A sociotechnical framework for the integration of human and organizational factors in project management and risk analysis

by

Fabrice Delmotte

Thesis submitted to the Faculty of the
Virginia Polytechnic Institute and State University
in partial fulfillment of the requirements for the degree of

Master of Science

in

Industrial and Systems Engineering
Dr. Brian M. Kleiner, Chairman
Dr. Tonya L. Smith-Jackson
Dr. Bruno Castanier

September 3, 2003

Blacksburg, Virginia
Key Words:
Project Management, Risk Analysis, Macroergonomics, Human Factors

A sociotechnical framework for the integration of human and organizational factors in project management and risk analysis

Fabrice Delmotte

Abstract

By definition, a system is comprised of hardware, software and "liveware". It also interacts with other systems composed themselves of those elements. However, the "human" element tends to be neglected in many projects, leading to unsafe or inefficient systems. Although some studies have shown that sociotechnical approaches to project management can generate economic gains of 20%, not to mention social gains, in practice, few projects integrate human factors correctly.

Many reasons can explain this lack of integration. Humans alone are much more difficult to model and understand than technology. When considering groups or organizations, the problem increases exponentially. Hence, traditional engineering and risk management methods cannot be used to address the human side of a system. There exist approaches and methods to use our current understanding of human behavior, however these tend to be understood and used only by a small number of specialists. Most project managers, designers and engineers have insufficient knowledge of their existence or do not understand how to make good use of them.

There are two major challenges in the integration of human factors. The first one is to justify an interest in such an approach. Given the educational background and experience of many engineers, this is no easy task. The SNCF (French Railways) has chosen to face this challenge and achieved quite good results. However, this does not solve the problem, as project managers and engineers then request tools and methods. Fulfilling this need represents the second challenge. This is

the subject of this study: to make a shift from technology-centered approaches to design and risk management to a more sociotechnical approach thanks to a macroergonomics project framework.

Human factors engineering and ergonomics is a multi-disciplinary domain. It goes from human resources management to physical ergonomics and integrates such subjects as psychology, sociology and human reliability. To improve the reliability or efficiency of systems, one approach is to develop a single tool addressing one aspect of human factors or integrating it with one kind of activities. However, many of those tools already exist, even if they have remained at the state of research results yet or been applied only in some very specific sectors.

Hence, for this research, it was decided to develop a method that covers the whole process of a project and contains the different considerations related to human factors as well as the activities required to ensure the safety of the system.

Recent research led by the US Army and adapted by the UK and Canadian Armies as well as Eurocontrol[1] have lead to the emergence of a new discipline called Human Factors Integration (HFI). This discipline proposes a project management process that covers different domains of human factors: manpower, personnel, training, ergonomics, safety, health and hazards, survivability. HFI is a good starting point but it responds only partly to our expressed need. Indeed, the SNCF requires a more general approach, easily accessible, with a greater emphasis on organization and risk management.

During this study, the HFI method was extended based on recent research results, especially in human and organizational reliability. The main improvements made are the addition of the "organization" domain and the development of safety-related activities. Many other principles were

[1] European Organisation for the Safety of air Navigation

also integrated including barriers, prescribed vs. real tasks, redundancy, recovery, degraded situation, system dynamics and measurement. Some interests of this method are its inheritance from systems engineering, its capacity to be utilized by users from different cultures and experience, and its independence from specific models of human behavior or task processing. The main output of the study is a documentation of this method defining the activities and tasks for each phase of the project as well as the composition of the team.

The method was evaluated based on its application on the "Sécurité des Travaux Organisation Réalisation Préparation" (STORP) project. This project aims at redesigning the infrastructure maintenance system of the SNCF, modifying the concepts, principles, guidelines and documentations, in order to improve its efficiency and safety. This application enabled to test the coherence and usability of the method, as well as highlight its main advantages, while underlining and improving the human factors integration in STORP. Through this evaluation, this study constitutes one of the first attempts to apply HFI to a non-military domain and to non-specific projects.

Acknowledgements

I would like to thank everyone at VT, EMN and SNCF who has encouraged me during this research.

First I would like to thank my committee members Dr. Brian Kleiner, Dr. Tonya Smith-Jackson and Dr. Bruno Castanier for their support during this project. I express special thanks to my committee chair Brian Kleiner and to Bruno Castanier. Brian Kleiner, your help through the thesis process is greatly appreciated, as well as your comments, which helped to improve the quality of this work. Bruno Castanier, you invested a great deal of time in helping me to overcome the pitfalls of a research project and encouraged me with constant enthusiasm. I would also like to thank Philippe Castagliola for guiding me through the dual degree program.

My grateful thanks go to Pierre Vignes and Yves Mortureux from the SNCF who have proposed me this very interesting topic and helped me to discover the richness of human factors and safety analysis. Thank you for your directions of research, pertinent advices and for the support I could benefit from during this study.

I also wish to thank Jacques Dubrulle to have introduced me to his project, accompanied during the application of my method with enthusiasm and provided with detailed feedback.

I would also like to thank all the other SNCF employees who have helped me to discover their company and provided me with interesting ideas and comments. Of course I also wish to acknowledge the SNCF for funding this research.

Last but not least, thanks to all of my friends who supported me during this dual degree program, whatever the distance between us.

Finally, thanks to all of you at VT, EMN, SNCF and outside whom I forgot to mention.

