity of safety assessment consists in foreseeing potential events and in taking appropriate actions to prevent undesired events to strike the organisation. The efficacy of safety assessment therefore relies in the ability of the organisation to predict as many risks as possible, since their non-identification will leave the organisation unprepared to cope with them.

To be effective, risks identification requires a systematic and rigorous application of an accident model, and its associated method, in order to make sense of the indicators used to predict the occurrence of future events (Figure 1). A safety definition, an accident model and the identification of indicators are used to develop a safety assessment method which is applied to interpret (i.e. to make sense of) field data. Risks identification and safety requirements are the concluding achievement of this process (Hollnagel, 1998).

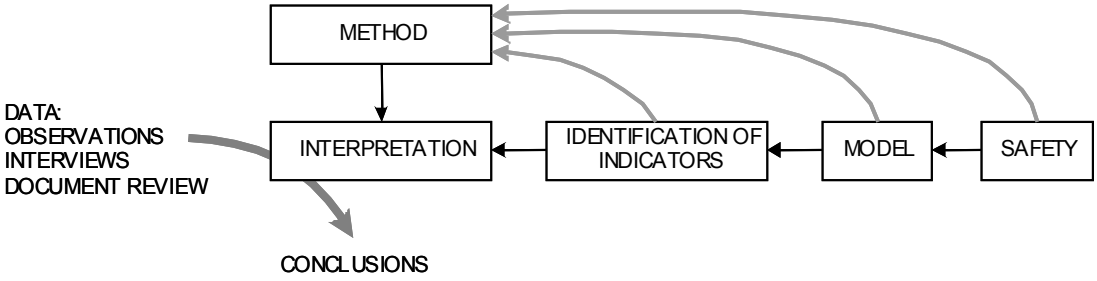


Figure 1: Relation between safety definition, model and indicators (Adapted from Hollnagel, 1998)

In the next section it is argued that there are three main stages in the development of safety assessment methods. The distinction refers to different assumptions, methods and attribution of accident causes characterising the history of industrial safety (Hale & Hovden, 1998). The evolution has been driven by the technological development of the industrial system, and it could be represented by the efforts of safety practitioners and scientific community to keep the pace with the changes of the industrial world.

3.1 Theories and models of the negative: three ages of industrial Safety assessment

New, more complex technologies and organisational structures required safety assessment models and methods more and more powerful to identify and to manage risks.

1. From the nineteenth century to the the end of the Second World War (the age of Technology), the concern was exclusively related to technological failures triggering accidents. Safety assessment methods searched for root causes by applying simple linear thinking about cause-effect relationships;
2. Starting from 1979 (the age of Human Factors), the human role in accident causation was considered. Together with probabilities of technical failures, the evaluation of probabilities of human errors became relevant. Safety assessment methods evolved towards the adoption of multi-cause linear thinking, also expressed by the epidemiological models;
3. From the late 1980s (the age of Safety Management), the role of organisations and organisational culture came into the picture. Safety assessments methods moved towards a more systemic approach and accidents started to be considered as the outcome of normal system functioning rather than out-of-the-ordinary events.

3.1.1 The age of Technology

Hale and Hovden (1998) identified the first age of safety in scientific studies that started in the nineteenth century and lasted until after the Second World War. In that period, safety concerns were related to technical reliability. The safety objective was the prevention of structures' collapse, explosions and failures. The need to have safe and reliable technologies drove the development of safety assessment methods to assure that nothing goes wrong as a consequence of technological failures.

That it is possible to warrant the safety of a technological system, through an appropriate safety assessment study, is related to the nature of the system itself. Technological systems are built from clear and explicit design principles. Their

architecture, components and functioning are known to designers. Models and analysis methods are formal, standardised and validated. In addition, a technological system has a well-defined mode of operation and high structural and functional stability.

The methods developed to perform safety assessment in the age of Technology (e.g. HAZOP, Fault Tree, FMEA) are based on the assumption that it is possible to identify the root causes of accidents through the application of a linear search of cause-effect relationships. Despite the efficiency of this approach in managing the safety of technological systems, linear reasoning shows its limitations when applied to more complex systems.

3.1.2 The age of Human Factors

The Three Mile Island (TMI) nuclear power plant accident that occurred in 1979 showed how a technical safety assessment could not solve every safety problem, and called for the inclusion of humans in the analysis focus. The most substantial development of the second age of industrial safety is nevertheless to be found in the merging of technological safety assessment and ergonomics/human factors studies.

In the age of Technology, as previously explained, it was possible to assure safety because the functioning of the technology was clear and understood. However the situation is not the same when humans are taken into account. When the same characteristics are considered, it is clear that for humans the design principles are unknown and their architecture is only partly known. If for technology, models are formal and explicit, in the case of humans, models are based on analogies and methods are unproven. Despite the evidence that humans are reliable, their mode of functioning is only vaguely defined and understood.

The urge to develop, in response to the TMI event, safety assessment methods and the practicality offered by available knowledge and experience, led to the development of methods with a similar approach for humans and technology.

The first methods (e.g. THERP, OAT SLIM/MAUD), also called first generation Human Reliability Assessment methods, were based on event tree representations,

and they aimed to estimate human error probabilities and their effect on system failures. The simple, linear casual thinking, that characterised the technological methods, evolved towards a complex, casual thinking. The safety community realised that it was needed to account for multiple causes of accidents, and the effect of the context, on error probabilities was also introduced into the analysis.

This evolution moved the accident models and methods towards the development of the so-called epidemiological models. Epidemiological accident models (the Swiss Cheese model (Reason, 1997) is the champion of this category) consider accident development as a linear phenomenon but their scope is longer in time, and levels of analysis (e.g. latent failures that originate from design) can be included. In terms of the causality approach to accident analysis, epidemiological models adopt an improved and more complete version of the linear cause-effect relation.

The age of Human Factors came to an end, according to Hale and Hovden (1998), when in the '80s dissatisfaction with the ability of the methods and models to match the safety needs of industrial systems became evident.

3.1.3 The age of Safety Management

The third safety age identified described by Hale and Hovden (1998) concerns the development of models and methods that expanded the focus of analysis from the workplace and the interaction between humans and technology, to the study of the organisation and its dynamics. If a birth date has to be set for the age of Safety Management, it could be 1986, when the Chernobyl nuclear power plant disaster and the Challenger explosion rose awareness that established approaches were no longer sufficient to assure system safety.

Before entering into the discussion of organisational theories and models it is worth addressing, as it has already been done for the Technology and Human Factors age, the question of the organisation's characteristics upon which safety is ensured.

The step-by-step design of an organisation and the actual final result are only partially known. The models used to assure safety are based on a semi-formal description of the organisation, and the methods could not be proved true. Despite

the fact that the modes of operation are complex and only partially definable, organisations tend to show a good functional stability.

However, the theoretical development of safety management approaches started earlier. Hale and Hovden trace the first attempts to account for the managerial dimension of safety back to the beginning of the twentieth century. The two authors recognise that those attempts were basically a collection of common sense and general management principles applied to safety.

In the age of Safety Management a wide number of theories and models have been proposed by the scientific community e.g. Man-made disasters (Turner, 1978); High Reliability Organisations (LaPorte & Consolini, 1991; Rosness et al, 2004); Normal deviation theory (Vaughan, 1996); Drift into failures (Rasmussen, 1997), but despite the enlarged focus of analysis they shared a common approach with earlier models: they were focused on accidents and aimed at the identification of their causes.

This is true for all three ages of industrial safety. Accidents were considered to be caused either by a fallible technology, or by careless, inexperienced, untrained humans or by the characteristics (complex, brittle etc.) of the organisations. Over the time, accidents causes were attributed to technology, to human errors or to organisational failures and the safety efforts were aiming at the implementation and improvement of safety barriers. This approach has two major consequences. The first consequence is that safety is, normally, perceived in competition with the core business of the organisation. Since safety is disjunct from business, every resource allocated to improve safety is perceived as detracting from business. The second consequence is related to the possibilities for organisational learning. Since learning is related to the number and typology of events, if safety efforts are successful, few (or ideally no) negative events will occur. In this scenario, safety management will lack information about the organisation's safety status and the planning of safety improvements might become a matter of expert-guess.

Acknowledging the drawbacks and limitations of the use of safety assessment methods based on a “negative” approach to safety, EUROCONTROL is currently developing an advanced and innovative safety assessment approach to cope with

the massive changes to European ATM, due to SESAR development. The main guidelines of this approach are presented in the following section.

3.2 Safety assessment for Air Traffic Management: the EUROCONTROL approach

In the need to ensure safety for European Air Traffic Management, EUROCONTROL acknowledges that a traditional, failure based approach to safety assessment will be unable to provide the full scope of assurances needed, and to ensure that the new operational concepts will be acceptability safe. Central to development of the innovative approach is understanding the relationship between pre-existing risk, the positive and negative contribution of the three ATM barriers (i.e. Strategic Conflict Management, Separation Provision, and Collision Avoidance), as well as the positive contribution of Providence (Fowler, Perrin & Pierce, 2009). The following figure expresses the relationship between pre-existing risk and the contribution (positive and negative) of the ATM barriers.

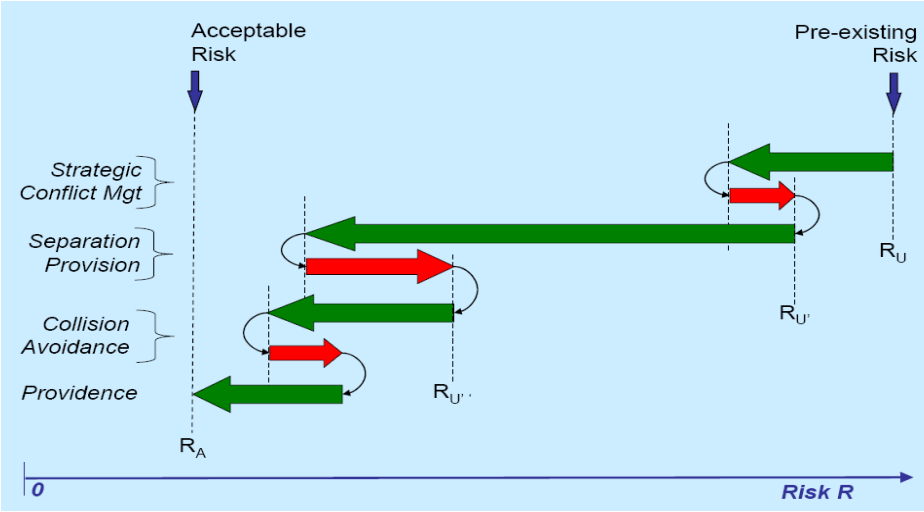


Figure 2: ATM risk graph (from Fowler et al., 2009)

The safety assessment is based on the construction of safety cases, that, once demonstrated, warrant that the risks identification and elimination process is at an acceptable level.

A safety case consists of two main elements: a set of arguments or statements which claim that something is true (or false), and supporting evidence to show that the

argument is valid. Arguments are normally defined in a hierarchical way, meaning that any particular argument is valid only if all the next-level arguments are themselves valid.

At some point in the decomposition of the arguments, the hierarchical structure requires that it can be determined that the ATM system has been designed in a satisfactory manner, and that all the system requirements and specifications are satisfied by the implementation. But in the case of the development and design of a brand new operational concept (as SESAR is at the current stage), it is not possible to assess the detailed physical design, since it will only become clear in a later implementation phase. In order to overcome this problem, EUROCONTROL (2009) proposes to base the safety assessment on a more generic representation of the future system, called the logical design. The logical design is composed of a *Logical Model* (LM), which is defined as:

> *A high-level, architectural representation of the system design that it is entirely independent of the eventual physical implementation of that design. The LM describes the main human tasks, machine functions, and airspace design parameters and what each of those "actors" provides in terms of safety functionality and performance – these are known as Functional Safety Requirements (FSRs). The LM normally does not show elements of the physical design, such as hardware, software, procedures, training etc.*

The correctness of the Logical design under normal and abnormal conditions of functioning is checked by means of a Thread analysis of the *Functional Safety Requirements* of the designed system.

Despite the formal acknowledgement of the limitations of a failure based safety assessment, EUROCONTROL approach is still focused on the search for hazards and risks. Accident prevention is based on the enforcement of barriers, for which both the positive and negative contribution to risk reduction is assessed.

To overcome the limitations of a failure based safety assessment, and to improve the management of safety in ATM it is necessary to use a language that does not emphasize structure, components, parts and interaction, cause and effect (Dekker, 2005). It is as well necessary to expand the focus of safety analysis by the

consideration of the normal functioning of the socio-technical system, the functioning which produces daily successful operations.

4 From focusing on the negative to also looking at the positive

In the age of Safety Management the normal characteristic of industrial accidents started to be highlighted in the safety literature. The Drift into failure metaphor, the identification of normal deviations and, obviously, the Normal Accident theory showed the non-extraordinary nature of the mechanisms leading to accidents. Despite this, approaches were still focused on the "negative", causes and barriers were the relevant focus of analysis. Rasmussen (1997), with the drift into failure metaphor, recognises the importance of trades-off in governing normal organisation activities and in influencing the possibility of failure or success. Vaughan's notion (1996) that deviations might become acceptable and that they therefore constitute the normal context for successful functioning of the organisation (until something goes wrong) pinpoints the fact that accidents should not be understood as something intrinsically different from success. Acknowledging that the organisational activities leading to an accident are the same as the organisational activities leading to success should draw the attention to the lack of theories and models able to explain operational success or normal work (Dekker, 2006).

4.1 Normal Accident Theory

The champion of the theories about the normal nature of accidents in industrial systems dates back to 1984 when the sociologist Charles Perrow introduced the idea that, for some types of industries, accidents have to be considered normal events rather than exceptional ones. Perrow describes industrial domains in terms of two qualities: complexity and coupling. The result of his classification is that systems could be either "linear or complex" and "loosely or tightly" coupled.

The complexity dimension, for Perrow means the degree of "baffling, hidden interactions" that have not been anticipated in the design and hold the potential to "jump" from one subsystem to another (Perrow, 1984).

The coupling dimension accounts for the amount of slack or buffer that is embedded in the organisation. Tightly coupled systems have no buffer available to absorb and reduce the propagation of disturbances and failures within the system. In other words, what happens to a component of the system affects directly other parts of the system. On the other hand, a loosely coupled system, hit by a perturbation, has the possibility to manage, recover and control the situation.

In 1984, Perrow classified some of socio-technical systems according to their degree of coupling and complexity. The result of his classification is presented in the following figure (Figure 3).

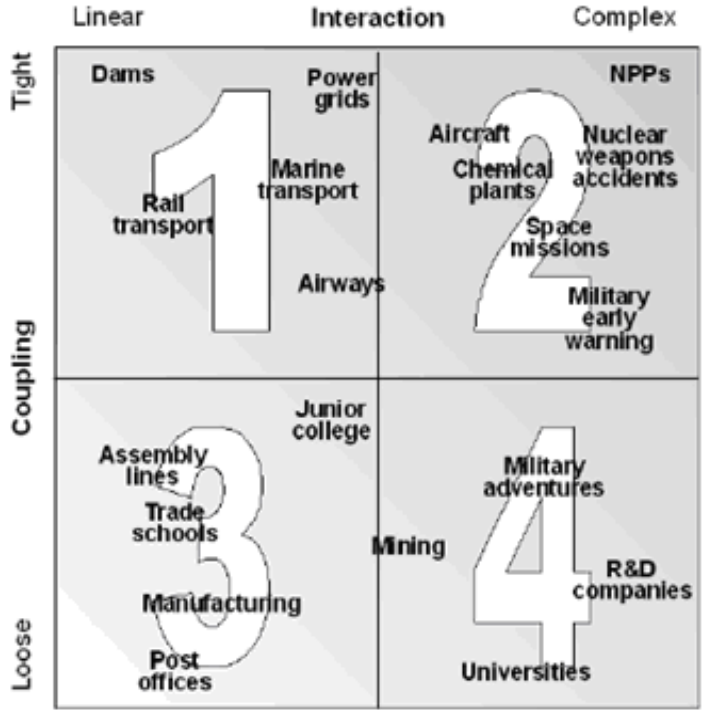


Figure 3: Distribution of socio-technical systems (Adapted from Perrow, 1984)

The approach followed by the author leads to the acknowledgement that, for certain industries and organisations accidents should not be considered as exceptional, but rather as normal in the sense that they are inevitable. For industrial systems like nuclear power plants, air traffic management, oil drilling platforms etc. it is very unlikely that a major accident is produced by an isolated technical or human failure. It is more likely that the combination of several failures (or even in the case of absence of failures) within the systems could generate accidents.

4.2 Resilience Engineering

The need to further develop theories and models to improve industrial safety is not related to the occurrence of a major industrial accident (as it was for the other safety ages), but rather to the recognition of the inadequacy of the available tools to predict accidents and, in more general terms, to manage organisational safety (Dekker, 2006). In October 2004 a group of safety scientists and safety practitioners held a symposium to discuss and develop the ideas of Resilience Engineering, i.e. ideas about an alternative approach to improve system safety. The motivation behind the development of Resilience Engineering is the need to find innovative ways to deal with risks in socio-technical systems that are more and more complex and tightly coupled (according to Perrow's definition of complexity and coupling previously mentioned), in a world where safety and productivity can no longer be disjunct.
There is a consensus about the newly born concept of Resilience Engineering as well as a common (but perhaps imprecise) understanding of what it is.

4.2.1 Resilience: multiple definitions on a common base

The term Resilience has a long tradition in many domains (physics, ecology, economy, psychology etc.) where it has generally been used to describe the characteristic or the ability of something to absorb blows, to deal with disruptions and stress, and to regain its original functional features. In the safety domain, the term has been used since 1993 when Foster defined it as "*an ability to accommodate change without a catastrophic failure*". It is not until 2004 that the term Resilience, in the safety literature, has been associated to the term Engineering with the idea that something could and should be done in an organisation to improve its *resilience*.

Since then, a proliferation of definitions for Resilience have appeared. The importance of having a detailed definition of what is meant by Resilience is the same as that which has been presented concerning safety: models, methods and indicators are developed in accordance to the definition. The definition sets the boundaries for what will be considered and what will be neglected and sets a coherent line to transfer theoretical concepts into practice.

The following three definitions represent how Resilience is differently understood by the research community:

1. The characteristic of managing the organisation's activities to anticipate and circumvent threats to its existence and primary goals (Hale & Heijer, 2006);
2. The system capability to prevent or adapt to changing conditions in order to preserve its control over a system property (Leveson et al. 2006);
3. The intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances, so that it can sustain required operations under both expected and unexpected conditions. (Hollnagel, 2010).

The Hale & Heijer definition refers to the ability the organisation must have to manage the conflict between safety efforts and production efforts and it is focused on the possible drift in the safe margins of operations. Leveson, in the development of the STAMP method, hints at the problem of loss of control that could happen in the attempt to adapt to fluctuating conditions. Hollnagel highlights the organisation's need for adjustments if normal functioning has to be guaranteed.

Reviews of the Resilience Engineering literature (Hollnagel, Woods & Leveson, 2006; Hollnagel, Nemeth & Dekker, 2008; Rigaud, 2008; SINTEF, 2009) supports the identification of three premises for Resilience Engineering:

1. Safety can not be separated from business;
2. Safety is a question of being in control and therefore requires a proactive as well as a reactive attitude;
3. Safety requires local adjustments.

4.2.2 Safety cannot be separated from business

The consequences of separating safety from business have already been mentioned. To summarise the adoption of an approach that considers these two aspects as two sides of the same coin resolves:

1. The problem of conflicting resources within the organisation;

2. The problem of having at our disposal only a limited number of events for organisational learning;
3. The problem of being stuck in a model of the negative.

4.2.3 Safety as a control issue (proactivity and reactivity)

To be effective and efficient, safety management cannot be based solely on hindsight, error tabulation, and failure probabilities. This point highlights the control problems that arise from the attempt to steer safety, by exclusively looking at what has happened in the past, or waiting for problems to emerge, before finding solutions. A proactive safety management approach will instead be able to anticipate risks, to eliminate some of them (not all risks can be predicted and therefore eliminated) and to create the conditions to cope with disturbances in an effective manner.

4.2.4 Safety requires local adjustments

The third premise of Resilience Engineering, concerns the need that socio-technical systems have for local adjustments to support their core business and therefore safety. This premise requires a thorough discussion, since it implies a further set of points to be acknowledged, and it has major implications for the development of this work.

Intractability of socio-technical systems. Since 1984, with Perrow's work on normal accidents, the complexity of some types of socio-technical systems has been acknowledged. This notion has been revised by Hollnagel (2008) and the notion of complexity substituted by the notion of intractability. An intractable socio-technical system is characterised by high complicacy (elaborate and detailed description), by low comprehensibility (principles of functioning not completely known) and by low stability (rapidly changes). Fabre & Macchi (2009) identified a more detailed list of characteristics (e.g. proximate production steps, low feedback quality, indirect information sources etc.) for intractable systems. These features imply that it is impossible to identify all potential working scenarios or working conditions that, consequently, are underspecified.

Underspecification of performance conditions. The above mentioned characteristics of intractable socio-technical systems result in the impossibility of specifying work operations exhaustively in advance, as organisations (as well as the people in them) are in a state of constant flux. The need for humans to perform efficiently in underspecified conditions requires their performance to be locally adjusted to current circumstances. Adjustments take place continually even in the highly standardised and proceduralised socio-technical systems like the nuclear industry, the army, the aviation maintenance etc. (Bourrier, 1999, Snook, 2000, McDonald 2001). Since adjustments take place with limited resources and time they are inevitably approximate.

Duality of performance variability. Approximate adjustments result in performance variability, i.e. human performance will vary to match current conditions. Due to the intractable nature of socio-technical systems, performance variability is not only an inevitable phenomenon, but it also constitutes an asset for the organisation. The impossibility of conceiving rules and procedures for every potential situation, shows how human performance variability represents normally, a source of success. For example, McDonald (2006) argues that operators, in the aviation maintenance domain, do not follow procedures routinely, but they adjust their performance in a better, quicker, safer way with respect to following the manual to the letter. The same deviations from norms and procedures can sometimes (hopefully rarely) result in incidents or accidents.

Accidents as emergent phenomena. Modern socio-technical systems are designed so that a single failure does not result in an accident (barriers implementation, redundancy of systems etc. serve this purpose). But their intractability and the required performance variability make possible the occurrence of accidents emerging from unexpected combinations of performance variability. This emergent nature of accidents is not addressed by traditional safety assessment methods, and it requires the adoption of methods able to account for performance variability, and the way it may combine in unexpected manners.

4.3 Implications of choosing a theory

This research recognises the potential advantages of Resilience Engineering in improving safety, and particularly safety assessment practices, in complex industrial systems. As highlighted in Section 3, to perform safety assessment it is necessary to apply a method which is coherent with a safety definition and with its theoretical assumptions. Thus, a Resilience Engineering safety assessment method has to satisfy the following requirements:

1. Resilience Engineering requires the adoption of a systemic safety assessment method. The scope of safety analysis can not be constrained to a specific part of the socio-technical system, but it has to consider a larger picture where the organisation is considered as a whole rather than as an assembly of components.
2. Resilience Engineering requires a method able to model the normal functioning of the socio-technical system. As presented above, most of the methods are focused on the possibility of failures and accidents. But in a Resilience Engineering perspective, normal system functioning is considered as the source for both success and failure.
3. Resilience Engineering also requires a method that looks at safety and accidents as emergent phenomena that are the result of the normal functioning of the socio-technical system. This fact that was somewhat recognised during the age of Safety Management (e.g. Normal Accident Theory, Normal Deviations, Drift into Failures) has never been exploited in the development of a safety assessment method.
4. Resilience Engineering requires a method able to take into consideration human performance, not in a nominal and standardised manner, but rather in a way that can describe performance variability as the expression of the local adjustments humans make in their daily work. In this respect, it is necessary to acknowledge the positive contribution to safety that humans bring to the organisation.

Conclusion

The need for a safe Air Traffic Management system is evident. ATM, considered as a socio-technical system, is becoming and, because of the anticipated reorganisation at European level, will become more and more complex. The complexity is due to the necessity of meeting environmental demands, and therefore to have advanced technologies to support human activities in an uncertain dynamic environment. Traditionally, the systematic identification of hazards and risks has been based on a decomposition of systems and an estimation of their failures probabilities. This approach, perfectly appropriate to systems which can be specified, is inadequate for socio-technical systems like ATM. This inadequacy is the result of the underspecification that characterises intractable dynamic socio-technical systems. EUROCONTROL (2009) acknowledges that a second inadequacy of traditional safety assessment methods is the failure based approach that characterises them.

Despite the different foci adopted during the evolution of theories and models, the main common concern was to find the unreliable, weak and problem-generating component of socio-technical systems, and to fix it. The approaches were, in other terms, looking only at the dark side of organisational functioning, i.e. they were exclusively interested in negative outcomes.

In agreement with Perrow's notion of Normal Accidents, the Resilience Engineering approach uses the understanding of normal performance as a premise to explain that accidents emerge from normal system performance, rather than resulting from technical, human or organisational failures.

The perspective shift introduced by Resilience Engineering requires a set of theoretical assumptions. When adopted, they guide the development of innovative safety assessment methods that overcome the limitations of those available. These assumptions could be summarised as follows:

1. Safety and core business are two sides of the same coin;
2. Understanding normal functioning is needed to improve safety;

3. Socio-technical systems are intractable and therefore performance conditions underspecified;
4. Local adjustments are necessary to ensure system functioning;
5. Local adjustments imply human performance is variable.

To ensure Air Traffic Management safety,we must renounce the optimistic attempt to base safety assessment on high-level, abstract representation of the socio-technical system (as suggested by EUROCONTROL Logical Model) and instead to represent, in the most realistic possible way, its actual normal functioning. Dealing with complex underspecified systems represents a difficult safety challenge. To improve system safety it is necessary to understand and to manage performance variability. Understanding the reasons for performance variability is the precondition for its management. The reasons for performance are addressed in the next chapter and the Functional Resonance Analysis Method is presented as a safety assessment method aiming at its modelling.