Table of contents

Abstract ii

Acknowledgements v

Table of contents vi

List of Figures xi

List of Tables xi

Chapter 1 - Introduction 1

1.1 Background 1

1.1.1 Preliminary definitions 1

1.1.2 Integration of human factors in projects 5

1.1.3 Human Factors and risk assessment 9

1.1.4 From traditional project management to Systems Engineering 12

1.2 Problem statement 12

1.3 Research objectives 14

1.4 Research questions and research hypotheses 15

Chapter 2 - Literature Review 17

2.1 Macroergonomics 17

2.1.1 Theory 17

2.1.2 Analysis and design of work system process 17

2.2 Integration of Human Factors in design / projects 18

2.2.1 Observations 18

2.2.2 Methods 19

2.3 Human factors in Risk Management 23

2.3.1 Concepts 24

2.3.2 Organization in risk management 24
2.3.3 Influence Modeling and Assessment System (IMAS) 25
2.3.4 System Actions Management SAM 25
2.3.5 Accident Map (AcciMap) 26
2.3.6 Defence-in-depth 27
2.3.7 Second generation HRA techniques 29
Chapter 3 - Methodology 31
3.1 Overview of the methodology 31
3.1.1 Introduction 31
3.1.2 Planning 33
3.2 Design of the framework 33
3.2.1 Introduction 34
3.2.2 Objectives 34
3.2.3 Global framework 35
3.2.4 Processes and tasks 36
3.2.5 Models 37
3.3 Evaluation of the framework 37
3.3.1 Case 38
3.3.2 Methodology of evaluation 40
Chapter 4 - Proposed framework 44
4.1 Analysis of the needs and resources 44
4.1.1 User ideas and requirements 44
4.1.2 Derived requirements 46
4.1.3 Choice of resources 46
4.2 Structure 47

4.2.1 Development of the structure 47
4.2.2 Proposed structure 49
4.3 Integration of the organization domain 51
4.3.1 Introduction 51
4.3.2 Evolution of the structure 51
4.3.3 Study of the context 52
4.3.4 Requirements analysis 52
4.3.5 Synthesis about the organization 54
4.4 Main modifications 54
4.4.1 Further changes to the function allocation activity 55
4.4.2 Other modifications 56
4.5 Development of risk management activities 57
4.5.1 Introduction 57
4.5.2 Risk management activities 58
4.6 Principles integration 62
4.6.1 Prescribed versus actual behavior 62
4.6.2 Degraded modes 64
4.6.3 Defence-in-depth 65
4.6.4 Redundancy 66
4.6.5 Recovery 68
4.6.6 Dynamics 68
4.7 Development and improvement 69
Chapter 5 - Results 71
5.1 Overview of the evaluation 71
5.1.1 Introduction 71

5.1.2 Scope of the application 73
5.2 Results of the application 74
5.2.1 Conceptual design 74
5.2.2 Design 132
5.2.3 Detailed design 136
5.2.4 Implementation and operations 137
5.3 Formative Evaluation 138
5.3.1 General observations 138
5.3.2 Improvements 140
5.4 Comparative evaluation 141
5.4.1 Important points identified 141
5.4.2 Main results of the application for the project 145
5.4.3 Feedback from the company 146
5.5 Conclusion 148
Chapter 6 - Discussion 149
6.1 Discussion of the questions and hypotheses 149
6.1.1 Question 1 – Integration of human and organizational aspects 149
6.1.2 Question 2 – Efficiency of the method 150
6.1.3 Question 3 – Acceptance of the method 152
6.2 Contributions of the research 154
6.2.1 Introduction: The context of applied research 154
6.2.2 Outputs and outcomes for industrial users 154
6.2.3 Outputs and outcomes for the research 155
6.3 Observations 156
6.3.1 Interest of using existing approaches 156

6.3.2 Beyond HFI: Systems Engineering 157
6.3.3 Cooperation between engineers and HF specialists 158
6.4 Prospects 159
6.4.1 Prospects for the company 159
6.4.2 Prospects for the research 161
6.5 Limitations 163
Chapter 7 - Conclusion 164
7.1 Recommendations 164
7.2 Synthesis 165
Bibliography 167
Annex 173

List of Figures

Figure 1-1 Risk Management Process 5

Figure 2-1 Overview of HIFA 20

Figure 2-2 Illustration of the structure of an "AcciMap" 27

Figure 2-3 Illustration of Defence-in-depth 28

Figure 2-4 The Swiss cheese model of organisational accidents 29

Figure 3-1 Global Structure 32

Figure 4-1 Main Structure 49

Figure 4-2 Team management activities 50

Figure 4-3 Organization of Risk Management activities 57

Figure 4-4 Process for prescribed/real functions, tasks and allocations 63

List of Tables

Table 1-1 Project Management Framework 4

Chapter 1 - Introduction

Design processes are often technology-centered and fail to integrate human factors adequately. This problem is encountered along the whole life cycle of a project, and is especially noticeable in risk analyses (Kirchsteiger, 2002).

Integrating human factors is a first step towards better-designed systems. However, organizational and environmental aspects can have a major impact on the personnel and technological subsystems and especially on the performance and safety of the system.

The focus of this research was the development and evaluation of a top-down sociotechnical framework for project management, which integrates risk assessment. The rationale behind such a framework is to design a system and study its risks not in a technology-centered or human-centered approach, but with a sociotechnical approach, in order to take into account personnel, technological, job design and environmental aspects at the design stage and during risk assessment.

1.1 Background

The aim of this research was to integrate human and organizational aspects in project management and risk assessment. First the terms are defined. The second section introduces the rationale and problems encountered in the integration of human factors in project management, as well as some actual solutions. Then, existing methods and current research attempts to integrate human factors in risk assessment are presented.

1.1.1 Preliminary definitions

This research dealt with three major disciplines: project management, risk analysis and

human factors. The aim of this section is to present those disciplines.

Human factors engineering and ergonomics

The expression "human factors" is used in respect to the following definition: "Human factors represent every element related to humans as well as their interactions with one another and with the system in which they are integrated" (Vignes, 2002, p1). As presented by Vignes (2002), the word "element" is purposely vague, in order to make the definition as broad as possible.

Human factors or ergonomics, as a discipline, is concerned with "designing sociotechnical systems to optimize people's interaction with systems, tools, products, and environments" (Hendrick and Kleiner, 2001, p1). These interactions, or interfaces, can be different in nature: to machines, to the work environment, to the software, to jobs and to the organization.

Optimizing can have different meanings: improving the reliability of the system, improving the safety for operators, making people more effective or happier at work are some example applications of human factors.

The initial focus of ergonomics was to optimize the interaction between operators and their work environment. Micro-ergonomics, as this initial discipline is now often referred to, started with human-machine interface design, that is the application of knowledge about human characteristics to the design of tools, controls, displays and human-environment interface design, focused on the arrangements and physical environment. The rapid expansion of computers led to the emergence of a new discipline focused on software design: cognitive ergonomics. Human characteristics were studied more in detail through human thinking processes. The last subdiscipline of microergonomics is human-job interface design. Those subparts of human factors focus on the individual and subsystem level. The latest subdiscipline, macroergonomics, has emerged from the need of adopting a more global approach, considering the overall work system, thanks to the integration of organizational design and management (ODAM) factors.

Project management

Project management, as defined in the RG0022 guideline, is a unique process that consists of a set of coordinated and managed activities with starting and end dates (Direction des Ressources Humaines, 2000). This process is used in order to reach an objective in conformance with the need of the customer, and constrained by time, costs and resources.

The main phases of a project are shown in Table 1-1.

<table>
<tr><th>Phases</th><th>Main actions</th></tr>
<tr><td>Conceptual design</td><td>• Study of the context (market, feasibility, environment, profitability)
• Formalization of the need
• Risk Identification
• Financial prospecting</td></tr>
<tr><td colspan="2">Output documents:
• Decisional documents of project launch
• Contractual documents (functional design review, performance, letter of mission, program…)</td></tr>
<tr><td colspan="2">Input document: Director plan</td></tr>
<tr><td>Design</td><td>Preliminary design
Detailed design</td></tr>
<tr><td colspan="2">Output documents:
• Study reports (PRA, PDA), general specifications, detailed specifications
• Definition report, definition of new modes in case of an adaptive or repetitive design
• Decision</td></tr>
<tr><td>Production / Implementation</td><td>• Building of the system (purchases, actions, …)
• Preparation of conditions for service</td></tr>
<tr><td colspan="2">Output documents:</td></tr>
</table>

• Technical conformance documents (authorization of exploitation, of circulation, report of verifications and preliminary tests)	
Pre-operational	• Financial operations • Verification of objectives • Project review (return on experience …)
Output documents: • Service report • Objectives report • Project report	
Operations	• Use • Maintenance • Return on experience
Disposal	• Phase-out • Disposal

Table 1-1 Project Management Framework (adapted from Direction des Ressources Humaines, 2000)

Risk assessment

Risk assessment is concerned with the study of a system to identify possible causes of harmful events. These risks can be of various natures: risk of accident, financial risk, and sociological risk, for example. Risk assessment is one aspect of project management, like human reliability can be considered one sub-discipline of human factors.

This research used the previous definition with emphasis on system safety. System safety is "a comprehensive and systematic examination of an engineering design or mature operation and control of any particular hazards that could injure people or damage equipment" (Bahr, 1997, p2).

The basic process for risk management and more specifically risk assessment is shown in Figure 1-1. This figure presents the main steps of risk assessment: identifying possible hazards, then quantifying them and evaluating their consequences in order to perform an evaluation of the risk.

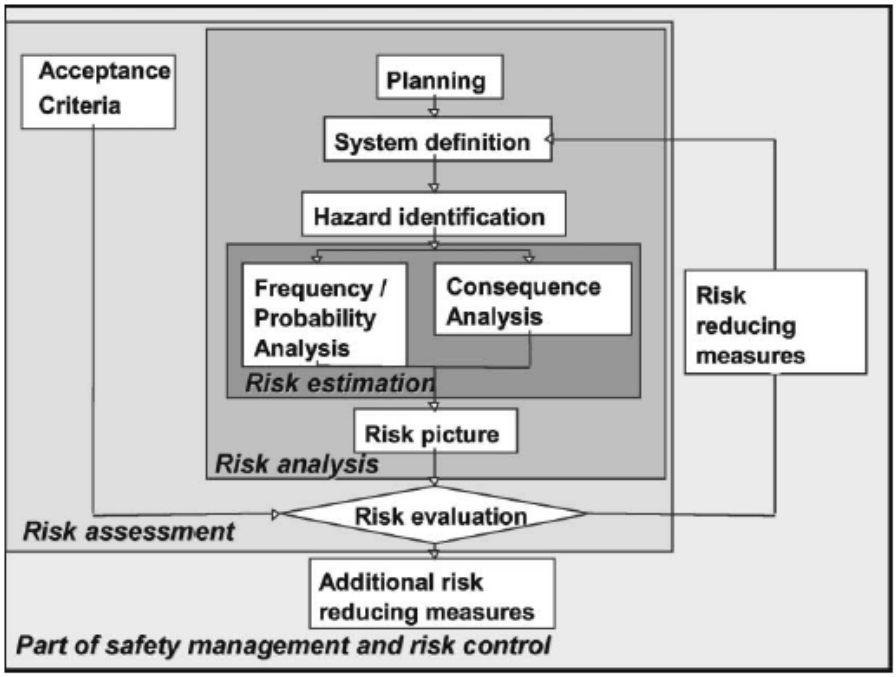


Figure 1-1 Risk Management Process

1.1.2 Integration of human factors in projects

As defined previously, the term 'human factors' is used to represent the human part of a system, including the organization. In this section, the integration of human factors in project management is introduced. First, the benefits of such integration are discussed. Then, the impacts of current evolutions in project management are evoked, as well as the problems faced by the integration. Finally, different approaches are reviewed.