Page intentionally left blank

Chapter 2: Managing Performance Variability to Improve System Safety

Page intentionally left blank

Résumé du Chapitre 2

Les caractéristiques majeures (présentées au Chapitre 1) du système de gestion du trafic aérien produisent leurs propres sous-spécifications. L'estimation de la sécurité de cette typologie de systèmes socio-techniques nécessite la reconnaissance de la présence de la variabilité de performance et son rôle dans le fonctionnement du système. L'objectif d'améliorer la sécurité en limitant les performances, et donc de réduire la probabilité d'écarts par rapport aux règles et procédures, ne pourrait être atteint, car il suppose une classification bimodale de la performance: correcte ou incorrecte. Mais la réalité est différente. La performance de systèmes socio-techniques complexes doit être variable afin de maintenir le fonctionnement du système. De toute évidence la variabilité de performance n'est pas seulement un atout pour le fonctionnement du système, elle pourrait en même temps représenter une atteinte à la sécurité lorsqu'elle se déroule de manière indésirable ou inattendue.

La perspective de *Resilience Engineering* – Ingénierie de la Résilience, souligne le rôle de la variabilité de la performance pour assurer le fonctionnement normal des systèmes socio-techniques. Le fait de décrire la performance en termes de défaillances, dysfonctionnements et erreurs humaines est manifestement insuffisant pour représenter une performance qui varie en fonction des possibilités et des contraintes pour être aussi efficace que possible. Ce chapitre présente une approche différente pour expliquer une performance qui satisfasse à la fois la nécessité d'exploiter des possibilités (par exemple, augmenter l'efficacité, le temps sûr, réduire la charge de travail, etc.) et de faire face aux contraintes (par exemple, résoudre des problèmes inattendus, la pression de production, la pression du temps, etc.). Le compromis Efficacité-Rigueur est présenté comme un cadre de discussion de la variabilité de la performance, et la *Functional Resonance Analysis Method* – FRAM, en français Méthode d'Analyse de Résonance Fonctionnelle- est introduite comme la méthode adéquate pour l'estimation de la sécurité.

Introduction

The prominent features (presented in Chapter 1) of an Air Traffic Management system create its underspecification. Safety assessment for this typology of socio-technical systems requires us to acknowledge the presence of performance variability and its role in system functioning. The attempt to improve safety by constraining performance, and therefore reducing the probability of deviation from rules and procedures, cannot be achieved, since it assumes a bimodal classification of performance; correct or incorrect. But reality is different. Complex socio-technical systems performance has to be variable to maintain system functioning. Obviously performance variability is not only an asset for system functioning, it could at the same time represent an obstacle to safety when it combines in unwanted or unexpected ways.

The Resilience Engineering perspective stresses the role of performance variability to ensure the normal functioning of socio-technical systems. Describing performance in terms of failures, malfunctions and human errors is clearly an inadequate way to represent performance that varies according to opportunities and constraints in order to be as efficient as possible. This chapter introduces a different approach to explain performance that satisfies both the need to exploit opportunities (e.g. increase efficiency, save time, reduce workload etc.) and to deal with constraints (e.g. solve unexpected problems, production pressure, time pressure etc.). The Efficiency-Thoroughness Trade-Off is presented as a framework to discuss performance variability and the Functional Resonance Analysis Method is introduced as an adequate safety assessment method.

1 Reasons for performance variability

To prevent accidents emerging from unwanted combinations of performance variability it is necessary first to understand what the reasons are. Humans are the main source of performance variability in socio-technical systems. Technology is designed, built and maintained to be as reliable as possible. Current technological progress produces extremely reliable systems in which variability might almost be forgotten. That does not mean that technology cannot fail, indeed it does and often

accident analysis also identifies technological failures. It only means that technology performs in a bimodal way which means "it works" or "it does not work". Normally it does work, it rarely fails and once this happens, humans have to cope with a degraded situation and adjust to it. Thus, describing performance variability, inevitably, is mainly a matter of human performance description.

Scientific studies of human performance at work have a tradition as long as the history of industry. Back to the first industrial revolution, physiological factors influencing performance variability have been identified. Since then the influence of several other factors has been identified.

It is possible to distinguish five classes of reasons for performance variability related to human, social or contextual conditions:

Physiological and/or fundamental Psychological factors This class of factors have an influence on perception and vigilance. They have been considered since the very beginning of Human Reliability Assessment methods (HRA 1st generation). Their effect on human reliability has been studied in Ergonomics and Human Factors in the analysis of human behaviour and by the development of cognitive models to estimate response times and human error probabilities.

Higher level Psychological factors. Ingenuity, creativity, adaptability etc. and their effect on human performance have been investigated by Human Resources management and selection studies. This kind of high level psychological factor, as noted by Hale & Hovden (1987) has been categorised for safety purposes as individual accident proneness. Incidents and accidents are more likely to occur to some people. To improve safety it is necessary to choose the right people.

Contextual factors. The second generation HRA methods overcame the limitations of the first generation by including the effect of contextual factors in human reliability analysis. Extensive lists of contextual factors have been compiled (e.g. Common Performance Conditions in CREAM, Error Forcing Conditions in ATHEANA, Configuration Importante de la Conduite Accidentelle in MERMOS) to account for the detrimental effect context may have on human reliability.

Social factors. Meeting personal or social expectations, and complying with informal work standards, are examples of how organisational culture influences human performance at work. Advanced models are developed and applied to improve and predict an organisation's safety culture. Safe behaviours, weak signals awareness, formal commitment to safety etc. are all expressions of a good safety culture within an organisation. An organisation is safe when there is a good safety culture.

Systemic factors. The need to stretch resources in order to meet performance demands or the need to substitute goals when dealing with unpredictable events are reasons why performance variability is influenced by systemic factors. From a systemic perspective, performance variability is due to local adjustments that are made to meet performance demands. The stability of the operative process as well as the minimum execution time, are *ideal* models that encumber our representation and understanding of the real world, rather than supporting us in understanding it (Musatti, 1971). Procedures and rules are designed to define performance under estimated conditions and they can be considered as resources for experienced workers. Referring to the concept of *frame* (Minsky, 1986), procedures can be seen as mental structures lacking their final parts, which are to be built in relation to actual conditions. In order to assure system safety, operators are taught not only procedures, but also how to use them, i.e. to locally adjust their performance to actual conditions. The human contribution, in terms of intelligent adaptations, to system reliability (Oddone, Re & Briante, 1981) is a matter of fact in most socio-technical systems. Experienced workers constantly assess upcoming situations and anticipate future actions both in low technological tasks, (e.g. party-structures installers or traffic wardens Lacomblez et al. 2007), and in a highly automated context, (e.g. air traffic control, De Terssac, 1992).When variability becomes a constitutive part of the work, actions should be seen *as part* of the context, rather than as a context's dependent variable (Bateson, 1979).

Overcoming the concept of standardised performance, potentially affected by contextual factors, this thesis focuses on the normal system functioning. Analysis of the normal functioning of the system includes the analysis of local adjustments that

are performed to maintain the same level of system functioning. As highlighted by McDonald (2006), the local adjustments result from the tension to respect planning and procedures, and the requirement of performance variability to meet the demands from the operational environment. Hollnagel (2004; 2009) describes this tension in terms of a constant trade-off between the need for efficiency and the need for thoroughness. The Efficiency – Thoroughness Trade Off principle, described in the following section, constitutes a useful framework to understand performance variability induced by systemic factors.

1.1 Efficiency-Thoroughness Trade Off (ETTO)

Human decision making and human behaviour are described by the ETTO principle as resulting from the balance between two antagonising needs: efficiency and thoroughness. Introduced by Hollnagel (2004; 2009) the ETTO principle accounts for the heuristics humans normally apply to achieve their objectives.

Efficiency refers to the resources and to the efforts required to achieve the desired objective. The less resources are used and the less effort made the more efficiency rises. Hollnagel (2009) mentions among possible resources time, materials, manpower, money. Psychological and physical efforts (e.g. workload and fatigue) are taken into account in the evaluation of efficiency. Thoroughness refers to the execution of an activity, if and only if, its preconditions are satisfied and if it can be assured that the desired objective will be obtained under the desired execution conditions.

From these elementary definitions of Efficiency and Thoroughness it is evident that it is impossible for humans to maximise both of them at the same time. The increase in efficiency inevitably creates a decrease in thoroughness, and vice-versa. Humans have therefore to choose, according to the context they are dealing with, the most appropriate balance between Efficiency and Thoroughness. Such balance is found by tacking into account:

- A subjective evaluation of available resources and time;
- Individual personality traits;

- Social habits, practices, safety culture etc.;
- Social and organisational pressure;
- The tendency to save time and resources in case of unexpected events.

Thus, the classical modelling (e.g. Rasmussen, 1986, Reason, 1990, Hollnagel, 1993, Cacciabue, 2004) of human behaviour as a rational information-based decision making process is not able to account for the Efficiency – Thoroughness trades-off.

The underlying assumption of the analogy of Information Processing System is that humans are ideal decision makers (the *homo economicus*). Despite the evidence that, in reality, humans are not rational in their behaviour, the analogy has been widely used in the development of cognitive modelling. The initial concept of absolute rationality has been revised over the years with the introduction of the idea of limited or bounded rationality, but the central point – that human behaviour can be explained in terms of some kind of principle – still exists. The thorny issue of describing human behaviour realistically and not with an unnatural rational flavour, can be addressed by taking into account the time pressure on almost every human activity. The rational paradigm considers that humans have all the information and all the time needed to take a decision that will maximise its benefit. The limited rationality paradigm assumes that humans do not have the cognitive capability to process all the available information prior to making the best choice. From an ETTO perspective, three typologies of explanations can account for such limitations.

Sacrificing Decision Making: Simon's (1955) theory on *satisficing* decision making (understood as the attempt to achieve a minimum level of a particular variable when making a decision) has been revised with the introduction of the *sacrificing* decision making. While the satisficing decision maker is unable to maximise a decision's benefit due to his/her bounded rationality (Hollnagel, 2009), the sacrificing decision maker is unable to maximise the benefit due to the complexity or intractability of the working environment (cf. Perrow's characterisation of socio-technical systems in Chapter 1). The intractable nature of complex socio-technical systems, induces humans to make decisions and implement actions even if they do

not have a complete understanding of the situation, the potential consequences of their actions and they have not cognitively explored all the available alternatives. The achievement of such a complete picture (supposing it is something achievable) will take so much time and effort that operators will not have enough time to implement the decision in corresponding actions. This is the reason why, in real working settings, people tend to be efficient rather than thorough. In this manner, they do something, reasonably precise and correct, rather than spend all their time evaluating the best possible option. Even if this attitude is proven to be valuable, it may sometimes lead to unwanted situations (e.g. sacrificing decisions has been used to explain the notion of Drift into failure; Rasmussen, 1997).

Mental models and schema: people use mental models and schema to simplify their interactions with the world. Johnson-Laird's theory (1983) of mental models explains how a person holds a mental working model of the phenomenon he/she interacts with. To encompass the scope required to support the human understanding of a situation, mental models must be simpler than the real-world phenomenon they represent. In this way a person can base his/her understanding on a check of salient characteristics rather than checking every detail. Mental models therefore provide an effective way to cope with the complexity of the world based on knowledge and experience of already encountered situations. Problems arise if a situation is misjudged and a response plan is implemented for a situation which is not as it was thought. An important contribution of the mental models theory is the acknowledgement that people's reasoning and behaviour is primarily influenced by the content-relatedness and form of the information presented rather than a logic reasoning.

Heuristics and rules: to reduce the complexity of tasks so that objectives are achieved, humans rely on the use of heuristics. It is possible to differentiate between heuristics to support the recognition of situations and heuristics to support the judgement of uncertainty. The first group of heuristics includes the two primitives of cognition introduced by Reason (1990) *similarity matching* and *frequency gambling*. The two primitives, (like mental models), serve to support the recognition of something that looks similar to something already known (similarity matching), and

something that happened frequently enough in the past to be expected to happen frequently again in the future (frequency gambling). The second group of heuristics is useful when uncertainty has to be judged prior to a decision. In such a case heuristics serve as short-cuts to discriminate among several potential options. Tversky &Kahneman (1974) describe three heuristics commonly used by people to deal with uncertainty. The first heuristic (*Representativeness*) concerns the assessment of the probability of a hypothesis by considering how much the hypothesis resembles available data (e.g. Probability that A is generated by B is evaluated by the degree of similarity between A and B). The heuristic of *Availability* concerns the assessment of the frequency of an event based on how easily an example can be brought to mind. The third heuristic (*Anchoring and adjustment*) concerns the assessment of the probability of an event starting from an implicit reference point (the "anchor") and making adjustments to it to reach the final estimate. The ultimate scope of heuristics is to improve efficiency (save time, save resources, save effort) while maintaining an acceptable level of thoroughness (relying on mechanisms proved to be usually correct).

From the ETTO perspective the understanding of human performance requires the acknowledgement that humans take sacrificing decisions, use mental models and apply heuristics. This leads to the definition of a set of rules observable in a working context. Hollnagel (2009) differentiates between *Work related* (e.g. it is normally OK, there is no need to check; it has been checked earlier, so no need to check it again; doing it this way it is much quicker), *Psychological* (e.g. different scanning styles) and *Organisational* (e.g. reduce unnecessary costs; report and be good) ETTO rules. These rules do not pretend to be exhaustive, they rather represent a set of characteristics that describe how and why the actual behaviour could differ from what would be considered rational and planned.

1.2 Resilience Engineering and ETTO

In the last section of Chapter 1 the Resilience Engineering discussion highlighted the importance of acknowledging the following:

1. Since safety and core business are strongly coupled models and methods must be able to account for the normal performance of the system. Normal performance has to be understood as a source of both successes and failures;
2. Industrial safety requires being able not only to anticipate and reduce risks, but to create the conditions for the organisation to cope with normal disturbances. It therefore requires both a reactive and proactive attitude;
3. The functioning of industrial systems is underpinned by humans' ability to locally adjust their behaviour to meet performance demands. The need for adjustments is due to the nature of industrial systems and implies that performance has to be variable.

In this framework, variability has to be understood as the expression of the influence of systemic factors on normal performance. The other four reasons (Physiological, Psychological, Contextual and Social) for performance variability are obviously important, and safety improvements are achievable only if these reasons are taken into consideration. But they do not account for the performance variability due to local adjustments to meet performance demands.

Performance is affected at the same time by what is happening at the sharp-end (normally the *foreground* of the analysis) and by what is happening at the blunt-end (those *background* parts of the socio-technical system normally external to the focus of analysis).

The Functional Resonance Analysis Method (FRAM) (Hollnagel, 2004) proposes a methodology to identify and assess performance variability. Based on a functional modelling, the FRAM shares Resilience Engineering assumptions about the complex socio-technical systems underspecification and recognises in it the need for local adjustments.

2 Functional Resonance Analysis Method (FRAM)

Introduced by Hollnagel (2004), as an accident investigation and safety assessment method the Functional Resonance Analysis Method (FRAM) is based on four principles:

1. The principle of equivalence of success and failures: Failures do not stand for a breakdown or malfunctioning of normal system functions, but rather represent the downside of the adaptations necessary to cope with the underspecification that is a consequence of real world complexity. Individuals and organisations must always adjust their performance to the current conditions; and because resources and time are finite it is inevitable that such adjustments are approximate. Success is a consequence of the ability of groups, individuals, and organisations to anticipate the changing shape of risk before damage occurs; failure is simply the temporary or permanent absence of that.

2. The principle of approximate adjustments: As already discussed, since operating conditions usually are underspecified and dynamically changing in a more or less orderly manner, humans have to find effective ways of overcoming problems at work, and this capability is crucial for safety. Indeed, if humans always resorted to following rules and procedures rigidly, in cases of unexpected events, the number of accidents and incidents would be much larger. Human performance can therefore at the same time both enhance and detract from system safety. Because resources and time are finite, it is inevitable that such human adjustments are approximate. If inadequate adjustments coincide and combine to create an overall instability this can become the reason why things, sometimes, go wrong.

3. The principle of emergence: The variability of normal performance is rarely large enough in itself to be the cause of an accident or even to constitute a malfunction. But the variability of multiple functions may combine in unexpected ways, leading to consequences that are disproportionally large, and hence produce a non-linear effect. Both failures and normal performance are emergent rather than resultant phenomena, because neither can be attributed to, or explained, only by referring to the functions or malfunctions of specific components or parts. Socio-technical systems are intractable because they change and develop in response to conditions and demands. It

is therefore impossible to describe all the couplings in the system, hence impossible to anticipate more than the most regular events.

4. The principle of functional resonance: FRAM replaces the traditional cause-effect relation by the principle of resonance. This means that the variability of a number of functions every now and then may resonate, i.e., reinforce each other and thereby cause the variability of one function to exceed normal limits. (The outcome may, of course, be advantageous as well as detrimental, although the study of safety has naturally focused on the latter.) The consequences may spread through tight couplings rather than via identifiable and enumerable cause-effect links, e.g., as described by the Small World Phenomenon (Travers & Milgram, 1969). The resonance analogy emphasises that this is a dynamic phenomenon, hence not attributable to a simple combination of causal links. This principle makes it possible to capture the real dynamics of the system's functioning (Woltjer & Hollnagel, 2007), hence to identify emergent system properties that cannot be understood if the system is decomposed in isolated components.

In the book *Barriers and Accident Prevention* (Hollnagel, 2004) the method has been presented and outlined. In its present form, the method comprises the following five steps.

1. Definition of the purpose of the analysis;
2. Identification and description of system functions;
3. Assessment and evaluation of the potential variability;
4. Identification of functional resonance;
5. Identification of effective countermeasures to be introduced in the system.

In the following sections an Air Traffic Management related example is presented. To illustrate the method the FRAM has been applied to model the *Over-flight control* activity, i.e. that part of Air Traffic Controllers work that serves to ensure the safe passage of aircraft through a sector (or a set of sectors). The Over-flight example will

also be used in Chapter 4 as basis for an evaluation of the performance variability assessment methodology.

2.1 Define the Purpose of the Analysis

The first step is the definition of the purpose of the analysis. As already mentioned, FRAM can be used both as an accident investigation method and as a safety assessment method. Although the major steps of the method are the same, some details needed for accident investigation will differ from the details needed for a safety assessment. For example, for something that has happened, the performance conditions will be known. Whereas for something that may happen in the future, the likely performance conditions must be estimated. It is therefore necessary to clearly state which of the two aspects of safety management it is going to be used for. In this case the focus is safety assessment and in this respect the FRAM has been applied.

2.2 Identification and Description of System Functions

The identification of the system takes place through the following steps.

- The first step of system identification is the choice of the overall functionality or performance that will be the focus of the analysis, i.e. what will be the *foreground* of the analysis;
- The second step of system identification is the determination of the system's boundaries. Since the FRAM considers functions rather than structures (or objects), there are not "natural" boundaries, such as those resulting from the physical characteristics of humans and machines or the physical delineation of an industrial plant;
- The third step of system identification is to choose a level of detail, or degree of resolution, for the function description.

2.2.1 System functionality and system's boundaries definition

A precondition for the use of the FRAM for safety assessment is the definition of the overall functionality and boundaries of the socio-technical system to be analysed.

The model of the *Over-flight control* has been focused on the normal activity of executive controllers (Macchi, Hollnagel & Leonhardt, 2008). The functions of executive controllers, have therefore been modelled with the FRAM. Other functions, constituting the interfaces of executive controllers have also been included in the system to be modelled.

The latter functions refer to:

1. The technical systems that support the controller activity;
2. The pilots with which he/she communicates; and
3. The planner controller.

Since the foreground of the system in analysis is constituted by the executive controllers' activities, the model only considers the functions of interfaces as the background source of inputs for foreground functions, or as receiver of the outputs produced by them. In Figure 4, the system, that has been modelled, is represented.

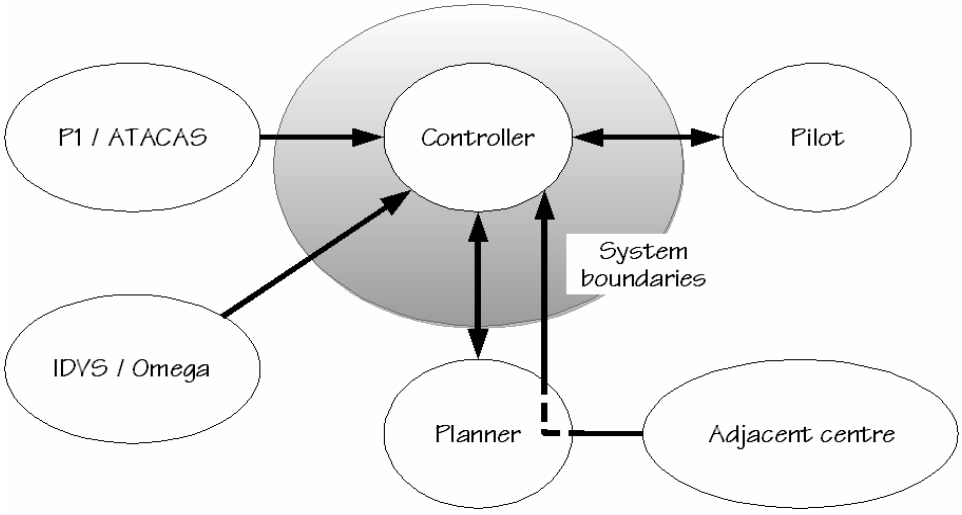


Figure 4: System functionality

2.2.2 Function identification

Once the focus and level of the modelling have been determined, the functions of the socio-technical system have to be identified. A function is an activity of the socio-technical system towards a specific object. Reiman (2007) refers to Leontiev (1978) distinction between function and task. A function is governed by the motive to ensure the functioning of the overall socio-technical system, which, as scope, is wider than the mere accomplishment of the action or task.

The principle that guides the identification of functions is the need to achieve a description of the normal activities performed by the socio-technical system being analysed. Figure 5 illustrates the graphical representation of a function in the FRAM.

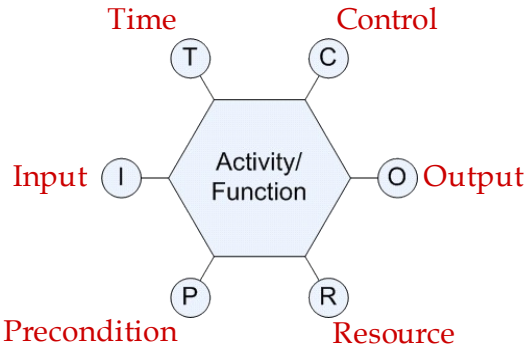


Figure 5: FRAM function

It is therefore necessary that the functions are described without any judgement about the possible quality or correctness of their outputs, e.g., whether they represent a possible risk. To proceed to the identification of the functions it is often useful to start from a task analysis or from the official documents of the interested organisation, e.g., procedures. The information gathered in this way needs to be integrated with the contribution of the domain experts.

These functions usually represent the sharp end activities of the socio-technical systems and they normally constitute the set of *foreground* functions.

For the *Over-flight control* example, ten functions have been identified (Table_ 1). The identified functions are intended to be sufficient to account for and describe the normal activity performed at the sharp-end of an Air Traffic Management control centre.

Table_ 1: Functions in the Over flight control activity

1	Monitoring
2	Planning
3	Provide ATC clearance to pilot
4	Strip marking
5	Coordination
6	Update flight data processing system
7	Provide meteorological data to controller (IDVS/Omega system)
8	Provide flight and radar data to controller (P1/ATCAS)
9	Controller pilot communication
10	Sector-sector communication

2.2.3 Function description

Following the function identification the safety assessment proceeds by characterising each function in terms of six aspects, namely: Input, Output, Preconditions, Control, Time and Resources. Hollnagel (2004) defines the six aspects in the following terms:

1. Input (I): that which the function processes or transforms or that which starts the function;
2. Output (O): that which is the result of the function, either a specific output or product, or a state change;
3. Preconditions (P): conditions that must be exist before a function can be executed;
4. Resources (R): that which the function needs or consumes to produce the output;
5. Time (T): temporal constraints affecting the function (with regard to starting time, finishing time, or duration); and
6. Control (C): how the function is monitored or controlled.

The description of each function is made using a simple table (Figure 6) which then becomes the basis for the further analysis.

Function X	
Input	
Output	
Time	
Control	
Precondition	
Resource	

Figure 6: Function description

Table_ 2 illustrates the description for the **Provide ATC clearance to pilot** function. For the purposes of the modelling it is not necessary to distinguish between the different clearances that this function could provide. It is possible to use a single function to provide several different outputs (in this case clearances) because it is the content of the clearances that changes (i.e. regulate speed, heading change etc.) while the function itself does not change.

The description of the six aspects is generally straightforward. As Table_ 2 shows, not all aspects need to be filled in; with the exception of *Input* and *Output,* the aspects should only be filled in if they clearly are relevant to the function in

question. As far as the *Preconditions* aspect is concerned, a function may often have a number of possible preconditions that must be considered either together or in combination. In Table_ 2 this is done by means of conjunctions (*and*) and disjunctions (*or*).

Table_ 2:Provide ATC clearance to pilot function description

	Provide ATC clearance to pilot
Input	Clearance plan
Output	Clearance provided = [regulate speed; heading change; climb; descend; adjust vertical rate; intermediate level off; holding instruction]
Time	-----
Control	Clearance procedures Letter of agreement RT standards Warning by safety net
Preconditions	Aircraft identified *and* Radio contact established *and* Sector capacity = [sector capacity satisfied] *and* Flight position = [entering the sector] *or* Request from pilot = [regulate speed; heading change; climb; descend] *or* Request from next sector = [flight level; speed; route; heading; flight not accepted]
Resources	Situation data display equipment Touch input device Flight progress strip RT equipment

2.2.4 FRAM model

The description of system's functions achieved in the previous step constitutes the FRAM model of the system. A FRAM model differs from classical models, such as fault trees and event trees, because of the fact that the model is not the diagram or the flowchart, but the verbal description of the functions, including the six aspects. The fact that a FRAM model does not include the actual links between the elements makes it possible for analysts to generate a set of possible instantiations to show the effect that the actual working conditions can have on the performance of the system. Classical models like fault trees and event trees show a single representation of the

system, which depicts a set of possible cause-effect relations. In the analysis, the propagation of an event is therefore constrained by the links in the diagram. In FRAM, no such constraints exist.