Benefits of integration

By definition, a system is composed of hardware, software and liveware. This definition can be extended with Sociotechnical Systems theory to include external environments. From this definition, it seems obvious that system design should integrate human factors.

The expected – and measured – benefits, among others, are reduced costs, improved productivity and improved safety (Hendrick, 1996).

Evolutions in Project Management

Traditional project frameworks are technology-centered. They focus on finding technical solutions to a given problem. This is especially the case with the sequential approach, in which the project is linearly planned in time. In such approaches, ergonomics are usually taken into consideration after the system was designed, and this is still a problem, even in major engineering companies (Skepper et al., 2000). In this case, the role of the ergonomist is to analyze an existing system and raise design issues (Lagrange and Fanchini, 1996). Ergonomics is also sometimes integrated in the design phase of the product. Without a good insight of the system's future operations, this often requires following some guidelines. Concerning safety assessment, operators are often considered as sources of unreliability. As such, they are viewed in reliability analyses as components with a given probability of failure for a given task.

Integrated Logistics Support (ILS) has helped to increase project's scope to include needed areas. Its aim is to integrate during design the necessary elements to ensure dependability (X50-420). A part of ILS concerns human factors, like the personnel and training need analysis, or the study of maintainer task design.

Concurrent Engineering (CE) extends the concept of ILS further, by taking into account during design phases the requirements for the whole life-cycle of the system, including its disposal (X50-415). This implies making various entities implicated in the project work together (AFAV, 1997). Early involvement of ergonomists is one approach that provides for better integration of human factors.

Thanks to the progresses made in the disciplines of ergonomics and human reliability, a new approach was researched, called “anthropo-centered design”. Examples of the developed models are

the ones of Engeström or Normann (Didelot, 2001). One major default of this approach is the lack of integration of technological elements.

Much work was done on integrating ergonomics into project management, however these approaches often fail practically due to a difference of culture and methods between engineers and ergonomists. This collaboration is a requirement for successful CE, and accounts for the failure of many ergonomic interventions.

Integration problems

Integrating ergonomics in projects requires overcoming many obstacles. Ergonomics tends to be considered by some as a "soft" science, which needs to prove it has some worth compared to "hard" engineering methods, that were used successfully for years (Kirwan, 2000). Helander (1999) points out some other obstacles. Many people still understand ergonomics as the "design of chairs" or knobs and dials science. Research in ergonomics often is perceived as too abstract to be used by engineers or project managers. Furthermore, since humans are adaptive, people tend to think that operators will adapt to the designed system.

Another problem is related to the culture of ergonomists and engineers. In Europe, Human Factors subjects are just beginning to be integrated in engineering studies (Lapeyrière and Massip, 1994). Amalberti (1998) underscores the very low level of engineers in human and social sciences in France. On the other hand, ergonomists often lack the knowledge and understanding of engineering methods and project management constraints (Jourdan and Bellies, 1996). Project managers also need a fair knowledge of the ergonomic intervention, so that ergonomists can be awarded appropriate time and resources (Colin and Vaxevanoglou, 1994).

Recent developments

Integrating human factors in projects is a worthwhile endeavor. Many of the problems

encountered can be solved methodologically. Such a methodology can define the modalities of cooperation between human factors specialists and other members of a project team, thanks to a good analysis of their work habits.

A successful case is related to the use of the ERCO framework for the design of new generation high-speed trains (Sagot et al., 1994 and 2000). Pomian et al. (1997) provide a good overview of engineering and ergonomic practices and analyze the methods to link them together.

However, such methods focus on ergonomic design alone. The aspects of manpower, personnel, training introduced by ILS are also important for a project. A global approach is being studied in the U.S. Army, called Human System Integration (MANPRINT program) and Canada, or Human Factors Integration in Europe (UK DEF STAN 00-25). This approach covers the following domains: Personnel capabilities, Manpower, Training, Human Factors Engineering, System Safety, Health Hazards, Soldier Survivability. An application to the civil context is performed through the Human Factors Integration for Future Air Traffic Management (HIFA) project (European Organization for the Safety of Air Navigation, 2000).

Many of these methods are interesting, and are reviewed more in detail in Chapter Two. However, they lack integration of organizational aspects.

Project management and sociotechnical systems

Complex projects often design an organization, which must integrate with a broader existing work system. In most cases, there will be chiefs, managers, top-managers and recruiters associated with the work of the operator. Hence, many projects can be considered work system designs. Furthermore, the environmental subsystem as defined in the STS theory will be tightly correlated with the system. This is why a more general approach is required.

Lewkowitch-Orlandi and Carballeda (1996) relate the case study of an organizational change. Ergonomists collaborated quite successfully in this project. The authors underline the fact that the

French approach adopted works bottom-up – ergonomists are assigned tasks and bring information to managers, whereas the American approach of macroergonomics is top down, bottom-up and middle-out, which is one potential reason for its efficiency. By using information on all levels of the organization to design it as a whole, macroergonomics help design a balanced and efficient work system.

Macroergonomics is a "top-down sociotechnical systems approach to the design of work systems and the application of the overall work system design to the design of the human-job, human-machine, and human-software interfaces" (Hendrick and Kleiner, 2001). This approach focuses on the human-organization interface, and defines a methodology to design work systems. Hence, it goes beyond traditional microergonomics approaches, and ensures a higher level of integration.

1.1.3 Human Factors and risk assessment

Risk assessment is one aspect of project management and has its own specific methods. This section presents some traditional approaches to the integration of human factors, as well as research orientations, before discussing of the integration between human factors, project management and risk assessment.

Traditional approaches

The integration of human factors in risk assessment started from the consideration that humans are unreliable. This led to the creation of techno-centered approaches. The aim of these approaches is to quantify human reliability for probabilistic safety assessment, as it is performed for hardware. Methods were created, like the well known Technique for Human Error Rate Prediction (THERP) (Swain and Guttman, 1980). These Human Reliability Assessment (HRA) methods were extended by

including more and more performance shaping factors, going from stress or fatigue in the first studies to collaborative aspects later. However, one major limitation of this approach is that it is based upon simplified models.

Then came the anthropocentered approach. Based on more complex models, the most famous being the ones of Reason (1990) and Rasmussen, they first enabled the creation of qualitative methods. These methods help design safer systems and understanding accident scenarios. Second generation HRA methods are also being developed (Hollnagel, 1996).

Fadier and Mazeau (1998) classify the methods related to human reliability in four categories:

- Methods of evaluation of human reliability: These methods describe and quantify human performance in a given task to evaluate and predict human reliability
- Methods of qualitative analysis of human components of reliability: These methods describe human variability when executing tasks, or in order to understand the psychological process leading to the error
- Methods for the management of human reliability: These methods integrate the description, quantification and psychological analysis of errors. They integrate in a global framework aimed at preventing error causes and designing more adapted systems
- Methods based on return of experience and databases: Using a posteriori evaluation of human reliability, these methods help to predict human reliability in similar cases.

New developments

The first HRA techniques enabled a good integration with traditional risk assessment methods used in projects, as they consider humans as a component. But recent methods are much more complex to integrate with traditional risk approaches, especially considering the elements to take into account. Better frameworks were then developed. The Méthode d'Analyse de Fiabilité et

d'ERGonomie Opérationnelle (MAFERGO) (Neboit et al., 1993) is a retrospective analysis method that covers both technical and human reliability by making use of functional and operational analysis. However, these methods are often to be applied on existing systems.

In terms of conception, the whole sociotechnical system was studied last with the apparition of macroergonomics. The case is similar in risk assessment, where the research is now oriented towards the safety of organizations. Rasmussen (1997) insists on the need of a "top-down, system oriented approach" in order to assess the risks linked with sociotechnical systems. Modeling of sociotechnical systems for risk assessment was a subject of recent researches (Svedung and Rasmussen, 2002), and integrating such models in PRA is also a source of concern (Paté-Cornell, 1997).

Integration with risk assessment in projects

Risk assessment activities are usually performed at different phases of a project life cycle. The best cooperation in technology-centered design comes from the linkage between functional analysis, value analysis and failure modes, effects and criticity analysis (FMECA). Indeed, the method used from the beginning of the design - external functional analysis - is also used for detailed design later – internal functional analysis -, for cost analysis – value analysis -, and for the risk assessment – FMECA. However, technology-centered design processes reduce the possibility of integrating human and organizational aspects efficiently.

Human reliability studies often need to be integrated in existing technology-centered methods in order to be used during projects. However, this limits their integration with the project, and the philosophy of human-centered design.

Some interesting work was done in order to use the MAFERGO method prospectively (Didelot, 2001). However such methods still lack the integration of organizational aspects.

1.1.4 From traditional project management to Systems Engineering

A good integration of human factors, especially of the aspects related to risk management, requires a more global approach. Such an approach is proposed by Systems Engineering (SE). SE can be defined as "a structured and integral approach for the engineering of systems, using customer requirements as a starting point, with proper and timely integration of necessary disciplines, ensuring open minded and careful design choices, working in a visible and controlled way and with customer requirements as a final touchstone" (Hamann, 1999, 2-6).

SE is a cross-disciplinary approach based on a top-down framework for the design of complex systems. It relies on models of the architecture of the system, both in terms of functions and physical architecture. In theory, SE covers the aspects of human factors and risk management and is related to practices like designing for usability, designing for reliability and designing for safety.

1.2 Problem statement

Existing project frameworks are technology-centered both in terms of design and risk assessment. As seen previously, some interesting methods enable the integration of human factors with those frameworks, however they create many limitations.

This research was sponsored by the Société Nationale des Chemins de fer Français (SNCF) – French Railways Company. Their desire was to integrate human and organizational factors more efficiently and effectively in project management and especially risk assessment. The SNCF, as part of European railroads, can be classified as an ultra-safe system (Amalberti, 2001). According to this definition, it is a rigid and over-regulated system in which accidents are linked to a complex combination of factors; and safety strategies are long-term ones. As Amalberti emphasizes, the effectiveness of such ultra-safe systems "tends therefore to become a political rather than a scientific subject". Optimization of such systems requires a different and more systemic approach.

Macroergonomics helped to successfully design work systems in many cases (Hendrick and Kleiner, 2001). It is possible to consider that a project aims to create a sociotechnical system and must be well integrated with a larger system, which it will impact and be impacted from. A macroergonomics project framework would enable an efficient sociotechnical approach to both design and risk assessment. Indeed, adopting a top-down, bottom-up and middle-out approach for project management enables many aspects to be taken into account, pushing far beyond traditional techno- or anthropo-centered approaches. Then, the modeling required to assess sociotechnical risks also necessitates a top-down approach (Rasmussen, 1997).