2.2.5 Consistency and completeness of FRAM model

As is the case for every description and model, the FRAM model has to be consistent and complete. Since the FRAM aims at the description of the couplings between functions, it is necessary to ensure that every aspect of every function is produced, as an Output, and used, as Input, Control, Precondition, Time or Resource, by functions identified and described in the model. In other terms, it is necessary to make sure that there are no "free floating" aspects in the model. This requires that description tables have to be checked for consistency.

The consistency check directly leads to the completeness check of the model. As every aspect has to be produced by a function and used, at least, by another function in the model, when the consistency check is done, then the required functions have been identified, and the FRAM model is complete.

As discussed in Chapter 2 - Section 2.2.2, the set of *foreground* functions will be checked for completeness in interaction with domain experts.

For every set of *foreground* functions it is possible to identify and describe a set of relative *background* functions. Their identification and description is based on the consistent application of check rules starting from the description of the aspects of foreground functions. A detailed description of this process is provided in Chapter 3 – Section 2.1.2

2.2.6 FRAM instantiation

When all the functions have been described, the next step is to identify the couplings between the functions. This is achieved by linking together these functions according to the description provided by the tables. The result constitutes a FRAM instantiation of the system, and is often shown graphically. Figure 7 represents the instantiation of the table-based description for the *Over-flight control* and it shows the nominal functioning system.

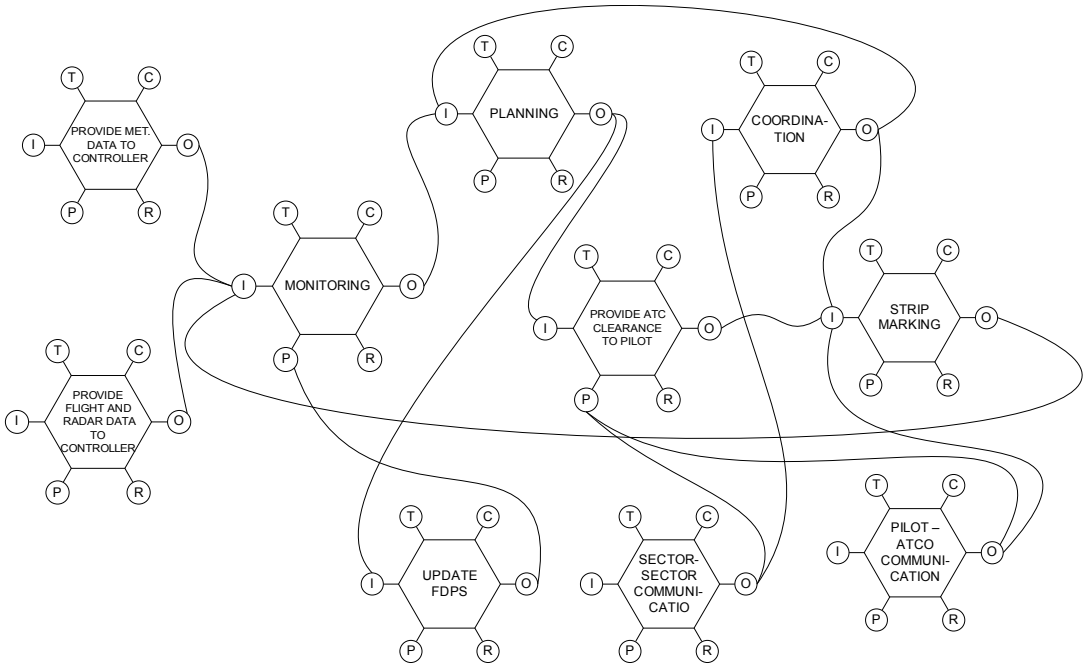


Figure 7: FRAM nominal instantiation for Over-flight scenario

This instantiation can be used as the basis for consideration of the effect of the variability of functions, and how this may create outcomes that propagate through the system. The variability of functions may also lead to unexpected couplings, as well as to expected couplings becoming dysfunctional.

In the FRAM instantiation, the links between the functions represent the dependencies between the functions as defined by the six aspects. Neither does the relative position of the functions in the graphical representation symbolise a temporal sequence, nor does ordering suggest cause-effect relations.

Conclusion

Performance variability represents an asset for modern ATM as well as for any other complex industry. The contribution provided by performance variability in filling the underspecification gaps that are due to the complexity of socio-technical systems is fundamental for the functioning of the system. Performance variability could also represent a danger to system safety when it combines in an unexpected and undesired manner. Emergent accidents, i.e. industrial accidents that happen in the absence of any major technological failure, are the result of combination of performance variability taking place throughout the system.

To improve system safety it is therefore necessary to understand performance variability, its reasons, its effects and to model its spreading through the system. In this chapter the ETTO principle has been presented as a powerful approach to describe performance variability due to systemic factors, i.e. to cope with a dynamic, unpredictable environment. In addition to the theoretical effort necessary to understand performance variability, it is also necessary to apply a safety assessment method that can model and evaluate system safety. The Functional Resonance Analysis Method is focused on the identification and reduction of emergent risks. The method, consisting of a series of five steps, requires the identification and description of system's functions to achieve a model and its instantiation. The important point in building the model is to make sure that the model is consistent and complete. As explained, consistency requires every functions' aspects to be produced and used by (at least) one function.

Performance variability, described as the result of local adjustments to meet performance demands, is affected by coupling among functions as much as by foreground and background functions. In the beginning of next chapter, the original FRAM methodology for the evaluation of performance variability is reviewed. On the basis of the theoretical discussion about the reasons for performance variability, previously presented, an improved methodology for the evaluation of performance variability is developed and detailed.

Chapter 3: Methodology for Performance Variability Evaluation

Page intentionally left blank

Résumé du Chapitre 3

Dans le chapitre précédent les deux premières étapes de la FRAM, la définition du but de l'analyse - l'enquête d'accident ou l'estimation de la sécurité- et l'identification et la description des fonctions d'un système, ont été décrites et illustrées par un exemple. Une fois ces deux étapes exécutées, le modèle FRAM est alors complet, et des instantiations potentielles peuvent être générées.

La troisième et plus importante étape de la FRAM consiste en l'estimation de la variabilité potentielle de la performance normale. Cette étape, dans la version originale de la méthode, était abordée par l'évaluation *a priori* d'un ensemble de *Common Performance Conditions* (CPC – Conditions de Performance Communes) qui désigne la possibilité de variabilité de la performance.

La première section de ce chapitre commence par un bref panorama de cette troisième étape de la FRAM. Par la suite, ses limites sont examinées.

La seconde section présente une méthodologie alternative pour estimer la variabilité de la performance normale. La méthodologie développée fait la distinction entre les variabilités de la performance de fonctions de natures différentes; cette méthodologie justifie la variabilité de la performance par l'existence de facteurs systémiques, et propose une représentation complète de la variabilité de la performance, afin que la FRAM puisse être utilisée de manière opérationnelle.

Cette méthodologie alternative sera appliquée dans une étude pratique d'estimation de la sécurité dans le Chapitre 4.

Introduction

In the previous chapter the first two steps of the FRAM were described and exemplified , i.e. the definition of the purpose of the analysis (accident investigation or safety assessment) and the identification and description of the functions of the system. Once these two steps are performed the FRAM model is complete, and potential instantiations can be generated.

The third and most important step of the FRAM consists of the assessment of the potential variability of normal performance. This step, in the original version of the method, was addressed by the *a priori* evaluation of a set of Common Performance Conditions (CPC) which indicates the likelihood of performance variability.

Section 1 of this chapter starts with a a brief overview of this approach to the third step of the FRAM. Then its limitations are discussed.

Section 2 proposes an alternative methodology to evaluate the variability of normal performance. The developed methodology differentiates between the performance variability of functions of different nature; the methodology accounts for the performance variability due to systemic factors and it proposes an aggregated representation for performance variability, so that the FRAM can be operationally use.

This alternative methodology will be applied in a practical safety assessment study in Chapter 4.

1 CPCs-based Performance Variability assessment

Since the age of Human Factors, safety assessment methods looked at the human contribution to risk in terms of error probabilities. The first generation of Human Reliability Methods (HRA) were criticised (Dougherty, 1990, Swain, 1990, Kirwan, 1994) for not considering the influence of context on human performance. Since then, the so-called second generation of HRA methods considered lists of contextual factors (e.g. Error Forcing Conditions (EFC); Common Performance Conditions (CPC); Important Configuration of Emergency Operations (CICAs- Configuration Importante de la Conduite Accidentelle) to represent the combined effect of context, plant conditions and organisational characteristics on the probability of human error.

The first FRAM version used quite the same approach. Acknowledging the importance of context, the set of Common Performance Conditions (previously used and validated in the CREAM method; (Hollnagel, 1998) was used to estimate the likelihood of performance variability. The underlying idea of the methodology was

that detrimental conditions would increase performance variability while advantageous conditions on the whole, would reduce it. Eleven Common Performance Conditions, listed below, were considered relevant: .

1. **Availability of resources.** Adequate resources are necessary for stable performance, and a lack of resources increases variability. The resources primarily comprise *personnel*, *equipment*, and *material*.
2. **Training and experience (competence).** Both *level* and *quality of training* together with the *operational experience* directly effect performance variability.
3. **Quality of communication**, both in terms of *timeliness* and *accuracy*. This refers both to the *technological aspects* (equipment, bandwidth) and the *human or social aspects*.
4. **HMI and operational support**. This refers to the human/machine interaction in general, including *interface design* and *various forms of operational support*.
5. **Availability of procedures and plans**. P*rocedures, plans* and *routine patterns of response* are used as the reference point for their routine activity.
6. **Conditions of work**. Lighting, noise, temperature, workplace design and the like.
7. **Number of goals and conflict resolution**. The *number of tasks* a person must normally attend to and the rules or principles (criteria) for conflict resolution.
8. **Available time and time pressure**. Lack of time, even if subjective, is one of the main sources for psychological stress for humans and may lead to a reduction of the quality of performance (Cox & Griffiths., 2005).
9. **Circadian rhythm and stress**, i.e., whether or not a *person is adjusted to the current time*. Lack of sleep or asynchronism can seriously disrupt performance.

10. **Team collaboration quality**. The *quality of the collaboration* among team members, including the overlap between the official and unofficial structure, *level of trust* and *general social climate*.

11. **Quality and support of the organisation**. This comprises the quality of the *roles and responsibilities of team members, safety culture, safety management systems, instructions*, of *guidelines for externally oriented activities*, and the *role of external agencies*.

According to Hollnagel (2004), Common Performance Conditions do not affect every function in the socio-technical system in the same manner. For this reason, the use of the HuMan – Technology – Organisation (MTO) framework was suggested to identify which CPC might influence which function. As example, the CPC "Circadian rhythm and stress" is likely to influence the performance of Human functions (it has no influence on Technological or Organisational ones); the CPC "Availability of resources" is likely to influence the performance of both Human and Technological functions. The complete set of matching between CPCs and MTO categories is illustrate in Figure 8.

	Functions affected		
	M	**T**	**O**
Availability of resources	X	X	
Training and experience (competence)	X		
Quality of communication	X	X	
HMI and operational support		X	
Availability of procedures and plans	X		
Conditions of work		X	X
Number of goals and conflict resolution	X		X
Available time and time pressure	X		
Circadian rhythm and stress	X		
Team collaboration quality	X		
Quality and support of the organisation			X

Figure 8: Matching MTO categories and Common Performance Conditions (adapted from Hollnagel, 2004)

To estimate the likelihood of performance variability, every function has therefore to be assigned to one of the three MTO categories. Once this assignment has been

done, the original methodology required the evaluation of CPCs on a three point : *Adequate, Inadequate* and *Unpredictable.* Figure 9 represents the likely performance variability of functions according to the evaluation of Common Performance Conditions. According to Hollnagel (2004) in presence of *Adequate* CPCs, functions have Small performance variability; in presence of *Inadequate* CPCs, functions have Noticeable – High performance variability; in presence of *Unpredictable* CPCs functions have High – Very High performance variability.

	Adequate	Inadequate	Unpredictable
Availability of resources	Small	Noticeable	High
Training and experience (competence)	Small	High	High
Quality of communication	Small	Noticeable	High
HMI and operational support	Small	Noticeable	High
Availability of procedures and plans	Small	Noticeable	High
Conditions of work	Small	Noticeable	High
Number of goals and conflict resolution	Small	High	High
Available time, time pressure	Small	High	Very high
Circadian rhythm, stress	Small	Noticeable	High
Team collaboration quality	Small	Noticeable	High
Quality and support of the organisation	Small	Noticeable	High

Figure 9: Likely performance variability as a function of Common Performance Conditions

The original description (Hollnagel, 2004) about the methodology to evaluate performance variability, stops at this stage. In order to evaluate the performance variability due to systemic factors, i.e. the performance variability due to local adjustments made to meet performance demands, the use of CPCs seems to be inadequate. The limitations of the CPCs-based methodology are detailed in the next section.

1.1 Limitations of the CPCs-based methodology

The CPCs-based methodology shown above has three main limitations.

The first and most critical limitation is related to the reasons for performance variability.

From a systemic perspective, performance variability has to be understood as the result of local adjustments made to meet performance demands and to ensure the functioning of the socio-technical system. In this situation, any list of contextual factors results to be only a place-holder for the influence of the context. Moreover, the variability resulting from the couplings and interactions among functions cannot be represented through the use of CPC.

The second limitation is related to the heterogeneity of functions performed in a socio-technical system and that can be modelled with the FRAM. As proposed by Hollnagel (2004), functions performed in a socio-technical system can be assigned to one of the three MTO categories. As explained, the use of this reference framework was used to identify which CPC was likely to impact which function. Anyway, the CPCs-based methodology does not differentiate between the likelihood performance variability expressed by Human or Technological or Organisational functions. To be improved, the methodology must be able to address the performance variability showed by heterogeneous functions composing the socio-technical system. This means differentiate between the performance variability of Human, Technological and Organisational functions.

The third identified limitation is related to the practical application of the methodology for safety assessment. In order to apply the method it is necessary to evaluate how much each function is potentially variable. Thus a single representation for performance variability is necessary. The way in which the eleven CPC scores can be aggregated into a single performance variability value, once the Common Performance Conditions have been singularly evaluated, it is not clearly described.

These three limitations could be summarised as follows:

1. CPCs-based methodology does not represent variability due to local adjustments;s
2. CPCs-based methodology does not consider the heterogeneity of functions in evaluating their performance variability;

3. CPCs-based methodology does not describe how an aggregated representation for performance variability can be achieved.

The contribution of this thesis to the Functional Resonance Analysis Method is therefore focussed on tackling these three points.

2 Improved methodology for performance variability evaluation

The objective to achieve an improved methodology for the evaluation of performance variability within the Functional Resonance Analysis Method, requires a solution to the limitations illustrated above. The improved methodology has to:

1. Differentiate between the performance variability of heterogeneous functions performed in a socio-technical system;
2. Represent the performance variability due to local adjustments, i.e. performance variability induced by systemic factors;
3. Achieve an aggregated representation for performance variability.

The first two points are discussed in the following sections. They prepare the ground for the actual methodology for performance variability evaluation which is presented in the last section of this chapter, and solves the issue of achieving an aggregated representation of potential performance variability.

2.1 Performance variability of heterogeneous functions

The heterogeneity of functions composing a FRAM model is addressed from two perspectives. The first one (Section 2.1.1) is related to the nature (Human, Technological or Organisational) of the functions. The second one is related to the focus of the analysis, i.e. if the functions are part of the foreground or of the background of the model (Section 2.1.2)

2.1.1 Human, Technological and Organisational functions

As proposed by Hollnagel (2004), the functions performed by a socio-technical system can be assigned to one of the three MTO categories: Human (M), Technology (T), and Organisation (O). In the original description of the FRAM, the use of the MTO framework provided an understanding of which Common Performance Condition influences a function. To improve the methodology the same framework is used to distinguish between different likelihoods of performance variability expressed by Human, Technological and Organisational functions.

Technological functions depend mainly on the technology implemented in the system. Technology is designed to perform in a stable, reliable and predictable way and despite the degree of complexity of modern technology, it can perform only as it is programmed to. Technology can fail, but it should not, if correctly developed and maintained, show performance variability. Therefore technological functions have a bimodal mode of functioning (i.e. work – do not work) and their performance can be assumed to be stable or slowly degrading over time. In the case of technology failure, the socio-technical system has to perform in degraded conditions and it is likely that humans will have to adjust their performance to cope with the unexpected and unpredicted situation. Due to their stability and reliability characteristics, technological functions cannot adjust their performance to meet unplanned or unexpected demands. Thus they cannot absorb or damp incoming performance variability.

Organisational functions depend on organisational activities and, traditionally, during safety assessment, they are part of the set of background functions. Organisational functions manifest some degree of performance variability since they are performed by humans, but they have a slowly developing effect on the daily activities of the socio-technical system. A typical example would be the production and updating of procedures. There can obviously be variability in the functions of designing and maintaining procedures, but it is extremely unlikely that this variability happens as fast as other human functions variability. Since the output of procedure writing nevertheless creates and shapes parts of the working environment, procedures may have a great influence on overall system

performance. As described above, the role of Organisational functions in the FRAM method is to provide support and means for human and technological functions. Organisational functions provide the system with the necessary means to damp performance variability. As an example, updated procedures, or adequate training create the conditions for humans to adjust their performance to cope with current conditions and thus dampen variability.

Human functions depend mainly on the people carrying them out. Since people have to adjust their performance to meet demands and to cope with underspecified rules, procedures and working conditions, Human functions are typically highly variable. As explained in Chapter 2. from a systemic perspective, the need for humans to fill in the underspecification gap, finding effective ways to cope with performance demands, is the primary reason for performance variability. If the objective is to perform a safety assessment, performance variability of Human functions is the most relevant factor to take into account. It is due to Human functions that the normal functioning of the socio-technical system is sustained. However, at the same time, it is in Human functions that the combination of performance variability is more likely to result in the so-called functional resonance effect.

The heterogeneity of performance variability could be summarised in the following table:

Table_ 3: Heterogeneity of performance variability

	Human	Technological	Organisational
Characteristic performance	Adjust their performance to current working conditions	Function in a stable, reliable, and predictable way	Provide support and means to human and technological functions
Variability	Variable (High frequency)	Stable, slowly degrading	Variable (High inertia)
Damping potential	Potential for performance variability damping	No potential for performance variability damping	Provide the means to damp performance variability

2.1.2 Foreground and Background functions

In a FRAM model, functions can be characterised not only on the base of their nature, but they can be as well differentiated according to their being part of the focus of analysis or part of the background.

The systemic approach of the FRAM supports the description of the characteristic performance of the system as a whole. A pivotal concept of systemic modelling is the relation between the sharp end and the blunt end. Hollnagel (2004) describes how performance variability of people at the sharp end is determined by a host of factors (Figure 10).

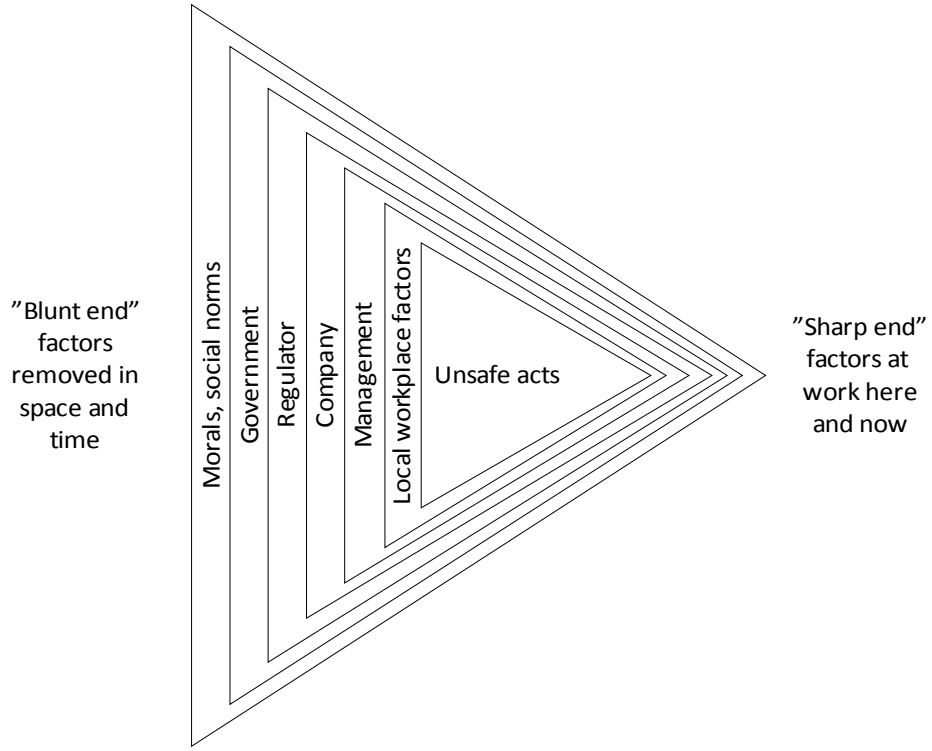


Figure 10: The Sharp end - Blunt end relationship (Adapted from Hollnagel, 2004)

The people at the sharp end are the people who are working in the time and place where operational activities happen and therefore where accidents might occur. At the blunt end one finds the people whose actions in another time and place have an effect on the people at the sharp end.

Traditionally safety assessment methods are concerned with risks at the sharp end. The blunt end is classically considered as the context affecting human performance reliability and is addressed as a background organisational entity outside the scope of the analysis. Thus it is presented as a factor influencing the way in which activity is performed, but in a static and settled manner.

Background activities have traditionally been described in the safety literature by lists of organisational activities that are required to ensure the safe functioning of the system. For example, Reiman & Oedewald (2009) identify a set of organisational activities (e.g. Resource management, Management of procedures, Competence management etc.) that an organisation needs to perform to create the optimal performance conditions for sharp end actors.

However, the systemic approach adopted by the FRAM has to account for the manner in which these blunt-end conditions are managed in the same way as all the other activities are considered, and therefore it requires modelling the background with the same approach used for the foreground.

In the FRAM model background functions provide support and means (i.e. Inputs, Controls, Resources and Preconditions) for the performance of the set of foreground functions. The identification of background functions is based on the consistency check of the model and starts from the description of foreground functions (Chapter 2 – Sections 2.2.3 and 2.2.5). For example, if a function requires a specific procedure as a Precondition to its performance, then this procedure has to be the Output of a background function somewhere in the same system. Thus it is possible to include in the FRAM model a background function (possibly called *Manage Procedure*) whose output is the procedure that will be used as Precondition by the foreground function.

Using a set of background functions to represent the context is an important improvement to the methodology. Context and environment have traditionally been regarded as elements that are external to the system while background functions stress the systemic view of the environment as *the aggregated sum of the unorganised origins and terminations of links crossing the boundary of the system or of any system with which is linked.* (Cornack, 1978).

The distinction between foreground and background is relative rather than absolute. Background functions can become foreground functions, for which a relative background has to be identified. When or if the analyst recognises in the background the primary source of performance variability a change in the focus of

analysis is undoubtedly appropriate to achieve a more detailed understanding of the functioning of the system.

A second advantage of this methodology is the consistency-check based approach of identification and description of background functions. Its application ensures that all the relevant context-related aspects for a defined model are considered, and at the same time only the relevant aspects are addressed, thereby reducing unnecessary effort in considering negligible factors.

2.2 Performance variability due to local adjustments

The Efficiency-Thoroughness Trade Off perspective (cf. Chapter 2) explains why functions must vary their performance to produce an acceptable output. The more the function is affected by degraded incoming aspects (Inputs, Resources, Preconditions and Controls) the more it has to adjust its performance to produce the required outputs. However, the presence of good quality Inputs, Resources, Preconditions and Controls reduces or damps the need to vary performance from the prescribed behaviour and therefore allows the performance of the function to be closer to standards and norms (Macchi, Hollnagel & Leonhardt, 2009). As described (Chapter 2- Section 2.2.5), each aspect is the output of a function and at the same time the Input or Precondition or Control or Resource for a downstream function. The time component of each aspect effects the available time for the downstream function to be performed i.e. increases or decreases temporal pressure. This in turn might have an impact on the accuracy and timing of the output production.

In order to assess performance variability is is therefore necessary to characterise the quality of aspects for all the functions. Each aspect can be characterised in terms of the accuracy and timing with which it is produced.

Accuracy-wise an aspect could be:

- Precise;
- Appropriate;
- Imprecise.

Time-wise each aspect could be:

- Too early;
- On-time;
- Too late.

It is possible to represent the quality of possible outputs by combining their accuracy and timing characteristic (Table_ 5)

Table_ 4: Functions: output characterisation

		Temporal characteristics		
		Too early	On time	Too late
Precision	Precise	**A**: Output to down-stream functions is precise but too early	**B:** Output to down-stream functions is precise with the right timing	**C**: Output to down-stream functions is precise but delayed, reducing available time
	Appropriate	**D:** Output to down-stream functions is appropriate but too late	**E:** Output to down-stream functions is appropriate with the right timing	**F:** Output to down-stream functions is appropriate but delayed, reducing available time
	Imprecise	**G:** Output to down-stream functions is imprecise and too early	**H:** Output to down-stream functions is imprecise but correctly timed	**I:** Output to down-stream functions is imprecise as well as delayed, reducing available time

Each aspect has an effect on the performance variability of downstream functions depending on its quality. The better the quality, the less the downstream function has to vary to maintain functioning and to meet performance demands. The more the quality is degraded, the more local adjustments have to be made and the downstream functions has to vary to ensure the functioning of the system. Good quality aspects create the conditions for downstream functions to damp variability (as in the Procedure and training example presented in on Section 2.1.1). Degraded quality aspects create the conditions for increasing performance variability.

The potential effect of the quality of an aspect on the performance variability of downstream functions can be summarised as follows:

1. Aspect's quality: **B** (Precise and On time) → High potential for variability Dampening.
2. Aspect's quality: **A** (Precise and Too early) → Medium potential for variability dampening**;**
3. Aspect's quality: **E** (Appropriate and On time) → Medium potential for variability dampening;
4. Aspect's quality: **C** (Precise and Too late) → Low potential for variability dampening;
5. Aspect's quality: **D** (Appropriate and Too Early) → Low potential for variability dampening;
6. Aspect's quality: **F** (Appropriate and Too late) → Low potential for variability increase;
7. Aspect's quality: **G** (Imprecise and Too early) Low potential for variability increase;
8. Aspect's quality: **H** (Imprecise and On time) → Medium potential for variability increase;
9. Aspect's quality: **I** (Imprecise and Too late) → High potential for variability increase)

The dampening effect of the good quality aspects on performance variability can be graphically represented as follow (Figure 11):

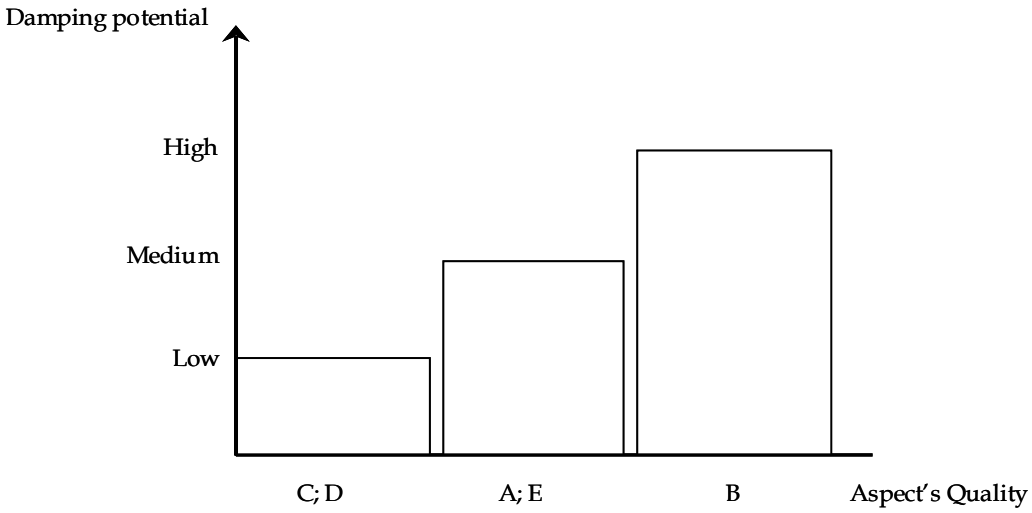


Figure 11: Dampening performance variability effect of good quality aspects

The increasing effect of degraded quality aspects on performance variability can be represented as follow (Figure 12):

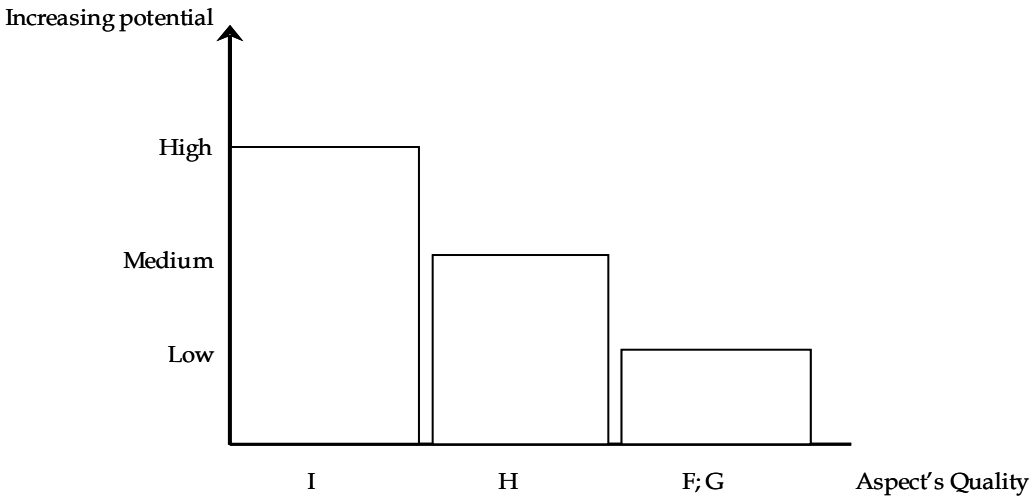


Figure 12: Increasing performance variability effect of degraded quality aspects

2.3 Aggregated representation for performance variability

The safety assessment process requires an estimate of the likelihood of performance variability for each function. So far, the methodology only describes the effect of the quality of a single aspect on the downstream function. To estimate the overall likely performance variability of a function it is necessary to aggregate the effects of the quality of all the aspects for that function, i.e. to achieve an aggregated representation for performance variability.

To achieve an aggregated representation it is necessary to clearly make a set of assumptions:

- ✔ Potential for dampening performance variability ranges from +1 to +3, where:
  - ✔ Low= +1
  - ✔ Medium= +2
  - ✔ High= +3
- ✔ Potential for increasing performance variability ranges from -1 to -3, where :
  - ✔ Low= -1
  - ✔ Medium= -2
  - ✔ High= -3

These assumptions constitutes an evident oversimplification of the reality, but they are necessary to understand the combined effect of incoming aspects on the performance of a function.

To exemplify this step the following figure is useful (Figure 13). A hypothetical Function Z is coupled to four upstream functions which provides four aspects:

- Two Inputs;
- One Control; and
- One Precondition.

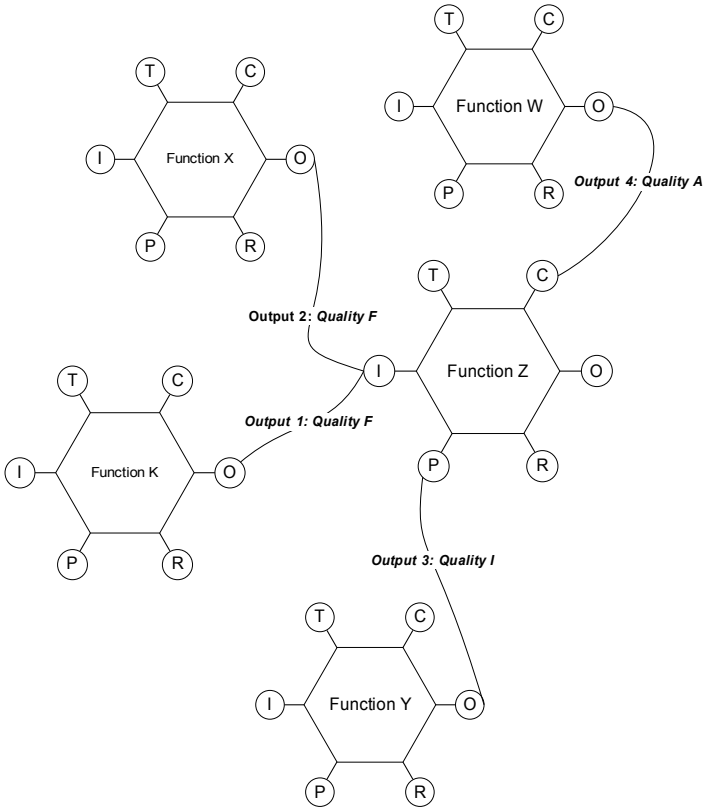


Figure 13: Example of aggregated representation for performance variability

The quality of these aspects is:

- Inputs – Quality **F**, i.e. Appropriate and Too late;
- Control – Quality **A**, i.e. Precise and Too early;
- Precondition – Quality **I**, i.e. Imprecise and Too late.

To evaluate the likely performance variability of Function Z it is necessary to understand the combined effect of the four aspects. The function description table (presented in Chapter 2) can be used to support this process (Table_ 4).

Table_ 5: Example of aggregated representation for performance variability

Function Z		Quality	Value
Input	Output 1 Output 2	F F	- 1 - 1
Output			
Control	Output 4	A	+ 2
Time			
Preconditions	Output 3	I	- 3
Resources			

The score, in this way obtained, can be aggregate using a simple indicator. For the time being a simple rule is proposed:

The median of the quality of the aspects is the quality of the output.

In this example the median value is -1. This value corresponds to an Output with quality F or G (Table_ 5). The disjunction between outputs belonging to the same quality group (e.g., small variability increase) has to be done on the basis of the instantiation.

Conclusion

With the aim of contributing to the development of the FRAM and in particularly to improve the methodology for the evaluation of the variability of normal performance, this chapter has addressed three issues. The first point addresses the heterogeneity of functions, required to ensure the functioning of a socio-technical system, and the different performance variability they can express. The second point addresses the need to represent performance variability due to systemic factors, i.e. due to local adjustments made to meet performance demands. The last issue is the need to have a single value to represent performance variability, so that the methodology can be used in practical safety assessment studies.

The FRAM aims to be a functional and systemic safety assessment method. It therefore needs a methodology for the assessment of performance variability based on a functional modelling of the system as a whole. The notion of foreground and

background functions was introduced for this reason. The different qualities of Human, Technological and Organisational functions makes the three typologies variable in different ways. While Technological functions normally perform in a reliable and standardised way and are therefore not variable, the variability of Humans and Organisational functions is an inevitable and necessary characteristic of their performance. For Human functions variability has high frequency, for Organisational functions it has more inertia. The fact that functions are coupled together, when the model is instantiated, means that every function is potentially subject to the performance variability of other functions in the system. It is therefore necessary to assess these combinations of performance variability. In the next chapter, the methodology is applied to a safety assessment study in the Air Traffic Management (ATM) domain. The methodology is applied to assess the effect of the introduction of a safety net, called Minimum Safe Altitude Warning, in the German ATM system. The results of the application of the performance variability methodology are compared with the results of an official safety assessment study conducted using a traditional method.

Page intentionally left blank

Chapter 4: Evaluation of the Developed Methodology: Case Study in the Air Traffic Management Domain

Page intentionally left blank

Résumé du Chapitre 4

En 2008 le Prestataire National de Service Aérien Allemand, *Deutsch FlugSicherung* (DFS), a réalisé une étude d'estimation de la sécurité concernant l'introduction d'un système de *safety net* (filet de sécurité) appelé *Minimum Safe Altitude Warning* (MSAW – Alerte d'Altitude Minimum Sûre). Ce chapitre décrit cette étude ainsi que les résultats obtenus. Le même cas est ensuite analysé à l'aide de la méthodologie basée sur FRAM développée dans le Chapitre 3. Enfin, les résultats obtenus pour chaque approche sont comparés.

La Section 1 décrit la MSAW, puisque, pour procéder à l'estimation de la sécurité, il est nécessaire de comprendre ses fonctionnalités, son architecture et ses interactions avec d'autres parties du système.

La Section 2 décrit l'estimation de la sécurité faite par DFS, qui a consisté en une série d'ateliers auxquels prirent part des experts en sécurité et dans le domaine aérien, sur l'identification des risques dus à l'introduction de ce nouveau système de support. Ces ateliers couvrirent les aspects aussi bien techniques opérationnels.

La Section 3 illustre l'application de la méthodologie développée pour l'estimation de la variabilité de la performance normale, dans le cadre d'une étude d'évaluation de la sécurité du cas cité.

Bien que l'application se concentre sur un scenario simplifié, il est possible de comparer les résultats obtenus pour les deux estimations de la sécurité et d'avoir un aperçu de la valeur ajoutée réelle d'une approche systémique fondée sur l'évaluation de la variabilité de la performance.

Introduction

In 2008 the German Air Navigation Service Provider, Deutsch FlugSicherung (DFS) performed a safety assessment for the introduction of a safety net system called Minimum Safe Altitude Warning (MSAW). This chapter describes that study and the results obtained. The same case is then analysed using the FRAM-based

methodology developed in Chapter 3. Finally, the results from the two approaches are compared.

Section 1 describes the MSAW as,to proceed to the safety assessment, it is necessary to understand its functionalities, its architecture and its interaction with other parts of the system.

Section 2 describes the DFS safety assessment which consisted of series of workshops where safety and domain experts collaborated on the identification of risks due to the introduction of the new support system The workshops covered both technical and operational aspects.

Section 3 illustrates the application of the developed methodology for the assessment of the variability of normal performance for a safety assessment study to the same case.

Although the application is focused on a simplified scenario it is possible to compare the results of the two safety assessments and to gain insight about the real added value of a systemic approach based on the evaluation of performance variability.

1 Case study: the Minimum Safe Altitude Warning system

The Minimum Safe Altitude Warning system is a ground-based safety net. Ground-based safety nets are that part of the Air Traffic Management system that help to prevent imminent or actual hazardous situations from developing into major incidents or accidents. According to the EUROCONTROL "Safety Nets Brochure", safety nets provide a comfort zone for human actors in the system and keep the societal outcome of aviation operations within acceptable limits. They rely primarily on Air Traffic Service surveillance data. Their goal is to alert Air Traffic Controllers (ATCO) sufficiently in advance to allow them to assess a hazardous situation and take appropriate actions.

Specifically, MSAW aims at to prevent a "serious situation from developing into a catastrophic one in case of loss of terrain awareness." (MSAW system requirement

document, Version 2.1, 2007) In more detail, MSAW alerts ATCOs to a potential Controlled Flight Into Terrain (CFIT), Controlled Flight Into Obstacle (CFIO) and serious approach path deviations. The MSAW System documentation (Version 2.1 issued 11.01.2007) states that MSAW is a safety function that "under normal circumstances, allows the ATCO to conduct his tasks with MSAW operating in the background and not disturbing ATC process". It is normally transparent to the controller.

The MSAW monitors:

1. General Terrain;
2. Minimum Radar Vectoring Altitudes;
3. Approach Path.

1.1 General Terrain monitoring

General Terrain monitoring informs the controller when an aircraft is below, or is predicted to fly below, a level that is considered to be too close to the ground or to obstacles. This level is designated as the Minimum Safe Altitude (MSA). For General Terrain monitoring the MSAW uses a Terrain Data Model (Figure 14) which includes obstacles (e.g., skyscrapers) that are significantly higher than the surroundings.

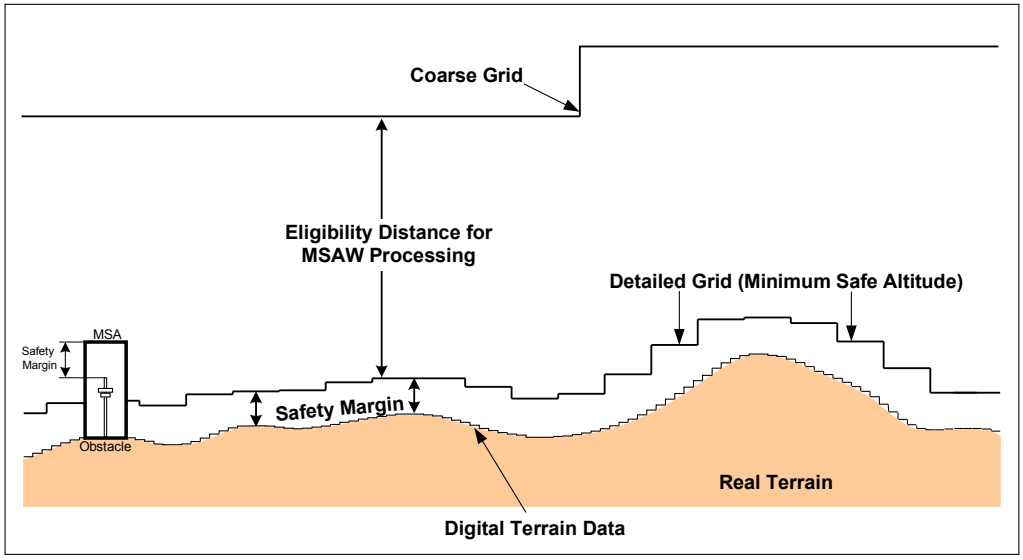


Figure 14: Terrain Data Model (from MSAW documentation)

1.2 Minimum Radar Vectoring Altitude monitoring

Above the Minimum Safe Altitude it is possible to define a second threshold, the Minimum Radar Vectoring Altitude (MRVA). This covers areas where the standard radar coverage does not reach the Minimum Safe Altitude. The MRAV monitoring alerts ATCOs if the current position of an aircraft is below this threshold.

1.3 Approach Path Monitoring

Approach Path Monitoring alerts ATCOs to an aircraft that deviates, or is predicted to deviate, from the approach path to a runway. The deviation might be either to the side or below. An approach path monitoring area is composed by:

1. A Glide Slope protection area;
2. A MSAW inhibit area;
3. Two Centreline protection areas.

Figure 15 and Figure 16 illustrate the Glide Slope protection areas and the two Centreline protection areas.

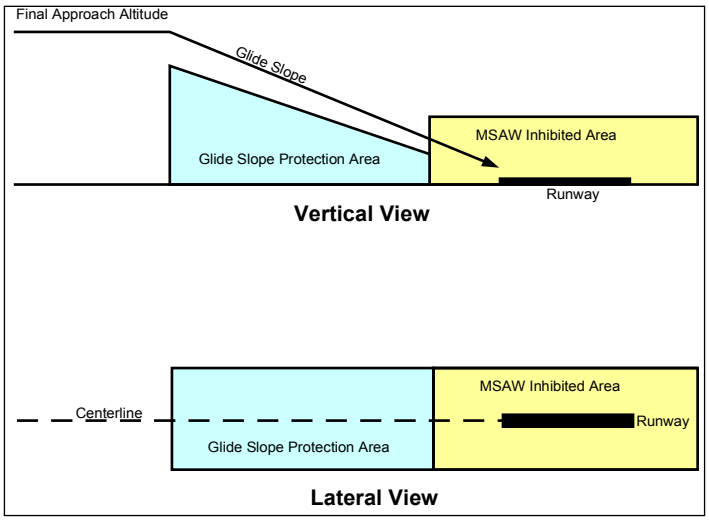


Figure 15: Glide Slope protection areas

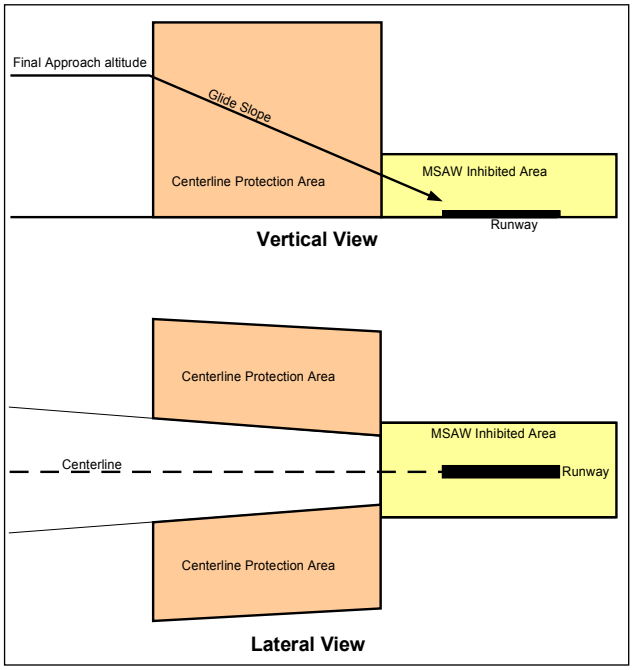


Figure 16: Centreline protection areas

In order to reduce the number of possible nuisance alerts, a time-related logic for the display of alerts has been proposed. The MSAW system requirement document states that "if a possibly hazardous situation is detected the first time, the display of the alert shall be delayed until it has been confirmed by a number of additional track data updates". And it continues: "if the alert is confirmed by the detection logic and the time to violation (TV) is still greater that the required warning time

(TR) the process of confirmation will be continued until the time to violation reaches the required warning time". While the application of this logic may be useful and reduce the number of nuisance alerts, it has the drawback of reducing the available time for an ATCO to respond.

The DFS safety assessment methodology and the preliminary results are presented in the next section.

2 The MSAW safety assessment process by DFS

Between July and August 2008 seven workshops were held at Deutsch FlugSicherung (DFS) to perform a safety assessment study in preparation for the introduction of the MSAW. The safety assessment, conducted in accordance with DFS safety assessment methodology involved Air Traffic Controllers, IT experts, the MSAW project manager and DFS safety experts.

2.1 Deutsch FlugSicherung safety assessment

The official DFS safety assessment started with the identification of a series of assumptions concerning the operating environment of the MSAW (section 2.1.1). Potential MSAW related accidents were identified (section 2.1.2) and an Hazard Analysis was conducted (section 2.1.3).

2.1.1 Environment assumptions

The safety assessment team prepared a list of assumptions about the Roles, Objects, Information, and Procedures that were expected to interact with (and might therefore possibly be affected by) MSAW. These assumptions were fundamental to the assessment as they set the boundaries of what should be considered and what can be ignored in the hazard identification process. The main environment assumptions are shown below (Table_ 6).

Table_ 6: Environment assumptions

Roles	Objects	Information	Procedures	Others
En-route and approach controllers	MSAW hardware and interfaces	Aircraft track data	MSAW maintenance guide	No change to airspace design
ATC supervisor	P1/ATCAS-CWP; SDPS	Meteorological data	ATC monitoring procedures	All traffic, all flight rules are included
MSAW adaptation maintainer	Phoenix System (back-up system)	Terrain and obstacle data	ATC response procedures to MSAW	All aircraft types are concerned (civil, military…)
Maintenance engineer/system management	IDVS/Omega	Airspace data	ATC-ATC communication procedures	All flight rules (IFR and VFR-if data available)
MSAW product manager	Technical supervisory system (CMMC)	MSAW parameters	Acceptance and clearance guideline	Aircraft equipment: No additional requirements
Requirement manager	CDM (Control and Monitor Display for supervisor)	System monitoring and control information	---	No change on Minimum Separation Criteria

2.1.2 Accidents considered

Several potential MSAW-related accident scenarios were identified. In addition, a description of the expected effect of introducing the MSAW was provided (Table_ 7).

Table_ 7: Accidents considered

Accident	Influence of MSAW introduction
Controlled flight into terrain (CFIT)	MSAW is designed to reduce this risk
Controlled flight into obstacle (CFIO)	MSAW is designed to reduce this risk
Mid-air collision (MAC)	MSAW alerts could force ATCO to issue clearance that may result in an increase in MAC risks
Wake Vortex Encounter (WVE) and consequent loss of control and/or structural damage	MSAW alerts could force ATCO to issue clearance that may result in an increase in WVE risks

It is noteworthy that the Safety assessment team considered two accident types beyond the accidents that the MSAW was designed to prevent (CFIT and CFIO). The increased risk of Mid Air Collision (MAC) and Wake Vortex Encounter (WVE)

were included because they were seen as possible drawbacks in the operational introduction of MSAW.

The next paragraph presents some of the technological and operational hazards that were identified during the safety assessment workshops.

2.1.3 Hazard Analysis

Hazard Analysis consisted of the identification of new hazards possibly generated as a consequence of the introduction of MSAW. For every hazard the following points were addressed:

1. Causes, i.e. what has created the hazard;
2. Effects, i.e. what are the effects if the hazard becomes manifest;
3. Mitigations, i.e. what has to be done to prevent the manifestation of the hazard.

A selection of the identified hazards is shown in Table_ 8. In addition to these, others were identified and discussed. However, as they refer mainly to hazards caused by technical failures (e.g., server crash, MSAW hardware failure, etc.) they are not relevant for the evaluation of the developed FRAM methodology (the FRAM is focused on performance variability) and will therefore not be further discussed.

Table_ 8: Hazards analysis

Hazard	Causes	Effects	Mitigation
Operators errors: • Switch on/off of interfaces • Switch on/off MSAW server	• Human error • Procedure incorrect	• No MSAW function • Degraded MSAW function • MSAW functioning with incorrect software or adaptation	• Training • Well defined and verified procedures
• Out-of-date flight plan leads to loss of APM alert	• Emergency diversion • Incorrect/incomplete flight plan • FDPS failure	• No APM alert generated	• Manual update flight plan
• Incorrect suppression of area	• Human error by supervisor • Supervisor workload	• MSAW function is not provided • False alert generated	• Training • Manning level
• Not clear to ATCO which aircraft/area is suppressed in MSAW	• MSAW area not displayed to ATCO • Insufficient information about suppression provided by supervisor to ATCO	• No MSAW functionality available when expected • MSAW functionality available when not expected	• Training • understand of MSAW requirement for each role
• Supervisor forgets to deactivate the suppressed areas	• Human error by supervisor • Supervisor workload	• MSAW function is not provided	• Time-based suppression in the future (To be confirmed)
• ATCO relies on MSAW and this reduce attention to aircraft altitude	This is not the way ATCOs should operate. NO concern on this point because it is not considered to be a real hazard		
• ATCO or pilot responds to MSAW alert in a way that may produce infringements	• Over-reaction or unexpected response of pilot to ATCO advice	• Variable depending on pilot reaction	
• ATCO get distracted or tunnel vision by an alert	• False alert: • Adaptation problems • Technical causes	• Distraction from more important tasks	

Even with these preliminary results, some specific comments can be made:

- Most of the hazards, as identified, are caused by human errors, or human error is the hazard itself;
- Most of the hazards, as identified, are mitigated with better training and verification / testing;
- There are no explicit references to contextual factors;
- Possible interactions between hazards are not envisaged;
- The possibility of reduced attention due to an over-reliance on the system capability to detect altitude related problems is not considered.

On the basis of the available conclusions from the official MSAW safety assessment, a further general comment is that the applied method seems to be effective and productive for the identification of single cause hazards. Technology related problems are thoroughly considered and analysed. The focus on single-cause technical hazards is in disagreement with the need complex socio-technical systems have to address multiple cause hazards or emergent risks (cf. Chapter 1). This phenomenon could be due to the intrinsic limitation of the applied method (developed to analyse linear and simple hazards).