One question may arise: Why not concentrate on risk assessment only, or on project management? One pitfall that many specialists in human factors or risk assessment often face is that their action is considered as an 'add-on' to the project. Another reason lies in the models. Both design and risk assessment are based upon models of the system. In the technology-centered approach, the success of FMECA for risk assessment is due to its integration with functional analysis in design. This is why we also need a common model to develop a sociotechnical framework.

This research has one particularity, which lies in its cross-disciplinarity. Svedung and Rasmussen (2002) raised the rationale for cross-disciplinary research in the field of risk management. Traditional approaches aggregate results of research in different disciplines. An integrated systems approach requires integrated models and methods, which is the aim of this research.

One can argue that Systems Engineering (SE) is the solution to this problem. SE offers indeed the base for a holistic top-down approach. However, some of its limitations can be identified:

- SE, as it is used, tends to be technology-centered. If SE was meant to be a holistic approach, it tends to be used as a technical system design methodology. A greater emphasis on human and organizational aspects is required.
- Human Factors and risk management are two aspects of SE. However, the aim of this research is to enable the design of safe systems from an organizational and human point of

view. Hence, human and organizational reliability will be at the center of the approach. The method of performing an efficient integration needs to be addressed.

- SE is often considered a complicated approach, intended for large engineering projects. Indeed, SE is rather a prescription than a method in itself. The researched method explains how to perform the prescribed integration.
- SE leaves a great choice in terms of modeling and methods. This restricts its acceptance, understanding, and the cooperation between project members. Simple unified models and methods are required.

The framework researched was inspired from SE. Its interest is that it defines how to integrate together human factors, risk assessment and project management.

1.3 Research objectives

The aim of this research was to produce a general framework to integrate human factors with project management and risk assessment, using a sociotechnical approach. This framework needed to be usable for civil projects of very different types, unlike the most developed methods currently developed, which for are intended for the military domain or for very specific projects. The intent was to set modular bases, in terms of processes, models and methods that can be further extended to include other aspects and tools.

The main objectives were to:

- define the main processes of the framework. These include:
    - the composition of the project team, especially in terms of HF specialists and people in charge of coordinating HF actions
    - risk assessment processes
    - processes for each phase, specifying cooperation between non-HF and HF specialists

and HF-related tasks

    - necessary points to be checked in output documents of the phase
- design a model of the system, including human factors, applicable to design and risk assessment
- assign methods to ensure a tight correlation between actions at the macroergonomics and microergonomics design levels
- evaluate the applicability of the framework

1.4 Research questions and research hypotheses

The research questions and hypotheses related to the previously defined objectives were:

Question 1: How can design and risk assessment integrate human and organizational aspects?

Hypothesis 1.1: Human factors integration in design and risk assessment can be achieved by coordinating and integrating together macroergonomics, microergonomics, organizational risk models and human reliability methods.

Question 2: Can an organization- and human-centered design methodology of safe complex systems be used efficiently?

Hypothesis 2.1: A sociotechnical project framework will enable the design of safe systems.

Hypothesis 2.2: A sociotechnical project framework will enable the design of efficient systems.

Question 3: Can an organization- and human-centered design methodology of safe complex systems be accepted by an interdisciplinary project team?

Hypothesis 3.1: Engineers will agree on the advantages of a sociotechnical project framework.

Hypothesis 3.2: Project managers will agree on the advantages of a sociotechnical project

framework.

Hypothesis 3.3: Human factors specialists will agree on the advantages of a sociotechnical project framework.

Chapter 2 - Literature Review

The previous chapter introduced the subject of this research. One major aspect is the inclusion of macroergonomics. Hence, this discipline is presented first. Chapter One also overviewed current developments for the integration of human factors. Those developments are reviewed here more in detail, first about project management and then dealing with risk assessment. Some literature relevant to very specific points of the research is reviewed later in Section 3.3, as well as in the description of the framework to be researched.

2.1 Macroergonomics

2.1.1 Theory

The discipline of Macroergonomics is based on Sociotechnical Systems (STS) theory. According to this theory, a system is comprised of three subsystems: personnel, technological and job design, in interaction with the environment (Hendrick and Kleiner, 2001).

A sociotechnical system is considered to be an open system, as it is permeable to the environment, which transforms inputs into outputs. A great interaction exists between the personnel and technological subsystems, which are both affected by environmental events. This is the principle of joint causation. Another important principle is the one of joint optimization: optimizing the system implies taking into account both the personnel and technological subsystem.

2.1.2 Analysis and design of work system process

This research considers a project as the design or evolution of a work system. The framework will be inspired from the MacroErgonomics Analysis and Design (MEAD) process (Hendrick and Kleiner, 2001):

- Phase 1. Initial Scanning
- Phase 2. Production System Type and Performance Expectations
- Phase 3. Technical Work process and Unit Operations
- Phase 4. Variance Data
- Phase 5. Construct Variance Matrix
- Phase 6. Variance Control Table and Role Network
- Phase 7. Function Allocation and Joint Design
- Phase 8. Roles and Responsibilities
- Phase 9. Design/Redesign
- Phase 10. Implement, Iterate, Improve

2.2 Integration of Human Factors in design / projects

Integrating human factors in projects requires addressing several issues. Section 2.2.1 introduces some of those issues and possible general approaches. Existing methods are then reviewed in Section 2.2.2.

2.2.1 Observations

As seen previously, collaboration potentially suffers from a difference of culture and methods between human factors specialists and other project members. A change of culture and education is not a possible solution in a short-term vision, so that one solution would be to ensure an efficient internal (or external) contracting between them, as studied by Naël et al. (1994). It is necessary to start the ergonomic intervention earlier, and this implies earlier planning that needs to be well-defined in contracts in to ensure optimal efficiency. The notion of a contract has many advantages. It

enables ergonomists to refine and make homogeneous their methods and how they present it. It also gives a better view of the contribution of the ergonomists, which is a major point for their acceptance and integration in projects. Finally it ensures a good integration with existing project management methodology.

However, Nikolopoulo (1998) reacted to this approach, stating that contracts tend to divide the ergonomic intervention into modules, which is contrary to the logic of concurrent engineering. Hence, contracting might represent a first stage towards recognition of the ergonomic intervention, but to become the engine of conception, it should become an integral part of the project.

2.2.2 Methods

Human Factors Integration / Human System Integration

Human Factors Integration (HFI) is an engineering discipline that applies theory, methods and research findings from ergonomics, psychology, physiology, anatomy and other disciplines to the design of manned systems. As defined by MoD Director Naval Architecture (1999, p3.1) , "Human Factors Integration (HFI) draws on this discipline [Human Factors] to provide a design process for application to platforms and equipments".

Human Systems Integration was first implemented in 1982 in the U.S. Army, under a development program called MANPRINT (MANpower and PeRsonnel INTegration). The consideration was that integrating manpower, personnel and training issues in design processes might improve them. Since then, MANPRINT was extended to seven domains – Personnel Capabilities, Manpower, Training, Human Factors Engineering, System Safety, Health Hazards and Soldier survivability – to become a comprehensive management system (U.S. Army, 2000). MANPRINT has now been adopted for the entire U.S. Department of Defense.

The success of MANPRINT prompted other countries to launch similar research programs;

for example, the initiative of the Canada's Department of National Defense (Greenley, 2000), and of the UK MoD (NMA, 2000). One of the main disadvantages of HFI was its lack of integration with other project management practices, like Integrated Logistics Support – there is indeed an overlap of domains between both approaches , Combined Operational Effectiveness and Investment Appraisal or Risk Management. Research in UK's HFI is now focusing on this better integration (Strain and Preece, 1999).

Previous initiatives were military ones. The Human Factors Integration in Future ATM Systems (HIFA) is a civil project initiated in 1997 as part of the Air Traffic Management (ATM) Human Resources Program (European Organization for the Safety of Air Navigation, 2000a).

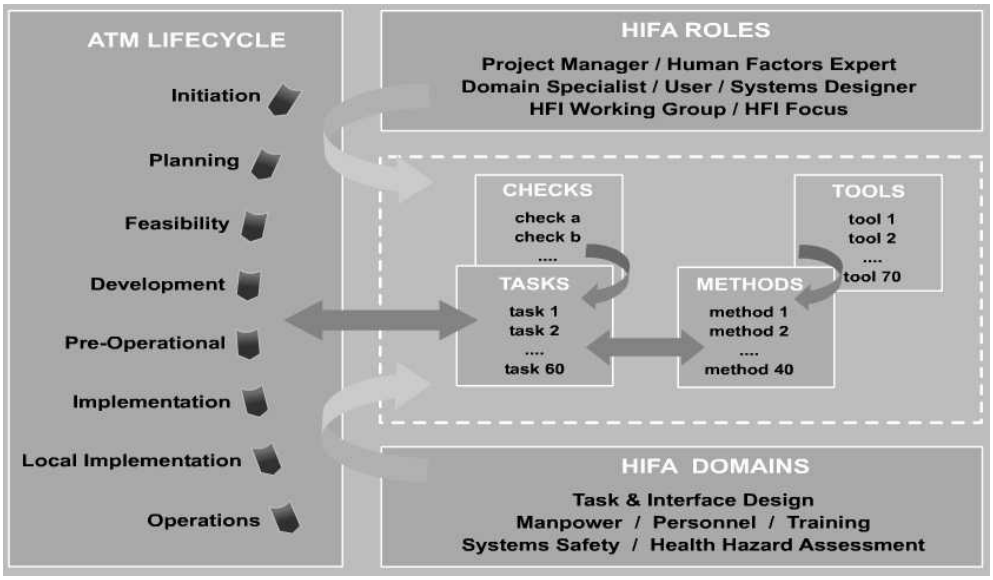


Figure 2-1 Overview of HIFA

This project adapted the US and UK programs to the development of ATM systems. As shown in Figure 2-1 HIFA offers a precise framework on how to organize the project team for HFI, describes the tasks and checklists for each phase of the project (European Organization for the Safety of Air Navigation, 2000b), as well as methods and tools that can be applied to perform those tasks

(European Organization for the Safety of Air Navigation, 2000c). One interest is that it is a civil application. The interactive computer presentation and search module is also of interest[2], as it enables any member of a project at any phase to know exactly what HFI tasks he/she has to perform and what methods or tools he/she can use, in a much easier way than the traditional paper guidelines.

The advantages of HFI are clear, and justified it as an source of inspiration for this research: reduced costs of re-engineering, reduced risks, through-life costs optimized thanks to anticipation, better safety and health of the personnel (Strain and Preece, 1999). Furthermore, it integrates both organizational (manpower) and micro-ergonomic aspects. However, many limitations are raised by Strain and Preece (1999). The integration of human users as part of the system still lacks scientific knowledge, it is difficult to produce contractual requirements for system developers about human factors, due to an absence of quantifiable parameters, and the HFI process does not take care of the organization that will be in charge or recruiting or training as defined during the project. This and the lack of integration with risk management are reasons for a macroergonomics approach including risk analysis that this research aims to produce.