3 Evaluation of the developed methodology

The developed methodology was applied to the MSAW case study in order to perform a preliminary evaluation. Specifically, the methodology was used to assess potential emergent risks for an *ad hoc* landing approach scenario at Stuttgart airport.

The evaluation of the methodology followed the following steps:

1. Scenario definition;
2. Identification of functions;
3. Instantiation of the model;
4. Evaluation of performance variability;

5. Comparison with DFS safety assessment results.

3.1 Scenario Definition: A Landing Approach in Stuttgart

The case is related to Air Traffic Controller activities at Stuttgart airport. The Stuttgart airport arrival chart is presented in Figure 17

In their approach to Stuttgart, aircraft normally follow the approach path before being transferred to the Tower control centre for the final landing phase. Every aircraft in the sector is under the responsibility of a Landing approach controller. The controller has to coordinate the movements of all the aircraft in the sector in an efficient way while respecting the minimum separation criteria (six nautical miles). Among others duties, a Landing approach controller has three main objectives:

1. Decide the landing sequence for all the aircraft in the sector;
2. Direct every aircraft to the Final Approach Fix (FAF) point and transfer it to the Tower; and
3. Descend every aircraft to an altitude of 4,000 Feet (at this altitude the aircraft should be transferred to the Tower).

Stuttgart airport has a standard landing rate of 20-30 aircraft per hour and every aircraft stays in the sector between 5 to 10 minutes depending on where they are coming from (some arrival routes are shorter than others). In this configuration, it is reasonable to build a scenario where the Landing approach controller has to deal with two aircraft at the same time.

- Aircraft #1 is approaching Stuttgart airport from the North at Flight Level (FL) 160 (approximately 16,000 feet). ATCO has to direct it towards FAF, reduce its speed, decrease its altitude and hand-over to the Tower control centre.
- Aircraft #2 is approaching Stuttgart from the South at FL 100 (approximately 10,000 feet). The ATCO has to guide it towards the FAF while decreasing its speed and reducing its altitude and then hand-over it to the Tower control centre.

The next section presents the FRAM functions which must be performed in order to fulfil the ATCO objectives.

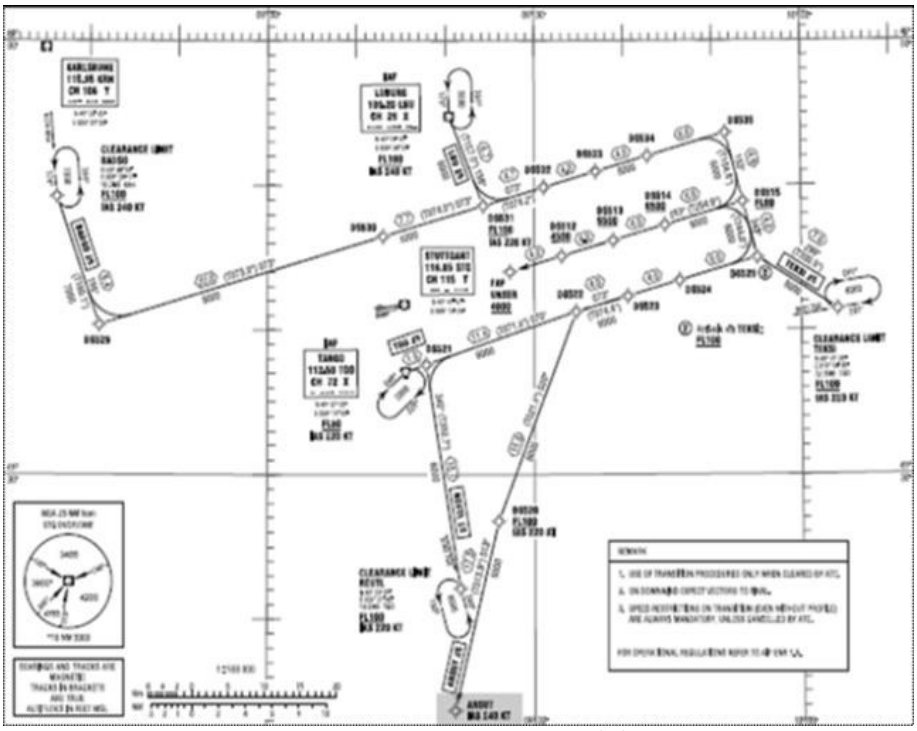


Figure 17: Stuttgart airport arrival chart

3.2 Foreground functions identification

In order to identify and describe the necessary Air Traffic Management (ATM) system functions, the model for an Over-flight scenario (Macchi, Hollnagel & Leonhardt, 2008) has been used.

The Over-flight scenario, presented in Chapter 2, is the result of the methodology which was developed as a starting point to investigate how an evaluation of performance variability can be made with the FRAM. The objective of the Over-flight model was to represent, using FRAM, the functions that are necessary to control aircraft traffic passing through an airspace sector. From the Air Traffic Management system point of view, the basic functions performed to manage Over-flights are the same as those executed to control a landing aircraft. The technical systems provide the same information about the flight and the meteorological situation. ATCOs monitor the flight progress and plan the best set of clearances to be issued to avoid minimum separation infringement while being as efficient as

possible. They also issue clearances to the pilot, mark progress strips, coordinate with adjacent sectors, etc.

What does change is the scenario that the socio-technical system has to deal with. Being the basic functions the same in both Over-flight and Landing approach scenario, it was therefore sensible to use the set of functions described by Macchi, Hollnagel & Leonhardt (2008) and update the model to match the requirements of the MSAW case study.

The Over-flight model is composed by the following functions (Table_ 9)

Table_ 9: Functions for the Over-flight control activity

1	Monitoring
2	Planning
3	Provide ATC clearance to pilot
4	Strip marking
5	Coordination
6	Update flight data processing system
7	Provide meteorological data to controller (IDVS/Omega system)
8	Provide flight and radar data to controller (P1/ATCAS)
9	Controller pilot communication
10	Sector-sector communication

This set of ten functions were modified as follow:

1. The function **Provide meteorological data to controller** and the function **Provide flight and radar data to controller** became **Provide meteorological data** and **Provide flight and radar data,** respectively. This change takes into account the fact that information is not directly provided to Air Traffic Controllers, but it is shown on radar and computer screens where other information is displayed.

2. The function **Display data on Controller Working Position (CWP)** was added to the model. This function collects the above mentioned information (and any possible other information, e.g., warnings) and displays them on the Controller Working Position.
3. The function **Update meteorological data** was added to the model. This function accounts for the possibility that meteorological data can be updated manually, when something is missing or incomplete.

Taking into account these modifications, the foreground model comprises therefore the following twelve functions (Table_ 10).

Table_ 10: Foreground functions

1	PROVIDE MET DATA	Provide to CWP QNH, wind speed and direction, heavy rain etc. Technical function performed by IDVS/omega system.
2	PROVIDE FLIGHT & RADAR DATA	Provide CWP flights call sing, flight level, aircraft typology, aircraft vectoring, route information etc. Technical function performed by P1/ATCAS system.
3	DISPLAY DATA CWP	Display data on Controller Working Position
4	MONITORING	Monitor traffic situation and anticipate traffic development. This function consists in building and updating a mental picture of traffic situation, as well as search for potential conflicts.
5	PLANNING	Develop a control plan to anticipate conflicts and manage traffic flow.
6	STRIP MARKING	Mark the issued clearances on paper or electronic strip
7	COORDINATION	Coordinate with adjacent sectors on desired flights level, vectoring, route, airplanes' reported problems etc. This function is performed by the planning controller to support executive controller activity
8	UPDATE FDPS	Update data processing system with respect to issued clearances.
9	PILOT-ATCO COMMUNICATION	Communication, initiated by pilots, to establish radio contact or to request information or clearances to controller
10	SECTOR-SECTOR COMMUNICATION	Radio telecommunication between adjacent sectors to initiate the coordination function.
11	ISSUE CLEARANCE TO PILOT	Issue clearances to pilots via radio communication system or data link.
12	UPDATE MET DATA	Manually update Meteorological data if technical system temporally fails and some data are missing

Once they had been identified, each of these twelve functions was described according to their aspects (Input, Output, Preconditions, Resources, Time and Control) as required by the FRAM.

Table_ 11 and Table_ 12 are examples of the result. The complete set of tables is presented in Annex II.

Table_ 11: Monitoring function description

Monitoring	
Input	Flight data displayed Radar data displayed MSAW alert displayed System message displayed Strip marked = [initial call; clearance; plane released to next sector; frequency changed]
Output	Flight position monitored = [entering the sector; flight in the sector heading towards (x); leaving the sector]
Control	Monitoring procedures Technical training Working conditions Adjustment of data display
Time	----
Preconditions	FDPS updated Interface design
Resources	Situation data display equipment Additional data display

Table_ 12: Display data on CWP function description

Display data on CWP	
Input	Flight data: 1. Call sign 2. Flight level/ Altitude 3. Vectoring 4. Type of aircraft 5. Aerodrome of departure 6. Aerodrome of destination 7. Time over target 8. Route information Radar data Traffic situation in next sector Meteorological data : 1. QNH; 2. Meters of visibility; 3. Wind speed; 4. Wind direction; 5. Clouds typology; 6. Heavy precipitation MSAW alert generated =[GTM alert; APM alert; MRVA monitoring alert] System messages
Output	Flight data displayed Radar data displayed Meteorological data displayed MSAW alert displayed System message displayed Maps
Control	Alert-inhibited airspace volumes defined Alert-inhibited SSR codes defined
Time	-----
Preconditions	-----
Resources	-----

The two functions could be instantiated according to their description and graphically represented as follow (Figure 18):

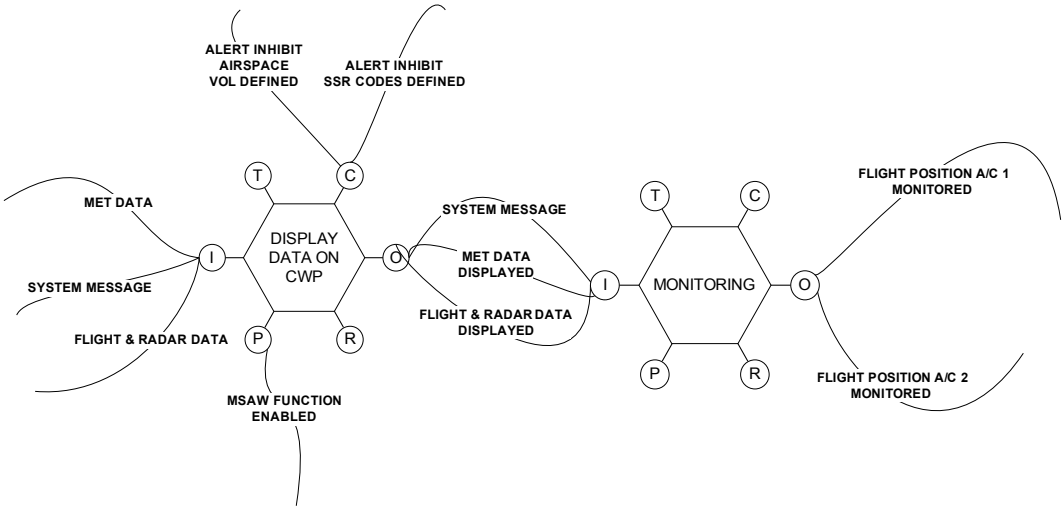


Figure 18: Display data on CWP and Monitoring instantiation

3.2.1 MSAW functions identification

Since the aim of this safety assessment study is the evaluation of the impact of MSAW introduction in the ATM system, MSAW related functions are clearly part of the foreground. Several interactions with MSAW system experts and Air Traffic Controllers lead to the identification of four FRAM functions related to the MSAW functionalities (Table_ 13).

As the objective is to understand their potential influence on the ATM system, these FRAM functions have a relative high level of description and, more importantly, a level which allows the identification and assessment of performance variability.

Table_ 13: MSAW functions

1	GENERATE MSAW ALERT	Generate alerts (General Terrain Monitoring, Approach Path Monitoring, Minimum Radar Vectoring Altitude) using predicted aircraft paths and MSAW prediction logic.
2	ENABLE MSAW ALERT	When MSAW is not enabled, the alert generation process continues, but alert transmission will be suppressed
3	DEFINE ALERT INHIBIT AIR SPACE VOLUMES	Define specified airspace volumes to inhibit the transmission of MSAW alerts
4	DEFINE ALERT INHIBIT SSR CODES	Define individual or list of SSR codes to inhibit the transmission of MSAW alerts.

The **Generate MSAW alert** is a Technological function as it is performed by the technical system that computes and generates alerts on the base of predicted aircraft paths and on the MSAW logic. It should therefore, according to the discussion in Chapter 3 on performance variability, not express performance variability in its normal functioning.

The three other functions (**Enable MSAW alert, Define alert inhibit air space volumes,** and **Define alert inhibit Secondary Surveillance Radar (SSR) codes***)* are Human functions since they require an important human contribution to their execution. They are part of an ATC supervisor controller's tasks and some kind of performance variability is therefore expected..

Table_ 14 presents the description for the **Generate MSAW alert** function. The complete set of functions is described in Annex II.

Table_ 14: Generate MSAW alert function description

Generate MSAW alert	
Input	Flight data: 1. Call sign 2. Flight level/ Altitude 3. Vectoring 4. Type of aircraft 5. Aerodrome of departure 6. Aerodrome of destination 7. Time over target 8. Route information Meteorological data : 1. QNH; 2. Meters of visibility; 3. Wind speed; 4. Wind direction; 5. Clouds typology; 6. Heavy precipitation Obstacle model Terrain model
Output	MSAW alert generated =[GTM alert; APM alert; MRVA monitoring alert]
Control	MSAW logic Met. Data updated
Time	TV < TL
Preconditions	Flight position below MSA Flight predicted to penetrate MSA Flight position below MRVA threshold Flight position within a glidepath/ centreline protection area Flight predicted to penetrate glidepath/ centreline protection area
Resources	-----

As an example, the potential instantiation of the functional coupling between the **Generate MSAW alert** function and **Display data on CWP** function is illustrated in the following figure.

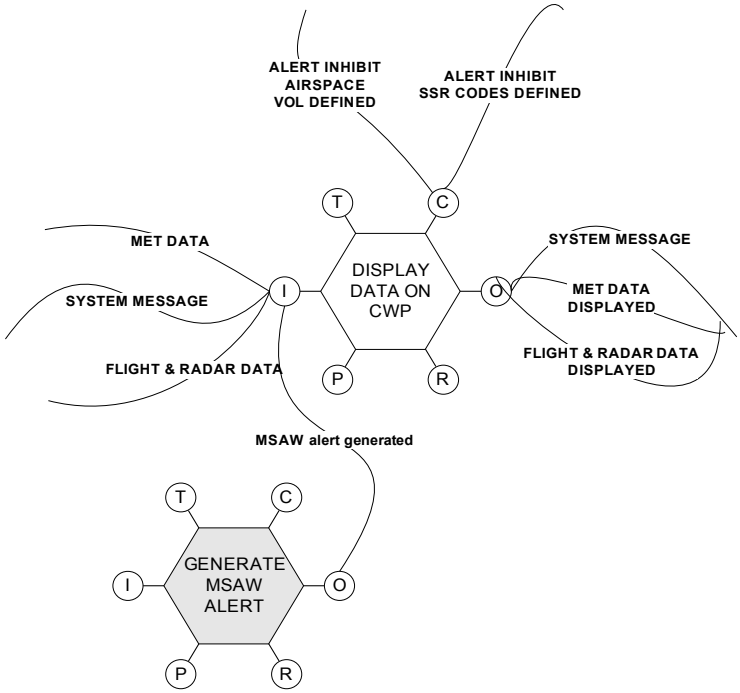


Figure 19: Generate MSAW alert and Display data on CWP instantiation

3.3 Background functions identification

As explained in Chapter 3, to represent the influence of context on performance it is necessary to first identify the set of background functions for the foreground functions under assessment.

The identification of background functions starts from the description of the foreground functions previously identified. This process is illustrated in the following example.

In Table_ 15 *Monitoring procedures* has been identified among other aspects, as a necessary Control for the foreground function of **Monitoring**.

Table_ 15: Monitoring function description

Monitoring	
Input	Flight data displayed Radar data displayed MSAW alert displayed System message displayed Strip marked = [initial call; clearance; plane released to next sector; frequency changed]
Output	Flight position monitored = [entering the sector; flight in the sector heading towards (x); leaving the sector]
Control	Monitoring procedures Technical training Working conditions Adjustment of data display
Time	------
Preconditions	FDPS updated Interface design
Resources	Situation data display equipment Additional data display

This implies the existence, in the socio-technical system, of a background function whose Output is *Monitoring procedures*. The same background function, in charge of producing appropriate procedures to support ATCOs work, is likely to produce procedures for other functions e.g. **Issue clearance to pilot**. It could therefore be identified as, for the time being, a general **Manage procedures** function (Table_ 16).

Table_ 16: Manage procedures function description

Manage procedures	
Input	-----
Output	Procedure Alert-inhibited airspace volumes List of SSR codes Coordination procedures Clearance procedures Monitoring procedures Minimum separation criteria RT standards Communication procedures Enables MSAW alert procedures
Control	-----
Time	-----
Preconditions	-----
Resources	-----

Graphically, the two functions (**Monitoring** and **Manage procedures)** can be instantiated as in Figure 20.

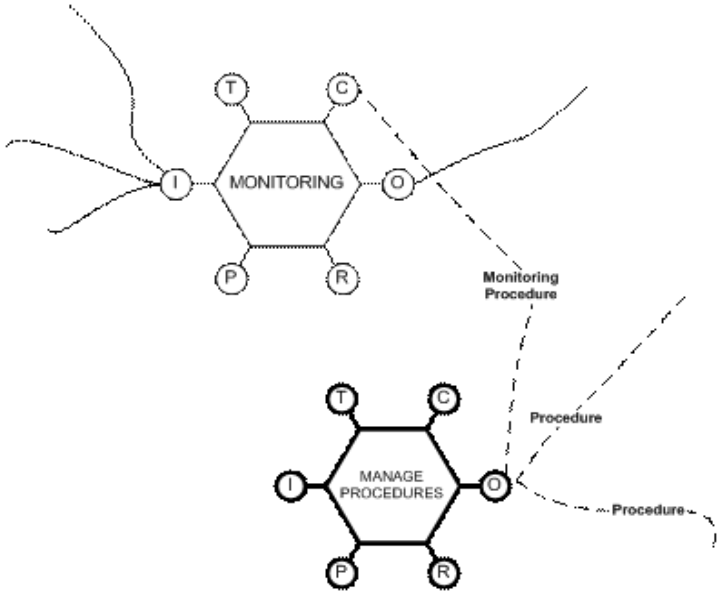


Figure 20: Monitoring and Manage procedures instantiation

Similarly both **Issue clearance to pilot** and **Pilot-ATCO communication** have – according to their description (cf. Annex II) – as a Control the *Teamwork* aspect. It is therefore possible to deduce the existence of a background function that manges *Teamwork*. The instantiation of this background function with the two foreground functions is shown in Figure 21.

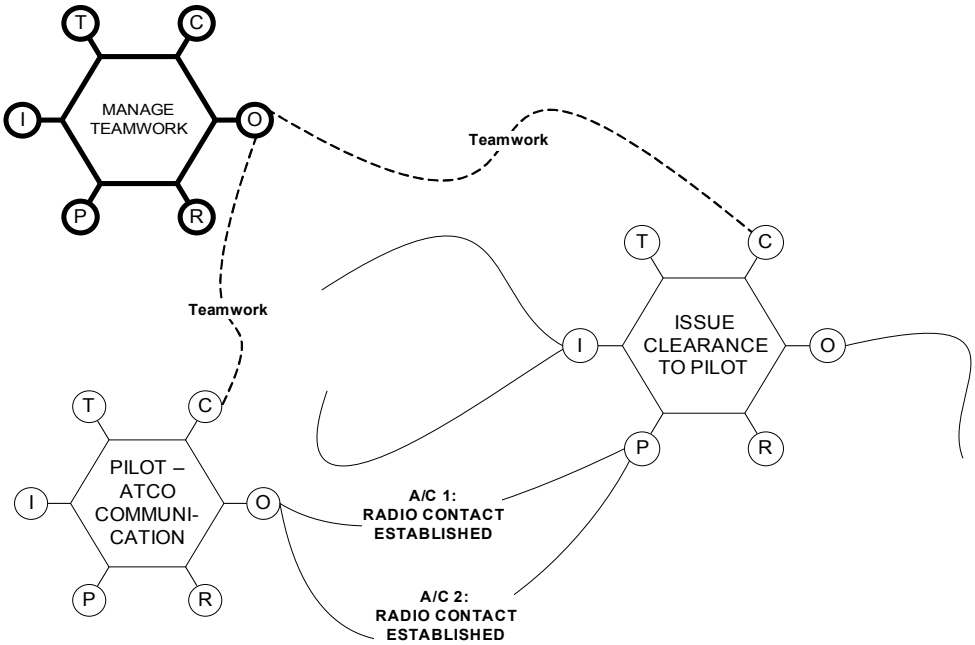


Figure 21: Pilot-ATCO communication, Issue clearance to pilot and Manage teamwork instantiation

The approach used to identify and describe background functions makes them 'dummy' upstream functions. This is because only their Outputs have been identified as the detailed identification of all the other aspects is not necessary for the scope of the analysis.

This identification process, starting from every foreground function, led to the five background functions shown in (Table_ 17) and which are fully described Annex II.

Table_ 17: Background functions

1	MANAGE RESOURCES	Provide and manage economical, technical and human resources to allow system functioning
2	MANAGE COMPETENCE	Provide operators with required competences and knowledge for system operation. This includes technical, safety competence and deference to expertise.
3	MANAGE PROCEDURES	Design, update, distribute procedures to support operational activity
4	MANAGE TEAMWORK	Manage teamwork to assure a desired quality in team collaboration
5	MANAGE WORKING CONDITIONS	Manage the conditions (e.g. HMI, ergonomic aspects, noise, lightening etc) in which the work is carried out

3.4 FRAM model

The identification of foreground and background functions leads to the constitution of the FRAM model of the socio-technical system (Figure 22). The model is composed of the two sets of functions presented above: Foreground functions (MSAW functions, shown in grey, are part of this set) and Background functions (shown in thick lines).

The functions in the model are not permanently coupled. The links between them are generated according to the scenario being analysed. In next section, a set of instantiations (i.e., the way in which functions are coupled under given conditions) of the model is presented. The instantiation, together with the evaluation of performance variability, are the basis for the safety assessment.

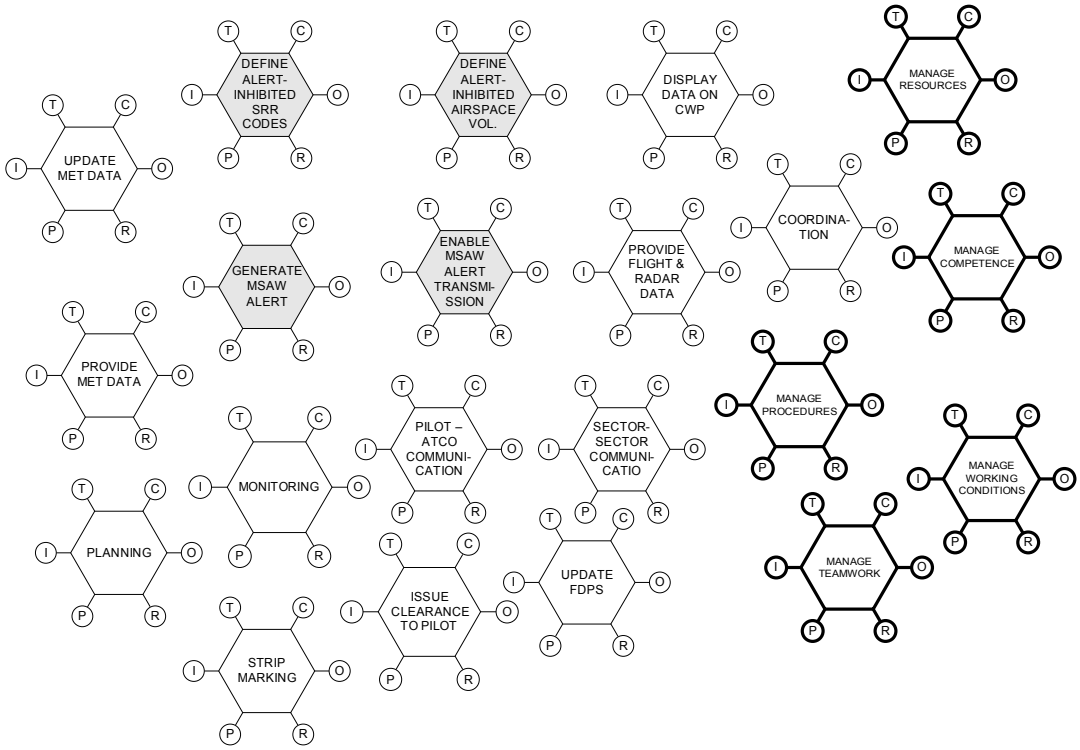


Figure 22: The FRAM model of the socio-technical system

3.5 Scenario instantiation

Several FRAM instantiations were developed for the scenario under consideration – a landing approach at Stuttgart airport.

Two scenarios will be presented here: the nominal scenario (i.e., what controllers ought to do according to the procedures) and a normal scenario (i.e. what controllers may actually do for such airspace and aircraft position). The normal scenario is based upon information gathered from interviews with controllers and from field observations.

3.5.1 Nominal scenario

The nominal scenario represents the performance that would result if procedures were strictly applied. It is a procedural descriptions of Air Traffic Controllers actions to deal with a specific situation.

In order to reach the Final Approach Fix point the procedural trajectory of an aircraft should follow the approach path (dotted lines in Figure 23). In this case a

standardised approach would be followed by the two aircraft in the scenario and ATCOs would make sure that minimal separation criteria were respected.

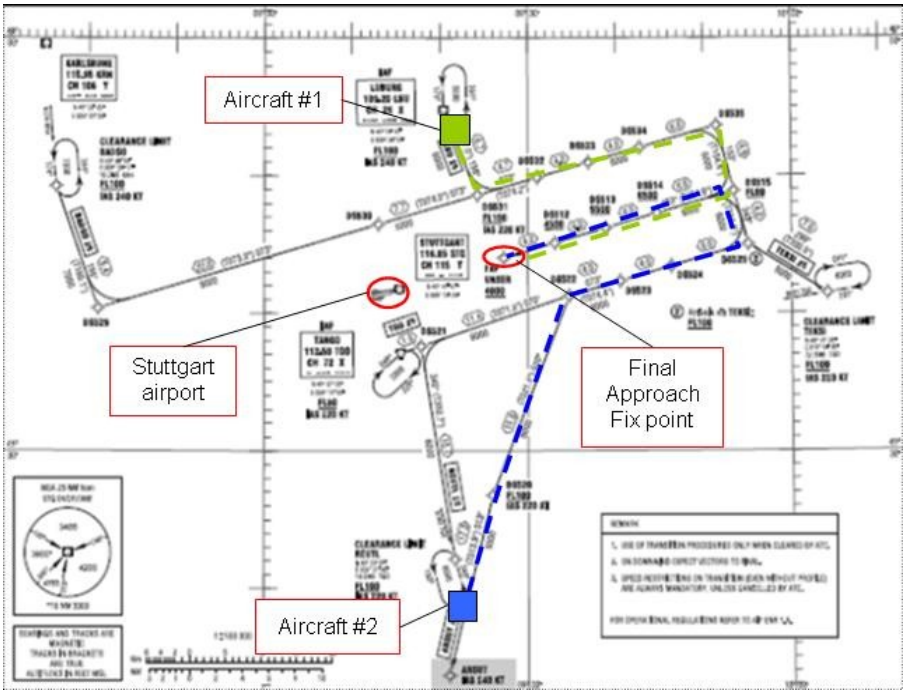


Figure 23: Aircraft approaching path for Nominal instantiation

3.5.2 Normal scenario

The normal instantiation represents the actual way in which controllers would deal with the two aircraft. The normal scenario is therefore more realistic, in the sense that the scenario does usually develop in this way. To arrive at this description, interviews and field observations were performed at DFS control centre in Langen (Germany). Using their experience and competences controllers prefer to adjust their work to provide pilots with more effective clearances. In this way the controllers' workload is reduced and aircraft reach the Final Approach Fix point faster (Figure 24). This situation is a clear demonstration of how the Efficiency-Thoroughness Trade Off can be beneficial for both ATC and airlines.

During the approach the following clearances are issued:

1. Aircraft #1 identified, proceed direct to DLS 512, descend altitude 5000 FT-QNH 1027
2. Aircraft #2 identified, descend FL60, proceed direct to DLS 512

3. Aircraft #1 descend altitude 4000 FT, turn right heading 230, cleared ILS25
4. Aircraft #2 descend altitude 4000 FT-QNH 1027, turn left heading 210, cleared ILS25
5. Aircraft #1 contact tower
6. Aircraft #2 contact tower

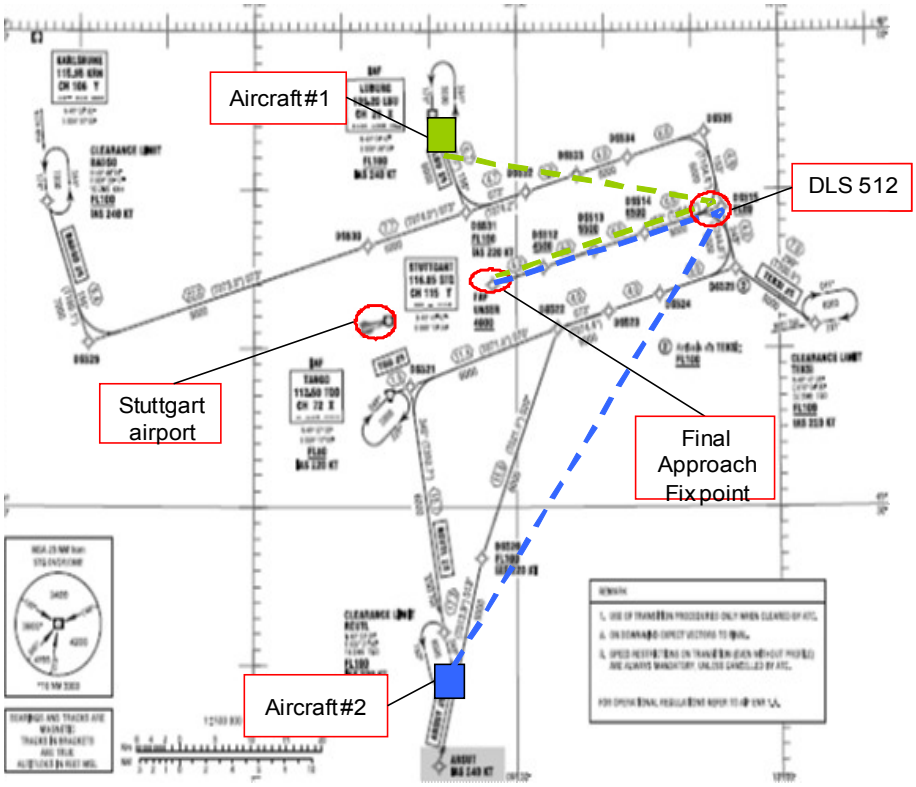


Figure 24: Aircraft approaching path for Normal instantiation

Since the purpose of this work is to assess the potential impact of the introduction of MSAW in the **normal** activity of ATM, this scenario will be used to generate instantiations for emergent risks identification.

3.6 Safety assessment for the normal scenario

The safety assessment for the normal scenario is based on a "paper and pencil" simulation. It illustrates how the proposed methodology can be applied to a safety assessment case, although such an application will be more intricate in reality.

The normal scenario could be instantiated in the model with a set of sequential instantiations representing the temporal development of the scenario. In order to apply the method a set of assumptions has to be made:

1. Background functions produce accurate outputs (Outputs quality: **E** according to Table_ 4 on page 73), therefore the context for foreground functions performance is appropriate and no variability is induced by the background functions;
2. In the scenario, the MSAW function **Generate MSAW alert** triggers an alert (for Aircraft #1). The other Technological functions are properly designed and implemented. Their outputs are correct and no variability is induced (Outputs quality: **E** according to Table_ 4 on page 73);
3. The MSAW function **Enable MSAW alert transmission** is inappropriately performed (Output quality: **H** according to Table_ 4 on page 73);
4. **Issue clearance to pilot** function is performed earlier than expected when the clearance *Aircraft #1 descend altitude 4000 FT, turn right heading 230, cleared ILS2* is issued (Output quality: **D** according to Table_ 4 on page 73);
5. The remaining functions are accurately performed (Output quality: **E** according to Table_ 4 on page 73).

It is now possible to present the instantiations, to apply the methodology and to draw preliminary conclusions.

The following instantiations use the following graphical conventions:

- Grey shaded hexagons represent MSAW related functions;
- Black hexagons represent foreground functions;
- Thick-lined hexagons represent background functions;
- Dotted lines represent the output of background functions;
- Only relevant functions are represented in the instantiations.

3.6.1 Normal scenario - First instantiation

The first instantiation (Figure 25) represents the starting point for the "paper and pencil" simulation. The purpose of this graphical representation is to show how functions are coupled under certain conditions.

To represent, in a realistic way, the dynamic evolution of the scenario, it would be necessary to present a sequence of instantiations where functions are performed and couplings arise as time goes by. For practical reasons, in Figure 25 all the couplings between the functions are presented as if they were established at the same time. Despite being formally inexact, this representation serves to show how functions are instantiated. The same applies to Figure 26 on page 112 and to Figure 27 on page 113 as well.

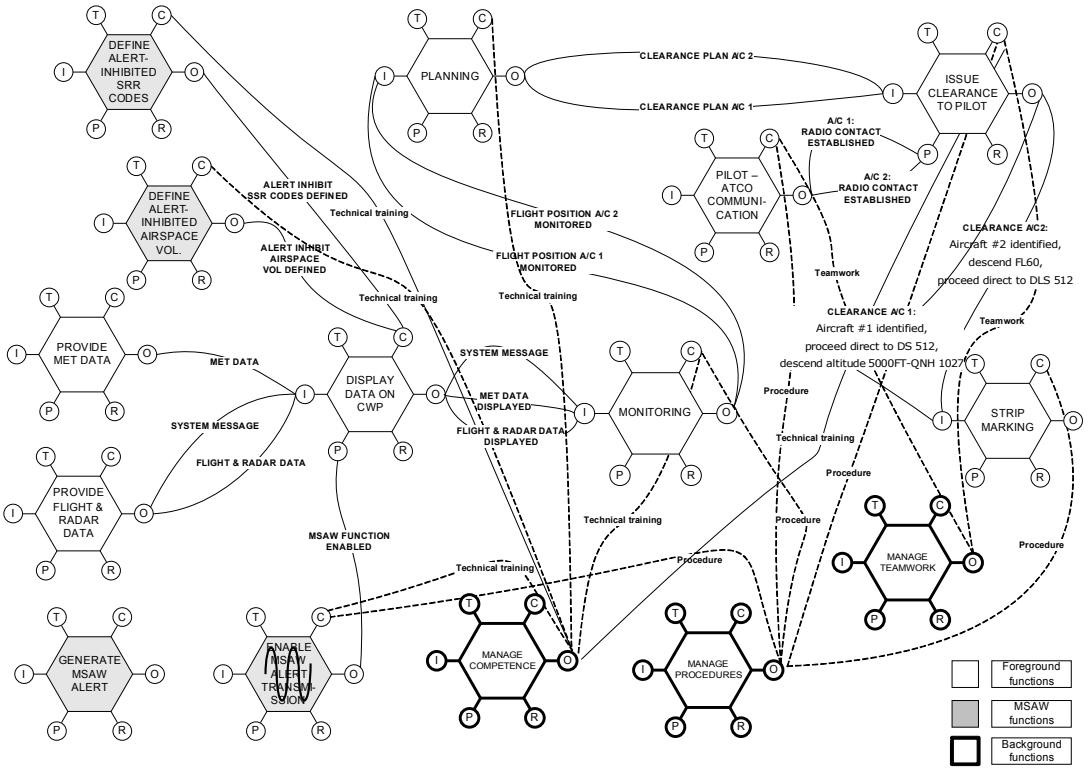


Figure 25: Normal scenario – First instantiation

Using the above mentioned assumptions, the non-accurate enabling of MSAW alert transmission introduces potential performance variability in the system. But the performance variability is not actuated since there is no need for a MSAW alert in the scenario at the time. Pilots are instructed to start their descent and to proceed directly to DLS 512.

3.6.2 Normal scenario- Second instantiation

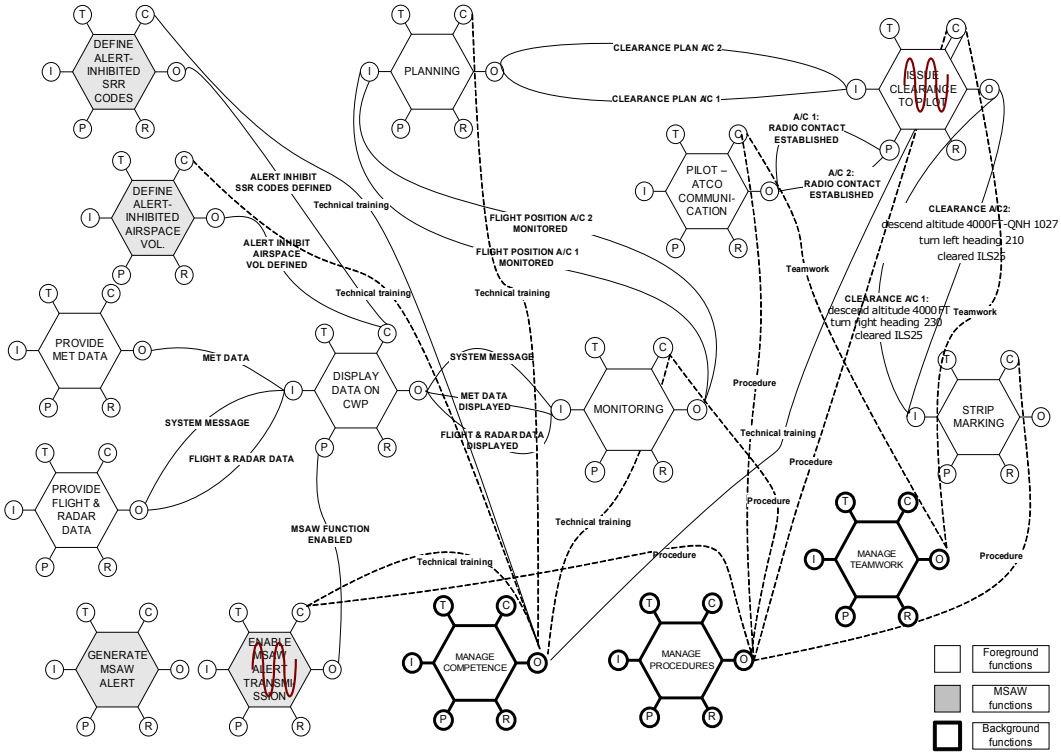


Figure 26: Normal scenario - Second instantiation

The second instantiation for the normal scenario represents the temporal evolution of the previous situation.

In this instantiation, two additional clearances are issued to pilots. Pilots are instructed to descend to 4000 FT- QNH 1027. Aircraft #1 has to turn right heading 230 and ILS25 is cleared. Aircraft #2 has to turn left heading 210 and ILS25 is cleared. The clearance *Aircraft #1 descend altitude 4000 FT, turn right heading 230, cleared ILS2* is anticipated (Output quality: **D**).

3.6.3 Normal scenario – Third instantiation

In the third instantiation an alert is calculated, but not displayed on the Controller Working Position because Preconditions are not satisfied.

The **Monitoring** function therefore receives:

- Appropriate and on time aspect from the **Provide Met. Data** (Output quality: **E**);

- Appropriate and earlier flight data for Aircraft #1 from the **Provide Flight Data** (Output quality: **D**);
- Inappropriate and on time data from the MSAW function (Output quality: **H**).

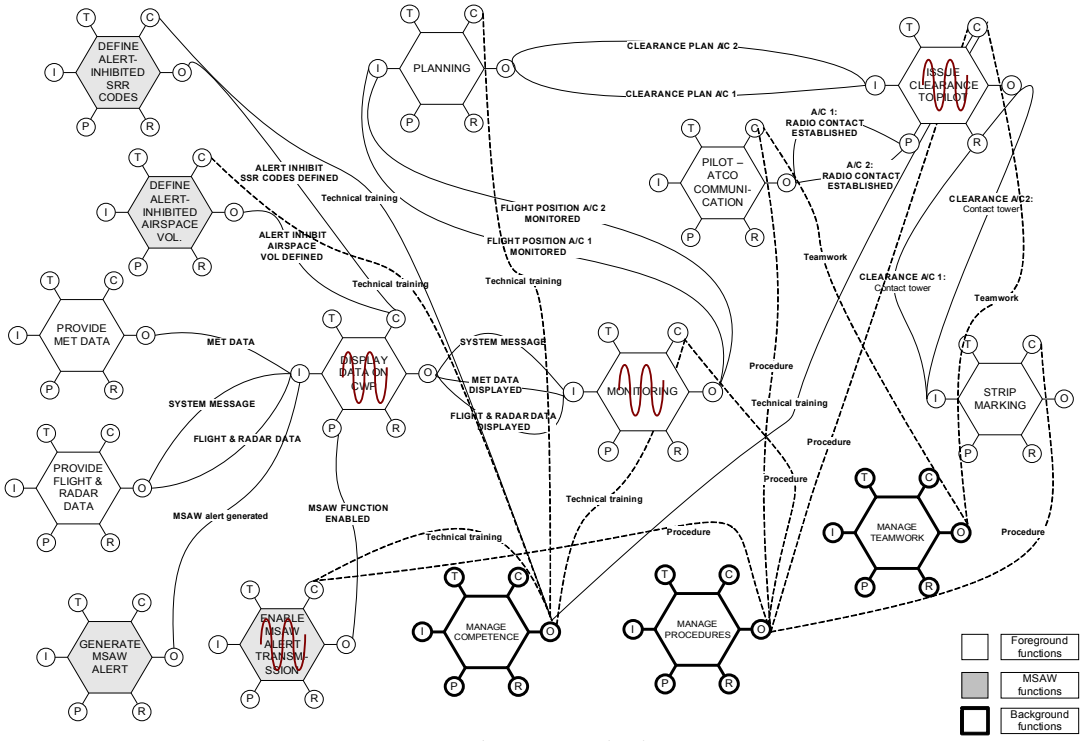


Figure 27: Normal scenario - Third instantiation

For this instantiation, the application of the methodology deserves detailed discussion.

The **Monitoring** function needs – according to the description in Table_ 18 – the following aspects.

Table_ 18: Monitoring function description and variability assessment

Monitoring			
Input	Flight data displayed	D	+1
	Radar data displayed	E	+2
	MSAW alert displayed	H	- 2
	System message displayed	E-	+2
	Strip marked = [initial call; clearance; plane released to next sector; frequency changed]	E	+2
Output	Flight position monitored = [entering the sector; flight in the sector heading towards (x); leaving the sector]		
Control	Monitoring procedures	E	+2
	Technical training	E	+2
	Working conditions	E	+2
	Adjustment of data display	E	+2
Time		–	–
Preconditions	FDPS updated	E	+2
	Interface design	E	+2
Resources	Situation data display equipment	E	+2
	Additional data display	E	+2

The right hand side columns contains the evaluation of the quality of the aspects with their associated scores (as presented in Chapter 3) for the dampening potential of the function. Positive scores mean that the function has the potential to damp performance variability. Negative scores means that the function has the potential to increase performance variability.

To evaluate the performance variability of the **Monitoring** function, using the methodology proposed in Chapter 3, it is necessary to calculate the median of aspects' quality effect on performance.

In this case, the median of those is +2.

This value for the **Monitoring** function is in the range of quality **A** or **E.** This means that the output can be either Precise-Too early or Appropriate-On time. As mentioned in Chapter 3, it is now necessary to distinguish between the two options.

According to the scenario we can imagine that the output will have a degraded precision (Appropriate), but be on time.

3.7 Discussion about results

The example shown above demonstrates how the FRAM allows the identification and characterisation of potential performance variability in the **Monitoring** function using a set of realistic assumptions.

With respect to the traditional safety assessment performed by DFS this result could be considered from two points of view: as an emergent risk and/or as the positive contribution of performance variability to system safety.

That the **Monitoring** function can produce an appropriate (rather than precise) output is a clear example of how risks could emerge from the combination of performance variability arising from multiple functions. The degradation and therefore the risk of something going wrong does not result from a direct cause-effect link between a MSAW function and the **Monitoring** function. It emerges from the combination of performance variability deriving from functions that are not even directly coupled together but, in a complex socio-technical system, any function may affect any other function in the system.

These risks cannot be identified with a traditional safety assessment method since, as illustrated, the analysis is limited to the new system, i.e. MSAW. In addition, using a bimodal classification of performance (discussed in Chapter 2) where performance can only be correct or faulty emergent risks cannot be identified because the identification of a erroneous performance constitutes the risk and a correct performance is assumed to be neutral to system safety.

This point leads to the second perspective for discussion of the methodology for the evaluation of performance variability.

The dual role of performance variability has been discussed in Chapter 2. Performance variability is at the same time a risk and an asset for the safety of complex, intractable, underspecified socio-technical systems. Thus it is useful to discuss, for the example presented, the positive role of performance variability.

The inappropriate enabling of the MSAW alert transmission, if identified during a safety assessment, would normally been addressed as a human error and some kind of classical barriers (e.g. training, specific HMI etc.) would be introduced. Those countermeasures are indeed important and have proved to be – to certain extent – effective. But they do not prevent performance variability occurring.

The possibility that functions can damp performance variability (as presented in Chapter 3) is an important alternative approach to manage performance variability (and its negative effects). In this example, an initial problematic event is not handled by labelling it as human error and ending the analysis.

From a performance variability perspective that the event is partially damped or compensated for by other functions in the system. The methodology is able to identify the dampening capability of functions in the system, and therefore their positive contribution to system safety.

Conclusion

This chapter presented an evaluation of the methodology developed in Chapter 3. The evaluation is based on the application of the methodology to a safety assessment study for the German Air Traffic Management system and in particular it is focused on the identification of risks due to the introduction of a ground based safety net system.

The methodology can be evaluated in two respects: its applicability and its capability to identify risks in comparison with a traditional safety assessment.

Applicability of the methodology. The Minimum Safe Altitude Warning case study demonstrates the application of the methodology for safety assessment. The case study illustrated, in the first instance, the process of functions identification and description conducted in collaboration with experts in the domain. The main challenge here is the need to make Air Traffic Controllers explain the normal, and not the nominal, way the work is done. Therefore analysts and domain experts must share a common view on safety and human performance. In order to achieve a neutral system description the traditional focus on failures and human errors must

be put to one side. The Resilience Engineering perspective, and in particular the notion of performance variability as a common source for success and failure, has to be accepted.

Once this step is accomplished, the methodology presented in Chapter 3 can be applied in a relatively straightforward way for a simplified safety assessment study. Its application to an extensive safety assessment case would require the development of a software able to account for the multiple interactions between functions and their reciprocal influences.

Its functional characteristic makes the methodology easy and practical to use. An existing FRAM model could be easily updated and the introduction of new functions (as well as their exclusion) does not require remodelling of the entire socio-technical system. The identification of background functions has been shown to be successful in tackling the issue of contextual influence on performance. The choice of a simple but robust indicator to aggregate several aspects influencing performance has been proved to be satisfactory.

Risk identification capability. The application of the methodology for the safety assessment study presented in this chapter sheds some lights on the potential of the FRAM, improved with the proposed methodology, to identify risks and to assess the role of performance variability for system safety.

As it is possible to compare this research with the official safety assessment some general concluding remarks are in order. As already discussed, the official extensive study performed for Deutsch FlugSicherung was mainly focused on technological hazards and human errors. The safety assessment study was only concerned with the effects of the introduction of the MSAW in the existent ATM system. This reduced the analysis to a relatively small part of the socio-technological system. Therefore the hazards identification process was based only on risks directly related to the implementation, maintenance and operation of the MSAW.

On the other hand, the FRAM and the proposed methodology looked for risks due to the combination of variability of normal performance rather than to system failures or breakdowns. The example illustrated how an inappropriate enabling of

the alert transmission in combination with a "trivial" anticipation of a clearance could result in degraded performance of the **Monitoring** function.

It is only possible to achieve this kind of results with a systemic functional analysis of the socio-technical system. The established safety assessment approach, one which analyses the MSAW system and not its effect on the normal performance, was not able to identify this typology of risks.

It has nevertheless to be recognised that the methodology does not take into account for technological failures. It is therefore important to clearly state that this methodology, even in a more mature version, should be considered as a complement to reliability analysis methods.

Chapter 5: Conclusions and Perspectives

Page intentionally left blank

Résumé du Chapitre 5

Le cas de MSAW présenté au Chapitre 4 a été utilisé afin d'évaluer l'applicabilité et les capacités d'identification des risques de la méthodologie de la *Functional Resonance Analysis Method* exposée au Chapitre 3. Les conclusions de cette thèse et ses implications pour la gestion de la sécurité sont examinées dans ce chapitre final, dans lequel deux perspectives de recherche ont été envisagées.

Les conclusions générales sont suivies par des conclusions plus spécifiques en ce qui concerne les acquis théoriques (i.e. les différentes perspectives d'analyse), des questions qui emerge dans le deroulement de cette recherche, et les réalisations pratiques (i.e la valeur ajoutée de la méthodologie développée).

Une perspective est aussi envisagé: l'intégration d'une estimation de la sécurité, basée sur la Résilience, dans les approches actuelles en matière de sécurité pour la Gestion du Trafic Aérien.

Introduction

The MSAW case presented in Chapter 4 has been used to evaluate the applicability and the risk identification capabilities of the Functional Resonance Analysis Method methodology developed and presented in Chapter 3. The conclusions of this thesis and their implications for safety management are discussed in this final chapter, where two research perspectives are presented.

General conclusions are followed by a more specific discussion of the theoretical aspects (i.e. the different perspective of the analysis,), some emerging questions, and practical achievements (i.e. the added value of the developed methodology).

A research perspective with practical implication is as well proposed: the integration of a Resilience-based safety assessment into current safety approaches for Air Traffic Management.

1 Conclusions

This thesis demonstrated the need of Air Traffic Management for the development – and the application – of systemic safety assessment methods to account for performance variability. Air Traffic Management, like many others complex socio-technical systems, requires performance to be variable because conditions cannot be completely specified. Therefore the positive effect of performance variability on the functioning of the system has to be acknowledged. But performance variability can combine in unwanted and unpredicted ways and therefore also represents a danger for safety. Thus, it is necessary that performance variability be thoroughly evaluated during safety assessment.

The Functional Resonance Analysis Method has been used in the past to model, with a systemic functional approach, complex socio-technical systems for accident analysis and safety assessment purposes (e.g. Woltjer & Hollnagel, 2007; Lundblad et al., 2008, Rome, 2009). This thesis contributes to the development and improvement of the FRAM by the development of a methodology to account for:

1. The heterogeneity of functions performed in socio-technical systems (Human, Technological and Organisational);
2. The variability of normal performance due to local adjustments, i.e. performance variability induced by systemic factors;
3. The practical need to achieve an aggregated representation of performance variability for safety assessment.

As a socio-technical system is composed of different typologies of functions it is necessary to distinguish the different ways they are affected by performance variability. This thesis applies the MTO framework to address the first point on the above list. Human functions are most subject to performance variability since they are the ones where the role of the human is prominent and it is up to humans to deal with unpredicted conditions. Technological functions are - or should be - less variable. Technology is designed to be stable and reliable, and it's ability to adapt and adjust to current conditions is negligible. Organisational functions have more

inertia (compared to daily activities) and can be considered stable over a relatively long period of time (e.g. to change procedures or to change the quality of teamwork are good examples of how long that period of time could be).

This thesis has also introduced the notion of foreground and background functions. Foreground functions being the focus of the analysis while background functions represent the relative context for the performance of foreground functions.

To account for the performance variability due to local adjustments made to meet performance demands, this thesis developed a methodology which recognises that each function, in a socio-technical system, produces an output with a certain quality (Precise – On time, Accurate – On time, Precise – Delayed etc.). In a socio-technical system, functions are coupled together, in the sense that every Output is used, as Input, Resource, Precondition, or Control by a downstream function. The more a function has at its disposal good quality Inputs, Resources, Preconditions and Controls, the less it has to adjust to them, and the more it is able to absorb the effect of incoming variability. On the contrary, the less Inputs, Resources, Preconditions and Controls are of good quality the more the function has to adjust to them. Its performance variability will be high and the the quality of its output will be degraded.

The third point developed in this thesis concerns the need to achieve an aggregate value to represent the performance variability of a function. This practical step is required to actually perform safety assessment. An aggregate value is much easier to interpret and it is much more manageable than a list of multiple indicators.

1.1 Conclusions: Theoretical achievement

The historical development of safety approaches, and associated safety assessment methods, from the age of Technology to Resilience Engineering, shows how thinking about safety has changed in relation to the evolution of technology and organisation.

Up to the age of Safety Management, the changes in safety approaches concerned mainly a broader scope of analysis. From being focused on technology, models and

methods acknowledged the need to include humans and organisations in the identification of hazards and safety assessment. This acknowledgement required accident models to change from being linear to being epidemiological, i.e. to recognise the contribution of multiple factors to accidents. Despite the great changes which took place in their development, safety approaches shared a common point: models and methods were interested exclusively in negative organisational outcomes, i.e. catastrophes, accidents, incidents, near misses etc.

The Resilience Engineering approach, driven by the need to improve safety management in modern complex-tightly coupled organisation, instead of simply adding a new layer to safety analysis introduced a different perspective.

The main contribution of Resilience Engineering, or at least the most important for this research, consists in highlighting the need to understand the normal performance of socio-technical systems to improve safety. This point triggers a series of other arguments about safety. Understanding normal functioning requires an acknowledgement that complex socio-technical systems are intractable and therefore their performance conditions usually underspecified. In this context, humans have to adjust their performance to cope with actual conditions,to ensure the functioning of the system. These adjustments result in performance variability that is considered as an asset (as well as a potential hazard when it combines in unexpected ways) to system safety.

Adopting a systemic perspective, performance variability is due to local adjustments made to meet performance demands. The need to stretch resources to meet performance demands or to substitute goals to deal with unpredictable events are the reasons why performance variability is influenced by systemic factors. The Efficiency-Thoroughness Trade Off principle constitutes an appropriate theoretical framework to explain the influence of systemic factors on performance variability.

Recognising performance variability and understanding its role in safety imply a major change in thinking about the human role in socio-technical systems. When performance is variable the pivotal notion of Human Reliability, i.e. human error, is no longer necessary to explain human behaviour and its consequences. When

adjustments are required to ensure the normal functioning of the system, how those adjustments should be considered? Since formally they are deviations from norms and procedures, they should be considered errors. But that is only the case when something goes wrong. In the majority of cases their existence is simply ignored. Swain (1989) defines human error as "*any member of a set of human actions that exceeds some level of acceptability, i.e. an out-of tolerance action where the limits of human performance are defined by the system*."

Hence acceptability levels for human performance are defined by the system, and when systems are underspecified, acceptability levels cannot always be specified. What is successful and acceptable under certain conditions, might be unsuccessful under different ones. To avoid this ambiguity, it is more straight forward to refer to performance variability, rather than to human error.

Safety assessment methods should therefore been able to identify and evaluate performance variability. If they fail in doing so organisations will remain exposed to emergent risks, which are unpredictable using failure based approaches.

1.2 Conclusions: Practical achievements

The Functional Resonance Analysis Method (FRAM) satisfies, the theoretical requirements for a safety assessment method that aims to evaluate the variability of normal performance. The FRAM, described towards the end of Chapter 2, and the original methodology for performance variability evaluation can be improved by the contributions presented in Chapter 3. This thesis improves the FRAM by the development of a methodology to:

1. Differentiate between the performance variability of heterogeneous functions;
2. Represent the performance variability due to local adjustments, i.e. performance variability induced by systemic factors;
3. Achieve an aggregated representation for performance variability.

The methodology has been tested in a safety assessment case study for the German Air Traffic Management system. The introduction of the ground based safety net

called MSAW, has been assessed with the FRAM. In a realistic scenario, the methodology has proved its ability to identify emergent risks and the human contribution to safety. A comparison of the results with the official safety assessment study performed by DFS allowed some preliminary conclusions to be drawn about the applicability and the power of the method.

The MSAW case demonstrated that the method is fully applicable in safety assessment and some advantages have already been mentioned. The most important point, in this respect, is the ease with which a FRAM model can be updated as required. The functional approach of the method ensures that the introduction of new technical systems or of new functions does not require a completely new model to be built. New instantiations have to be created, but this process is more effective than what is the case with a traditional methodology. The introduction of a set of background functions, identified by starting from the set of foreground functions, reduces the effort needed to evaluate extensive lists of contextual factors. Finally, aggregating the effect of the aspects into a single representation for performance variability is an effective solution to the question of how to achieve an operative method.

As for the capability to identify emergent risks, the MSAW case showed that the methodology is valuable. The identification of a potential risk (quality degradation of the **Monitoring** function) in a function not directly related to the MSAW suggests that the methodology can be successfully applied. The scenario also showed how performance variability might be damped within the system. This point is extremely important because it offers a way to assess the positive contribution to system safety. Safety assessment, as recognised by the approach developed by EUROCONTROL (Fowler, Perrin & Pierce, 2009) presented in Chapter 1, requires the identification of both positive and negative contributions to risks.

As mentioned towards the end of Chapter 4, the FRAM, consistent with the Resilience Engineering approach, is focused on risks due to the combination of performance variability. It is not suited to technical reliability analysis. Therefore the method has to be considered as complementary to, rather than as a substitute for,

the traditional and established safety approaches. The integration between this approach and the EUROCONTROL approach is presented in section 3.1 of this chapter.

2 Emerging questions

Four theoretical and operational issues emerged during the development and application of the methodology for assessing performance variability in complex socio-technical systems.

The first question is related to the management of performance variability and to its negative effect on systems' integrity and safety.

A second issue concerns the limitations of the methodology for evaluating performance variability as presented in this research. Limitations are related to the justification of the methodology, to the relative importance of the FRAM aspects (Input, Output, Time, Control, Resources, Precondition) and to the use of the median as an aggregator.

Data collection for this research, and for safety assessment in general, is a further point deserving to be discussed.

A final point is related to the need for safety assessment method to be efficiently usable.

This section does not want to provide exhaustive and comprehensive responses to the above mentioned points, rather its scope is to clarify certain aspects of this research and to point towards future research developments.

2.1 Management of performance variability

The methodology presented in this research aims at modelling performance variability in a complex socio-technical system. Once performance variability is identified and modelled, the following logical steps are:

1. to manage it; and
2. to prevent it becoming a problem for system's integrity and safety.

At the current stage of development, the methodology does not propose any acceptability levels for the combination of performance variability. It is important to remember that the analysis of performance variability has to be done at the level of foreground functions. The performance variability can be relatively small but the emergence of the so-called resonance effect has to be envisaged. In order to a-priori assess under which circumstances the combination of performance variability can become problematic for system safety, the identifications of critical functions for system's functioning is one possibility. For those functions, acceptability thresholds should be defined.

In order to prevent that performance variability exceeds the acceptability thresholds, it has to be effectively managed by the organisation. In the original description (Hollnagel, 2004), the Functional Resonance Analysis Method comprises five steps, four of the which have so far been developed at a practical level. The fifth step concerns the definition and implementation of effective countermeasures to manage performance variability.

The defence-in-depth tradition consists in the definition of multiple layers of barriers introduced into the system to prevent human errors and failures and to protect the system from their effects. According to this view, physical, functional, symbolic and immaterial barriers are meant to protect systems from the brittleness of humans, and conversely to protect humans from the less-than-perfect predictability of the system functioning (Hollnagel, 2004). Also barriers ought to mitigate risks by constraining performance, reducing discretion and therefore performance variability.

Actually, this thesis has demonstrated that performance variability has to be managed rather than reduced or eliminated since it constitutes an asset as well as a danger to the safety and functioning of complex socio-technical systems.

In order to be managed, performance variability first has to be monitored. This requires the identification and development of sets of appropriate indicators. Their interpretation allows conclusions to be drawn about the safety level and supports

the prediction of the occurrence of future events (Figure 28 is a FRAM specific version of Figure 1 presented on page 20).

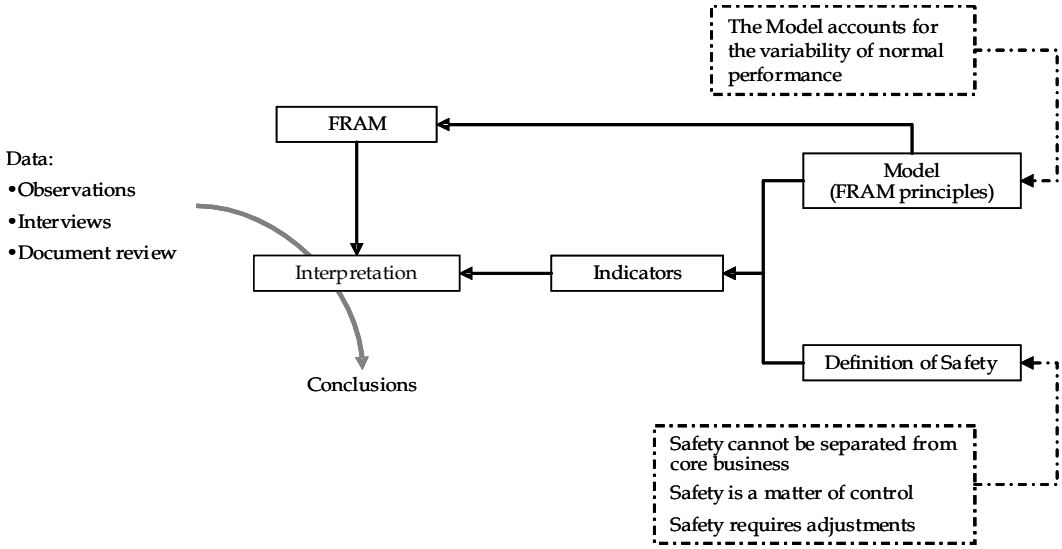


Figure 28: Relation between safety definition, model and indicators – FRAM specific version

The selection of indicators is often a pragmatic affair representing a combination of operational and meaningful factors – or a trade-off between efficiency and thoroughness. In some cases their validity is empirical (or statistical), i.e. it refers to an extensive set of observations, specifically of correlations between two events or data sets. The literature offers extensive lists of this kind of performance indicators (Tarrants, 1980; TGRE, 2004; Kjellen, 2000; Wreathall, 2006, 2007; Webb, 2009). Yet few of these documents, if any, discuss the reasons behind the selection of the indicators. Although it is more important that indicators are meaningful than easy to use, indicators are often selected because they are simple. In order to avoid this, it is necessary to find a proper balance between measurably and meaningfulness.

The FRAM could support the identification of meaningful performance indicators by the identification of the relevance of functional coupling for performance variability. With a set of instantiations it is possible to understand the dynamics of the system and and its likelihood to resonate.

2.2 Methodological limitations

The proposed methodology is the first attempt to evaluate performance variability

in a socio-technical system by means of the Functional Resonance Analysis Method. Ordinal values are proposed to represent the potential a function has to dampen or increase performance variability. The central aspect of the methodology consists in the possibility to represent both the dampening and the increasing potential of a function. Such potential is then transformed during the instantiations of the model. The simplification done by using the set of ordinal values is compensated by the advantages to have a methodology that can be used for safety assessment. Despite its limitations, it constitutes the first step toward the development of a more precise evaluation of performance variability.

The same argument is valid for the choice of the median as an aggregator. The practical need to achieve an aggregated representation for performance variability led to the selection of a simple and robust indicator. As previously mentioned, it is a simplification of reality, but it has been judged appropriate for the exploratory attempt to model and to evaluate performance variability with the FRAM. In future developments of the method, a more accurate and sensible way to evaluate performance variability has to be envisaged. The use of fuzzy logic is a possible solution.

A further issue deserves to be here discussed. The methodology assumes that all aspects have the same potential impact on performance variability, i.e. that a degraded Input has the same effect as a degraded Control or Precondition. It is reasonable to consider this as yet another simplification of reality. To obtain a more realistic representation of how performance variability emerges, it is necessary to gather more knowledge and insight on the actual effects of the coupling between functions. In his doctoral thesis, Runte (2010) identifies several facilitators of local adjustments, i.e. of performance variability. To establish a connection between those facilitators and the FRAM aspects, seems like a promising approach to understand how much each aspect can increase or dampen performance variability or, in other words, how much each aspect "weighs".

2.3 Field data collection

In this research, the identification and description of the functions has been done by

means of field observations and interviews with domain experts. In total, fifteen days were spent at DFS premises situated in Langen, Germany. Two objectives were pursued during the field study:

1. to get acquainted with the challenges and the specificities of the Air Traffic Management domain;
2. to check if the FRAM model was consistent with the real activities performed by Air Traffic Controllers.

The interviews done with Air Traffic Controllers (nb. 6) and with MSAW system experts (nb. 3) have been used to constitute a consistent set of functions, that is sufficient for the modelling of the landing approach scenario.

In order to build a FRAM model for safety assessment, both interviews and observations have to be focused on the day to day functioning of the system.

2.4 Efficiency of the analysis

Critical aspects for any method are its efficiency and its ease of application. At the current stage of development, the safety assessment process with the FRAM can be improved with respect to efficiency. The safety assessment case study performed in this research has been based on a time and effort consuming paper and pencil simulation. A requisite for the adoption of the FRAM for safety assessment in safety-critical organisations is to improve its efficiency. The development of a software to run simulations represents, at the moment, the best option to reduce the cost of analysis. The availability of a FRAM software will also contribute to improve the precision of the method. In order to tune and improve the method, it will be possible to run several computerised simulations changing the parameters of the simulation and the aspects of the functions. For performing safety assessment, the data collection has to obey one main criteria: data shall be about work-as-done. Runte (2010) refers to the French ergonomics tradition for the analysis of work practices when the scope of the analysis is the identification of the characteristics of work as it is performed, at a specific point in time and under specific conditions (Leplat, 1997).

3 Perspectives

This research offers a perspective for the integration of the FRAM or, in more general terms, of any Resilience Engineering approach, into current safety assessment. Since the Air Traffic Management domain constitutes the context of this research, the possibilities for integration have been explored with respect to the EUROCONTROL safety approach described in Chapter 1.

3.1 Perspectives for integration

In this section, the perspectives for integration between a traditional and a Resilience Engineering safety assessment method are explored, taking as an example the EUROCONTROL methodology. As described in Chapter 1, EUROCONTROL is currently promoting a safety assessment plan to ensure that the massive changes expected before 2020 will not impact the safety level of European skies. These changes will be implemented through the SESAR programme, the purpose of which is to define, design, and deliver the operational and technological changes necessary to achieve a more efficient, better integrated, more cost-efficient and more environmentally sustainable European ATM infrastructure by the year 2020 (EUROCONTROL, 2009).

In order to draw guidelines for the integration of the FRAM, or of any other Resilience Engineering based method, into EUROCONTROL safety assessment plan, it is necessary to remember the basic principles of the current EUROCONTROL safety assessment. Then the identification of connecting points will allow the identifications of possibilities for integration.

The EUROCONTROL approach is:

1. Focused on the identification of positive and negative contributions to risks of safety barriers;
2. Based on safety cases composed of sets of *Arguments* and *Evidences*;
3. Built on the Logical Model: which is a *"..high level representation of the system design that it is entirely independent of the eventual physical implementation.."*

4. Checked for correctness by a Thread analysis

The main problem with the Logical Model is that, by definition, it is a high-level description of the system design that is entirely independent of the eventual physical implementation of that design. This is, of course, necessary for the safety assessment to be manageable, but it also means that the correspondence between the Logical Model and the system that is actually implemented will be less than perfect.

The imperfect correspondence is due to the specification of both technical and human-organisational functions. This thesis stressed the point that human performance cannot be completely specified as procedures can never cover all eventualities, but always require some kind of judgement for their execution. As an example, the PANS-OPS (Doc 8168), Part VIII, Chap 3, Para 3.1.2 states:

> *Nothing in the procedures specified in 3.2, "Use of ACAS indicators", shall prevent pilots-in-command from exercising their best judgement and full authority in the choice of the best course of action to resolve a traffic conflict or avert a potential collision.*

In other words, pilots should follow the guidelines except in cases where their sound judgement tells them not to. While this certainly makes sense, it also means that it becomes impossible *a priori* to know what a pilot will do in a situation.

For any but the most trivial systems it is simply impossible to provide full specifications. As described in Chapter 1, underspecification is a near-universal condition that affects every phase of a system's life-cycle, including the safety assessment. The Logical Model refers to a nominal description of the future architecture and functioning of the ATM system. Because of the unavoidable underspecification of the Logical Model, and indeed of *any* model, it is inevitable that the understanding of the system is lacking in some aspects.

The possibilities of combining the Resilience Engineering approach with established safety assessment practices can be explored from three different perspectives:

1. Can the Resilience Engineering perspective contribute to the definition of the Logical Model?

2. Can the Resilience Engineering perspective overcome the consequences of the underspecification of the Logical Model?
3. Can the Resilience Engineering perspective contribute to the management of performance variability?

3.1.1 Can the Resilience Engineering perspective contribute to the definition of the Logical Model?

As previously explained, the Logical Model is by definition a high-level, hence simplified representation of how the actual system is supposed to function. Being a high-level representation of a complex, dynamic, and tightly coupled socio-technical systems, such as the ATM, it is inevitably incomplete and underspecified.

A Resilience Engineering perspective cannot directly be used to propose changes to the definition or use of the Logical Model. But it can help to understand the possible shortcomings of the Logical Model and the consequences that may arise.

By its symbolic nature, a Logical Model does not account for the variability of (human) performance that is an unavoidable consequence of the underspecification of ATM. The Resilience Engineering approach to safety assessment suggests a way of taking into account performance variability. The improved methodology for the evaluation of performance variability, introduced and explained in this thesis, can support the identification of potential shortcomings and potential couplings among functions which the Logical Model is not able to spot.

3.1.2 Can the Resilience Engineering perspective overcome the consequence of the underspecification of the Logical Model?

The underspecification of the Logical Model means that there is a gap between the way it describes human tasks and the way in which the tasks are actually carried out. This thesis has highlighted and stressed the essential contribution of performance variability in filling in these gaps.

As previously mentioned, a Logical Model is not intended to account for performance variability since it relies on a nominal description of system functioning.

The Resilience Engineering perspective recognises the need to expand the focus of analysis that is the basis of the Logical Model, with information concerning the normal functioning of the system. In this manner, the theoretical aspects of the Logical Model can be supplemented by some practical information that will broaden the scope of the model.

The Functional Resonance Analysis Method has been demonstrated to be capable of modelling the normal functioning of the ATM system, including the performance variability. Its application clearly demonstrated the potential of the method to identify risks due to combinations of variability of normal performance. The application of the FRAM can therefore provide the necessary knowledge to achieve a more realistic ATM model. In addition the FRAM can highlight the potential gaps due to the underspecification of the system and can support the identification of emergent risks that a traditional approach is not likely to identify.

3.1.3 Can the Resilience Engineering perspective contribute to the management of performance variability?

The Logical Model constitutes a powerful representation of the nominal functioning of the system, but it is a representation that cannot be completely specified. In the underspecification of the Logical Model there is the space – and need – for performance variability.

Because performance variability is needed for coping with the complexity of the Air Traffic Management domain and for meeting its performance demands, it should not simply be constrained or eliminated. Therefore, the safety assessment challenge becomes to find effective ways to identify, model and manage performance variability.

The main focus of this thesis has been on the improvement of a method specifically centred on the issue of performance variability. The FRAM, belonging to the Resilience Engineering approach, clearly has the potential for the modelling and management of performance variability. The information from an incident database could be used to identify functions affected by performance variability. The use of retrospective data is a powerful means to support the identification of potential

performance variability even if the collected incident data normally refer to human error rather than performance variability. Therefore, a change in the methodology is required to do incident analysis so that more appropriate information could be gathered.

Final thoughts

The long and honoured tradition of safety assessment methods is rooted in the need to make technological systems safe. For systems that were completely specified, the approach based on decomposition of systems and arguments in an orderly and logical manner was successful. Complete knowledge of the functioning of the components of the systems, allows the distinction between correct and incorrect outputs and their structural analysis. It is a powerful means to prevent negative events. Safety assessment methods have, and often still do, rely on event trees representations of failures and their combined effect on system safety. For those methods the central problem was to determine and calculate the probability of failures and the probability that a combination of failures could result in accidents or incidents. With the technological and organisational evolution of industrial systems, the structural approach started to manifest its limits.

The complexity and the tight coupling characterising most of modern industrial domains, the increased use of software and information technology, and the actual way in which socio-technical systems perform requires the adoption of a different approach to safety.

Since the age of Safety Management alternative perspectives on safety have been proposed. Concepts like “Drift into failures” (Rasmussen, 1997), “Normal deviations” (Vaughan, 1996) and “Man-made disasters” (Turner, 1978) raised awareness that organisational factors have to be considered, and they introduced models where, to identify risks and explain accidents, the actual performance of the system was described.

The observation of adverse outcomes, in absence of failures or malfunctions, proves right Perrow's theory (1984) about normal accidents for systems that cannot be

completely specified. To address emergent risks, typically resulting from the combination of performance variability, the structural approach is not enough. The functional approach, adopted by the Functional Resonance Analysis Method, helps us to understand not only how functions can fail, but also to describe how functions are actually performed to assure the normal functioning of the system. The consideration of normal performance, which might be – and normally is – different from its normative description, highlights the limitations of being focused exclusively on negative events resulting from deviations from the prescribed rules and procedures. The Resilience Engineering, as the Normal Accident Theory did in 1984, recognises, the nature of socio-technical systems as one of the reasons for incidents and accidents. The important difference is the attitude towards this problem. Another added value of Resilience Engineering approach consists is the attempt to engineer methods to support the systemic management of risks and to be active in tackling this challenge.

The Efficiency-Thoroughness Trade Off principle offers a valuable approach to understand human behaviour as it tries to represent the intention-driven nature of human behaviour. To describe humans, as the only competent and intelligent components of a socio-technical system; flexible and able to adjust their behaviours to cope with a dynamic system, will allow the identification of the positive contribution of humans to system safety.

The Resilience Engineering perspective and the ETTO principle have been used in this research to contribute to the development of the FRAM as a safety assessment method, and to provide industries with an operative tool to improve their safety management.

Page intentionally left blank

References

Page intentionally left blank

Bateson, G. (1979) *Mind and Nature. A Necessary Unity*: Bantam Books.

Bourrier, M. (1996). Organizing Maintenance Work At Two American Nuclear Power Plants. J*ournal of Contingencies and Crisis Management.* 4 (2), 104-112.

Bourrier, M. (1999). Constructing organisational reliability: the problem of embeddedness and duality. In J. Misumi, B. Wilpert, R. Miller (Eds.),*Nuclear safety: A human factors perspective.* London: Taylor & Francis

Brehmer, B. & Allard, R. (1991) Real-time dynamic decision making: Effects of task complexity and feedback delays. In J. Rasmussen, B. Brehmer, and J. Leplat (Eds.) *Distributed decision making; Cognitive models for cooperative work*. Chichester: Wiley.

Cacciabue, P. C. (2004). *Guide to applying human factors methods: Human error and accident management in safety-critical systems*. London [u.a.]: Springer.

Cornack, S. (1978) The structure of the systems paradigm. In *Progress in Cybernetics and Systems Research,* vol. 4, 139-148, 1978.

Cox, T., & Griffiths, A. (2005). The nature and measurement of work-related stress: theory and practice. In: In: Wilson, J. R. & Corlett, N. (eds.) *Evaluation of human work*. 3rd ed. Boca Raton, FL: Taylor & Francis. pp. 553 - 571.

Dekker, S. W. A, (2005). *Ten questions about human error: A new view of human factors and system safety*. Mahwah, N.J.: Lawrence Erlbaum.

Dekker, S. W. A. (2006). Resilience engineering: Chronicling the emergence of confused consensus. In E. Hollnagel, D. D. Woods & N. Leveson (Eds.), *Resilience Engineering: Concepts and precepts.* Aldershot, UK: Ashgate Publishing Co.

De Terssac, G. (1992) *Autonomie dans le travail*. Paris: Presses Universitaires de France

Dougherty, E. M. (1990). Human Reliability Analysis - Where shouldst thou turn? *Reliability Engineering and System Safety , 29* (3), 283-299.

EUROCONTROL (2009). *Episode 3-Safety assessment plan for the safety assessment of*

the SESAR operational concept, circa 2020

EUROCONTROL (2009). Hindsight Nr. 8. http://www.eurocontrol.int/safety/gallery/content/public/library/HindSight%20Magazine/n8/hindsight_08_winter_hyperlinked.pdf

EUROCONTROL (2007). Air Traffic Safety Fact Sheet. http://www.eurocontrol.int/corporate/public/standard_page/press_fs_air_traffic_safety.html

EUROCONTROL (2003). Air Traffic Management Strategy for the Years 2000+. http://www.eurocontrol.int/eatm/gallery/content/public/library/ATM2000-EN-V1-2003.pdf

EUROCONTROL (2001) SAF.ET1.ST01.1000-POL-01-00 <http://www.eurocontrol.int/safety/gallery/content/public/EATMP%20Safety%20Policy%20-%20Edition%2021.pdf>

Fabre, D. & Macchi, L. (2009). Defining criteria to characterize activity domains: refining Perrow's assumptions. Proceedings of the 9th European Sociology Association Conference. September2-5, 2009. Lisbon, Portugal

Foster, H.D. (1993): Resilience theory and system evaluation. In J.A. Wise, V. D. Hopkin and P. Stager (eds),*Verification and Validation of Complex Systems: Human Factors Issues*. Berlin: Springer, 35-60.

Fowler, D., Perrin, E., and Pierce, R. (2009). 2020 Foresight A systems-engineering approach to assessing the safety of the SESAR Operational Concept. Eighth USA/Europe Air Traffic Management Research and Development Seminar (ATM2009)

Hale, A., & Heijer, T. (2006). Defining resilience. In E. Hollnagel, D.D. Woods & N. Leveson (Eds.),*Resilience Engineering: concepts and precepts* (pp. 31-36). Aldershot, UK: Ashgate publishing

Hale, A.R., & Hovden, J. (1998) Management and culture: the third age of safety. A review of approaches to organizational aspects of safety, health and environment. In: Feyer, A.-M., Williamson, A. (Eds.), *Occupational Injury: Risk,*

Prevention and Intervention. Taylor and Francis, London.

Hale A. R., & Glendon A. (1987) *Individual behavior in the control of danger*, Elsevier

Hollnagel, E. (1993). Human reliability analysis: Context and control. London u.a: Academic Press.

Hollnagel, E. (1998). *Cognitive reliability and error analysis method (CREAM).* Oxford: Elsevier Science Ltd.

Hollnagel, E. (2004). *Barriers and accident prevention.* Aldershot: Ashgate

Hollnagel, E. & Woods, D. D. (2005) *Joint cognitive systems: The foundations of cognitive systems engineering.* Taylor & Francis

Hollnagel, E., Woods, D. & Leveson, N. (Eds) (2006). *Resilience Engineering: Concepts and Precepts*. Aldershot, UK: Ashgate.

Hollnagel, E. (2008). Safety management-Looking back or Looking forward. In: Hollnagel, Nemeth & Dekker (Eds.) *Remaining sensitive to the possibility of failures*. Ashgate.

Hollnagel, E., Nemeth, C.P., Dekker, S. (2008) *Remaining sensitive to the possibility of failure*. Ashgate

Hollnagel, E. (2009). *The ETTO principle: Efficiency-thoroughness trade-off. Why things that go right sometimes go wrong*. Aldershot, UK: Ashgate.

Hollnagel, E. (2010). Prologue. In: E. Hollnagel, J. Pariés, D. D. Woods & J. Wreathall. *Resilience engineering in practice: A guidebook*. Farnham, UK: Ashgate.

ICAO (2006). Procedures for Air Navigation Services - Aircraft Operations - Volume I Flight Procedures - Doc. 8168 OPS/611, Fifth edition – 2006 plus Amendment 3

Johnson-Laird, P. N. (1983). *Mental models: Towards a cognitive science of language, inference and consciousness*. London: Cambridge University Press.

Kjellén, U. (2000). *Prevention of Accidents Through Experience Feedback*. London and New York: Taylor & Francis.

Kirwan, B. (1994). *A guide to practical human reliability assessment*. London: Taylor & Francis.

Lacomblez, M., Bellemare, M., Chatigny, C., Delgoulet, C., Re, A., Trudel L., Vasconcelos, R. (2007). Ergonomic analysis of work activity and training: basic paradigm, evolutions and challenges. In Pikaar R., Koningsveld E., Settels P. (Eds). *Meeting Diversity in Ergonomics.* London: Elsevier (UK).

LaPorte, T.R. & P. Consolini (1991), Working in practice but not in theory: theoretical challenges of high reliability organizations, *Journal of Public Administration Research and Theory*, vol. 1, pp. 19-47.

Leplat, J. (1997). Regards sur l'activité en situation de travail - Contribution à la psychologie ergonomique. Paris: PUF.

Leontiev, A.N. (1978). *Activity, Consciousness and Personality* Hillsdale: Prentice-Hall.

Leveson, N., Duplac, N., Zipkin, D., Cutcher-Gershenfeld, J., Carroll, J., Barrett, B. (2006) "Engineering Resilience into Safety-Critical Systems." In: E. Hollnagel, D.D. Woods, and N. Leveson (Eds.), Resilience Engineering – Concepts and Precepts. Ashgate Publishing Company, pp. 95-123 L

Lundblad, K., Speziali, J., Woltjer, R., & Lundberg, J. (2008). FRAM as a risk assessment method for nuclear fuel transportation. In *Proceedings of the* 4th *International Conference Working on Safety*. Crete, Greece.

Macchi, L., Hollnagel, E., Leonhardt, J. (2008). *A systemic approach to HRA: A FRAM modelling of Control Over Flight activity.* EUROCONTROL Safety R&D seminar. 22-24 October, 2008, Southampton, UK.

Macchi, L., Hollnagel, E., Leonhard, J. (2009).Resilience Engineering approach to safety assessment: an application of FRAM for the MSAW system. EUROCONTROL Safety R&D seminar. 21-22 October, 2009, Munchen, Germany.

McDonald, N. (2001). Human systems and aircraft maintenance. *Air and Space Europe* 3 (3-4), 221-224.

McDonald, N. (2006). Organisational resilience and industrial risk. In E. Hollnagel, D.D.Woods & N. Leveson (Eds.), *Resilience engineering. Concepts and precepts.* Aldershot: Ashgate

Minsky, M. (1986) *The Society of Mind*: Simon & Schuster.

Musatti, C. L. (1971) Studio sui tempi di cottimo in una azienda metalmeccanica. *Rassegna di Medicina dei Lavoratori, n.3, pp. 120-149*.

Oddone, I., Re, A., & Briante, G. (1981) *Redécouvrir l'expérience ouvrière* : *vers une autre psychologie du travail*? Paris: Editions Sociales.

Perrow, C. (1984). *Normal Accidents: Living with high risk technologies.* Princeton: Princeton University Press.

Rasmussen, J. (1986). *Information processing and human-machine interaction*. Amsterdam: Elsevier.

Rasmussen, J. (1997). Risk management in a dynamic society, a modelling problem. *Safety Science, 27*, 183-214.

Reason, J. (1990). *Human error.* Cambridge [u.a.]: Cambridge Univ. Pr.

Reason, J. (1997). *Managing the Risks of Organisational Accidents.* Aldershot: Ashgate

Reiman, T. (2007). *Assessing organisational culture in complex sociotechnical systems – Methodological evidence from studies in nuclear power plant maintenance organisations.* VTT publications 627.136s. + liitt.155 s. Espoo

Reiman, T. & Oedewald, P. (2009). Evaluating safety critical organizations – emphasis on the nuclear industry. Report number 2009:12. Swedish Radiation Safety Authority. <http://www.stralsakerhetsmyndigheten.se>

Rigaud, E. (2008). Formalisation d'une démarche d'ingénierie de la résilience. 16ème congrès de Maîtrise des Risques et de Sûreté de Fonctionnement - Avignon 6-10 octobre 2008

Rome, F. (2009). De l'analyse de l'accident à l'analyse du travail: Application à deux cas d'étude dans la sécurité aérienne. PhD Thesis: Ecole Doctorale "Cognition, Comportament, Conduites Humaines". Universitè Paris

Descartes.

Rosness, R., Guttormsen, G., Steiro, T., Tinmannsvik, R.K. & Herrera, I.A. (2004). *Organisational Accidents and Resilient Organisations: Five Perspectives*. SINTEF report (STF38 A 004403), ISBN: 82-14-02724-1.

Runte, E. (2010). Productivity and safety: adjustments at work in socio-technical systems. PhD Thesis: École doctorale n° 432 : Sciences et Métiers de l'Ingénieur . Spécialité " Science et Génie des Activités à Risques " Mines ParisTech

Simon, H. (1955). A Behavioral Model of Rational Choice. The Quarterly Journal of Economics 69: 99-118

SINTEF (2009) Resilience Engineering, the Sixth Perspective. A12404 ISBN: 978-82-14-04834-6

Snook, S. A. (2000). *Friendly fire: The accidental shootdown of U.S. Black Hawks over Northern Iraq*. Princeton, N.J.: Princeton University Press.

Swain, A. (1989). *Comparative Evaluation of Methods for Human Reliability Analysis.* Köln: Gessellschaft für Reaktorsicherheit (GRS) mbH.

Swain, A. (1990). Human Reliability Analysis: Need, Status, Trends and Limitations. Reliability Engineering and System Safety , 29 (3), 301-313.

Tarrants, W., E. (1980). *The Measurement of Safety Performance*. New York, USA.

Task Group on Regulatory Effectiveness (TGRE) (2004). Direct indicators of nuclear regulatory efficiency and effectiveness.

Trist, E. L. (1978). On socio-technical systems. In, Pasmore, W. A. & Sherwood, J. J. (Eds), *Sociotechnical systems: A sourcebook*. San Diego, CA.: University Associates.

Turner, B. A. (1978). *Man-made disasters*. London, England: Wykeham Publications.

Travers, J. & Milgram, S. (1969). An Experimental Study of the Small World Problem. *Sociometry*, Vol. 32, No. 4, pp. 425-443.

Tversky, A. & Kahneman, D. (1974). Judgement under uncertainty: Heuristics and biases. *Science*, *185*, 1124-1130.

Vaughan, D. (1996). The Challenger launch decision. Chicago: University of Chicago Press.

Vicente, K. J. (1999). *Cognitive Work Analysis Toward Safe, Productive, and Healthy Computer-based Work*. CRC Pr I Llc.

Webb, P. (2009). Process safety performance indicators: A contribution to the debate. *Safety Science* 47, 502-507

Woltjer, R., Hollnagel, E. (2007). The Alaska Airlines Flight 261 Accident: A Systemic Analysis of Functional Resonance. *Proceedings of The 2007 (14th) International Symposium on Aviation Psychology, April 23-26.* Dayton, OH.

Wreathall, J. (2007. Some rumblings on a framework for identifying metrics and their use in resilience. Handed out at Resilient Risk Management Course, Juan les Pins, France.

Wreathall, J. (2009). Leading? Lagging? Whatever! *Safety Science* 47, 493-494

Page intentionally left blank

ANNEXES

Page intentionally left blank

1 Annex I: Over-flight functions

Annex_I_Table 1: Provide ATC clearance to pilot function description

Provide ATC clearance to pilot	
Input	Clearance plan
Output	Clearance provided = [regulate speed; heading change; climb; descend; adjust vertical rate; intermediate level off; holding instruction]
Time	
Control	Clearance procedures Letter of agreement RT standards Warning by safety net
Preconditions	Aircraft identified Radio contact established Sector capacity = [sector capacity satisfied] Flight position = [entering the sector] Request from pilot = [regulate speed; heading change; climb; descend] Request from next sector = [flight level; speed; route; heading; flight not accepted]
Resources	Situation data display equipment Touch input device Flight progress strip RT equipment

Annex_I_Table 2: Monitoring function description

Monitoring	
Input	Meteorological data : 1. QNH; 2. Meters of visibility; 3. Wind speed; 4. Wind direction; 5. Clouds typology; 6. Heavy precipitation Flight data: 1. Call sign 2. Flight level 3. Vectoring 4. Type of aircraft 5. Airdrome of departure 6. Airdrome of destination 7. Time over target 8. Route information Strip marked = [initial call; clearance; plane released to next sector; frequency changed] Traffic situation data in next sector
Output	Flight position monitored = [entering the sector; flight in the sector heading towards (x); leaving the sector]
Time	
Control	ATC monitoring procedures Adjustment of data display
Preconditions	Flight data processing system updated Adequate HMI
Resources	Situation data display equipment Additional data display

Annex_I_Table 3: Planing function description

Planning	
Input	Flight position monitored = [entering the sector; flight in the sector heading towards (x); leaving the sector] Updated information from coordination: 1. Request from next sector = [flight level; speed; route; heading; flight not accepted] 2. Information from preceding sector = [flight level; speed; route; heading; request from pilot]
Output	Clearance plan
Time	
Control	Minimum separation criteria Letter of agreement
Preconditions	Flight position = [entering the sector]
Resources	Planner available

Annex_I_Table 4: Strip marking

Strip marking	
Input	Clearance issued = [regulate speed; heading change; climb; descend; adjust vertical rate; intermediate level off; holding instruction] Updated information from coordination: 1. Request from next sector = [flight level; speed; route; heading; flight not accepted] 2. Information from preceding sector = [flight level; speed; route; heading; request from pilot] Radio contact established Request from pilot
Output	Strip marked = [clearance; frequency change; initial call; plane released to next sector]
Time	
Control	Strip marking procedures
Preconditions	
Resources	Strip Pencil

Annex_I_Table 5: Coordination function description

Coordination	
Input	Request from next sector = [flight level; speed; route; heading; flight not accepted] Information from preceding sector = [flight level; speed; route; heading; request from pilot] System messages
Output	Updated information from coordination: 1. Request from next sector = [flight level; speed; route; heading; flight not accepted] 2. Information from preceding sector = [flight level; speed; route; heading; request from pilot]
Time	
Control	Strip marking Coordination procedures
Preconditions	Planner available
Resources	

Annex_I_Table 6: Update flight data processing system function description

Update flight data processing system	
Input	Clearance plan
Output	Flight data processing system updated
Time	
Control	System messages
Preconditions	Adequate HMI
Resources	Touch input device

Annex_I_Table 7: Provide meteorological data to controller function description

Provide meteorological data to controller	
Input	
Output	Meteorological data : 1. QNH; 2. Meters of visibility; 3. Wind speed; 4. Wind direction; 5. Clouds typology; 6. Heavy precipitation
Time	
Control	
Preconditions	
Resources	

Annex_I_Table 8: Sector- Sector communication function description

Sector- Sector communication	
Input	
Output	Request from next sector = [flight level; speed; route; heading; flight not accepted] Information from preceding sector = [flight level; speed; route; heading; request from pilot]
Time	
Control	
Preconditions	
Resources	

Annex_I_Table 9: Provide flight and radar data to controller function description

Provide flight and radar data to controller	
Input	
Output	Flight data: 1. Call sign 2. Flight level 3. Vectoring 4. Type of aircraft 5. Airdrome of departure 6. Airdrome of destination 7. Time over target 8. Route information Traffic situation in next sector Warning by safety net System messages
Time	
Control	
Preconditions	
Resources	

Annex_I_Table 10: Pilot-controller communication function description

Pilot-controller communication	
Input	
Output	Radio contact established Request from pilot
Time	
Control	
Preconditions	
Resources	

2 Annex II: Landing approach functions

Annex_II_Table 1: Enable MSAW alert function description

Enable MSAW alert	
Input	
Output	MSAW alert transmission enabled
Control	Technical training Enable MSAW alert procedure
Time	
Preconditions	
Resources	

Annex_II_Table 2: Define alert inhibit air space volumes function description

Define alert inhibit air space volumes	
Input	
Output	Alert-inhibited airspace volumes defined
Control	Procedure Alert-inhibited airspace volumes Technical training
Time	
Preconditions	
Resources	

Annex_II_Table 3: Generate MSAW alert function description

Generate MSAW alert	
Input	Flight data: 1. Call sign 2. Flight level/ Altitude 3. Vectoring 4. Type of aircraft 5. Aerodrome of departure 6. Aerodrome of destination 7. Time over target 8. Route information Meteorological data : 1. QNH; 2. Meters of visibility; 3. Wind speed; 4. Wind direction; 5. Clouds typology; 6. Heavy precipitation Obstacle model Terrain model
Output	MSAW alert generated =[GTM alert; APM alert; MRVA monitoring alert]
Control	MSAW logic Met. Data updated
Time	TV < TL
Preconditions	Flight position below MSA Flight predicted to penetrate MSA Flight position below MRVA threshold Flight position within a glidepath/ centreline protection area Flight predicted to penetrate glidepath/ centreline protection area
Resources	

Annex_II_Table 4: Define alert inhibit SSR codes function description

Define alert inhibit SSR codes	
Input	
Output	Alert-inhibited SSR codes defined
Control	List of SSR codes Technical training
Time	
Preconditions	
Resources	

Annex_II_Table 5: Update met. data function description

Update met data	
Input	
Output	MET data updated
Control	Technical training
Time	
Precondition	
Resource	

Annex_II_Table 6: Provide met. data function description

Provide met data	
Input	
Output	Meteorological data : 1. QNH; 2. Meters of visibility; 3. Wind speed; 4. Wind direction; 5. Clouds typology; 6. Heavy precipitation
Control	
Time	
Precondition	
Resource	

Annex_II_Table 7: Provide flight & radar data function description

Provide flight & radar data	
Input	
Output	Flight data: 1. Call sign 2. Flight level/ Altitude 3. Vectoring 4. Type of aircraft 5. Aerodrome of departure 6. Aerodrome of destination 7. Time over targetRoute information Radar data Traffic situation in next sector System messages
Control	
Time	
Precondition	
Resource	

Annex_II_Table 8: Strip marking function description

Strip marking	
Input	Clearance issued = [regulate speed; heading change; climb; descend; adjust vertical rate; intermediate level off; holding instruction] Updated information from coordination: 1. Request from next sector = [flight level; speed; route; heading; flight not accepted] 2. Information from preceding sector = [flight level; speed; route; heading; request from pilot] Radio contact established Request from pilot = [regulate speed; heading change; climb; descend]
Output	Strip marked = [initial call; clearance; plane released to next sector; frequency changed]
Control	Strip making procedures Technical training Working conditions
Time	
Precondition	Working conditions
Resource	Strip Pencil

Annex_II_Table 9: Display data on CWP function description

Display data on CWP	
Input	Flight data: 1. Call sign 2. Flight level/ Altitude 3. Vectoring 4. Type of aircraft 5. Aerodrome of departure 6. Aerodrome of destination 7. Time over target 8. Route information Radar data Traffic situation in next sector Meteorological data : 1. QNH; 2. Meters of visibility; 3. Wind speed; 4. Wind direction; 5. Clouds typology; 6. Heavy precipitation MSAW alert generated=[GTM alert; APM alert; MRVA monitoring alert] System messages
Output	Flight and Radar data displayed Meteorological data displayed MSAW alert displayed System message displayed Maps
Control	Alert-inhibited airspace volumes defined Alert-inhibited SSR codes defined
Time	
Preconditions	
Resources	

Annex_II_Table 10: Monitoring function description

Monitoring	
Input	Flight data displayed Radar data displayed MSAW alert displayed System message displayed Strip marked = [initial call; clearance; plane released to next sector; frequency changed]
Output	Flight position monitored = [entering the sector; flight in the sector heading towards (x); leaving the sector]
Control	Monitoring procedures Technical training Working conditions Adjustment of data display
Time	
Preconditions	FDPS updated Interface design
Resources	Situation data display equipment Additional data display

Annex_II_Table 11: Planning function description

Planning	
Input	Flight position monitored = [entering the sector; flight in the sector heading towards (x); leaving the sector] Updated information from coordination: 1. Request from next sector = [flight level; speed; route; heading; flight not accepted] 2. 2. Information from preceding sector = [flight level; speed; route; heading; request from pilot] Request from next sector = [flight level; speed; route; heading; flight not accepted] Information from preceding sector = [flight level; speed; route; heading; request from pilot]
Output	Clearance plan
Control	Minimum separation criteria Letter of agreement Working conditions Technical training
Time	
Preconditions	Flight position = [entering the sector] Working conditions
Resources	ATCO planner available

Annex_II_Table 12: Coordination function description

Coordination	
Input	Request from next sector = [flight level; speed; route; heading; flight not accepted] Information from preceding sector = [flight level; speed; route; heading; request from pilot] System messages
Output	Updated information from coordination: 1. Request from next sector = [flight level; speed; route; heading; flight not accepted] 2. Information from preceding sector = [flight level; speed; route; heading; request from pilot]
Control	Coordination procedures Team collaboration
Time	
Preconditions	
Resources	ATCO planner available Team collaboration

Annex_II_Table 13: Update FDPS function description

Update FDPS	
Input	Clearance plan
Output	FDPS updated
Control	System messages
Time	
Preconditions	Interface design
Resources	Touch input device

Annex_II_Table 14: Pilot-ATCO communication function description

Pilot-ATCO communication	
Input	
Output	Request from pilot=[regulate speed; heading change; climb; descend]
Control	Working conditions Communication procedures
Time	
Preconditions	
Resources	

Annex_II_Table 15: Sector-Sector communication function description

Sector-Sector communication	
Input	
Output	Request from next sector = [flight level; speed; route; heading; flight not accepted] Information from preceding sector = [flight level; speed; route; heading; request from pilot]
Control	Communication procedures Working conditions
Time	
Preconditions	Team collaboration
Resources	

Annex_II_Table 16: Issue clearance to pilot function description

Issue clearance to pilot	
Input	Clearance plan
Output	Clearance issued = [regulate speed; heading change; climb; descend; adjust vertical rate; intermediate level off; holding instruction]
Control	Clearance procedures Letter of agreement RT standards Warning by safety net Team collaboration Working conditions
Time	
Preconditions	Aircraft identified Radio contact established Sector capacity = [sector capacity satisfied] Flight position = [entering the sector] Request from pilot = [regulate speed; heading change; climb; descend] Request from next sector = [flight level; speed; route; heading; flight not accepted]
Resources	Situation data display equipment Touch input device Flight progress strip RT equipment

Annex_II_Table 17: Manage resources function description

Manage resources	
Input	
Output	Strip Pencil ATCO planner available Situation data display equipment Additional data display RT equipment
Control	
Time	
Preconditions	
Resources	

Annex_II_Table 18: Manage competence function description

Manage competences	
Input	
Output	Technical training Safety aspects
Control	
Time	
Preconditions	
Resources	

Annex_II_Table 19: Manage procedures function description

Manage procedures	
Input	
Output	Procedure Alert-inhibited airspace volumes List of SSR codes Coordination procedures Clearance procedures Monitoring procedures Minimum separation criteria RT standards Communication procedures Enables MSAW alert procedures
Control	
Time	
Preconditions	
Resources	

Annex_II_Table 20: Manage teamwork function description

Manage teamwork	
Input	
Output	Team collaboration
Control	
Time	
Preconditions	
Resources	

Un approche de l'Ingénierie de la Résilience pour l'évaluation de la variabilité de la performance: développement et application de la Functional Resonance Analysis Method pour l'évaluation de la sécurité dans la Gestion du trafic Aérien

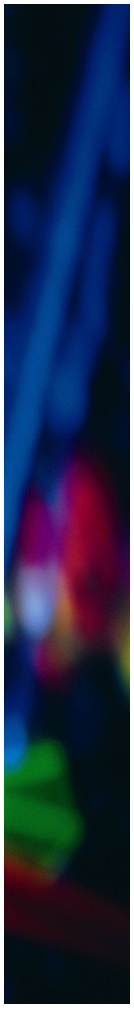
RÉSUMÉ: Cette thèse montre la nécessité de développer des méthodes systémiques d'estimation de la sécurité permettant de tenir compte de l'effet de la variabilité de la performance sur la sécurité de la gestion du trafic aérien. Comme la plupart des systèmes socio-techniques modernes, la gestion du trafic aérien est tellement complexe que il lui est impossible d'être complètement décrite. Comme conséquence directe, sa performance ne peut être complètement explicitée, car elle doit varier afin de correspondre aux conditions réelles. La variabilité de la performance est un inévitable atout pour assurer le fonctionnement d'une organisation. Mais en même temps elle peut représenter une atteinte à la sécurité du système lorsqu'elle se déroule de manière indésirable ou inattendue. Cet argument indique la nécessité de méthodes d'estimation de la sécurité qui puissent traiter la variabilité de la performance. La Functional Resonance Analysis Method (FRAM) a la capacité de modéliser la variabilité de la performance. Cependant, certains points de la FRAM pourraient être améliorés dans le but de développer ses capacités a évaluer la variabilité de la performance. Cette thèse aborde ce point faible et développe une méthodologie pour l'évaluation de la variabilité de la performance. Cette méthodologie a été appliquée dans une étude de cas dans le domaine de la Gestion du Trafic Aérien Allemand. Ses résultats ont été comparés aux résultats officiels obtenus en utilisant l'estimation de la sécurité traditionnelle. La comparaison montre la valeur ajoutée de la méthodologie proposée. En particulier elle illustre la possibilité d'identifier des risques émergents et la contribution humaine a la sécurité d'un système.

Mots clés: Ingénierie de la Résilience, FRAM, Variabilité de la performance, Estimation de la sécurité, Gestion du trafic aérien

A Resilience Engineering approach for the evaluation of performance variability: development and application of the Functional Resonance Analysis Method for Air Traffic Management safety assessment

ABSTRACT: This thesis demonstrates the need to develop systemic safety assessment methods to account for the effect of performance variability on Air Traffic Management safety. Like most modern socio-technical systems, Air Traffic Management is so complex that it is impossible for it to be completely described. As consequence, performance cannot be completely specified because it must vary to meet performance demands. Performance variability is an inevitable asset to ensure the functioning of an organisation and at the same time can be harmful for system safety when it combines in an unexpected manner. This argument clearly indicates the need for safety assessment methods that can deal with performance variability. The Functional Resonance Analysis Method (FRAM) has the ability to model performance variability. However parts of the FRAM can be improved to expand its capabilities to evaluate performance variability. This thesis addresses this weakness and develops a methodology for the evaluation of performance variability. The methodology has been applied on a safety assessment case study for the German Air Traffic Management domain. The results have been compared with the official results of a traditional safety assessment. The comparison shows the added valued of the proposed methodology. In particular it illustrates the possibility to identify emergent risks and human contribution to system safety.

Keywords: Resilience Engineering, FRAM, Performance variability, Safety assessment, Air Traffic Management



MINES ParisTech

ParisTech
INSTITUT DES SCIENCES ET TECHNOLOGIES
PARIS INSTITUTE OF TECHNOLOGY