The SNCF sociotechnical framework

Previous work was conducted at the SNCF on a sociotechnical framework (Direction des Ressources Humaines, 1997). The aim of this framework is to take into account human and social aspects from one end of the project to the other. Its main interest is to focus on a very broad range of human factors – including interesting points like the impact of the project on work organization in breakdown- situations. One of its limitations however is that it gives little direction on the methods that can be used for the different points, or on the modalities of cooperation. It was of inspiration for this research as the personnel of the SNCF have already been in contact with it, and it is one reason

[2] Available online at http://www.hifa.org

why they asked for a more detailed and complete framework including explicit methods and models.

MAFERGO (Méthode d'Analyse de Fiabilité et d'ERGonomie Opérationnelle)

MAFERGO is a method developed for the analysis and ergonomic intervention in complex automated systems. Its objective is to improve the reliability and safety of sociotechnical systems by minimizing the probability of a negative occurrence in the technical system or in the human-system interaction (Neboit et al., 1993). This method is comprised of five steps. The first one describes the normal operations of the system and its structure, using functional analysis and ergonomic analysis to describe prescribed tasks and real activities. In the second step, the dependability of the system is evaluated thanks to operational analysis, as the ergonomic analysis describes spatial activities, timing, occupation ratios and planning problems. During the third step, a list of malfunctions is established by using FMECA, and the recovery activities by the operators are studied. It is noticeable that this method considers the operator as a source of reliability rather than only as an unreliable component. The fourth step focuses on describing incidential scenarios as a combination of the technical, human and organizational events. Simulation can help understand better the recovery actions involved. Finally, the fifth step is to suggest improvements, including technical, ergonomic and organizational. Predictive simulations can help evaluate the impacts of those suggestions in terms of efficiency, safety, and work context.

At first, MAFERGO was intended for the evaluation of existing systems. However, Didelot (2001) studied its interest for design phases. Thanks to a study in a printing plant, the author showed that MAFERGO could help identify the Limit Activities tolerated by Usage (LAU) developed by operators to cope with the objectives and constraints. As it uses traditional design and risk analysis tools and gives a quite general overview of the situation, MAFERGO could be integrated in design phases (Didelot, 2001).

One limitation of MAFERGO is that it is designed for use on complex automated systems.

Hence, it still encourages a technology-centered design. However, its efficiency at the micro-ergonomic level made it an inspiration for the part of our framework that focuses on task design and detailed technical design.

Other developments

Garrigou et al. (1995) raised the question of activity analysis in design. Indeed, this practice is the core of the ergonomic discipline in French-speaking countries. However, one approach is to use activity analysis on future tasks, and another one, of major concern for this research, is to know if there is no contradiction between this practice as a bottom-up approach and top-down systemic design. An approach is proposed to combine top-down, bottom-up and simulation-based approaches, which is of interest for this research (Garrigou et al., 2001).

In terms of microergonomics design, some general guidelines can be useful for this research, especially concerning methods (Buck, 1999; Wagner et al., 1996). The interface between engineering and ergonomic practices proposed by Pomian et al. (1997) seems efficient, in that it analyzes in detail the methods used by the engineers and the requirements of an ergonomic intervention, and tries to coordinate them at best. The proposed approach lacks a guiding framework, however the work made on specific functional analysis methods is of interest for detailed design.

2.3 Human factors in Risk Management

As discussed in Chapter One, the current challenge is to integrate not only individual but also organizational aspects in risk assessment. First, some concepts about human reliability are introduced. Then, the concept of organizational reliability is presented. Finally, various methods of interest are reviewed.

2.3.1 Concepts

This research tried to integrate some important points of view as a guiding philosophy. The first one is that human shall be considered for their positive effect in the system, and not only as a source of unreliability (ISdF, 1996). Indeed, the operator is able to recover from technical malfunctions, but also socio-organizational ones caused by conflicts of objectives or insufficient procedures (Hutchins, 1995). However, this implies enough visibility of the error, and reversibility (Amalberti, 1996). This can be achieved by assuming errors at the conception stage (Laprie, 1985).

Then, mistakes are cognitively useful, so that they cannot and should not be totally eliminated (Amalberti, 2001). They must be understood not only as individual errors, but also in a more systemic or sociological framework. Amalberti (2001) provides a good analysis of the way to handle the different kinds of error (routine-based, knowledge-based and violations) in design. Another point is that safety procedures and rules will often be violated and should be conceived in respect to this consideration (Gerard, 2001).

2.3.2 Organization in risk management

Different approaches were developed to study the reliability of organizations. Bourrier (2001) identifies three main approaches. In the first one, organizational reliability is seen from the individual point of view who adapts to the organization (Amalberti, 1996) and who suffers from its unreliability under the form of latent failures (Reason, 1990). The second approach tends to demonstrate that this reliability cannot be achieved with the traditional resources offered by the organization (Perrow, 1984). Finally, the third approach assumes that organizational reliability is the consequence of a successful interaction with its environment, through mechanisms like confidence (La Porte, 2001).For these different conceptions correspond different methods and models of interest for this research.

2.3.3 Influence Modeling and Assessment System (IMAS)

Influence Modeling and Assessment System (Embrey, 1992) is based on an accident model showing organizational factors in accidents: the Model of Accident Causation using Hierarchical Influence Network (MACHINE) model. MACHINE is organized around three categories of events - external, technical and human - and three types of causation - from the direct cause to the indirect one linked to the decisions of the company. IMAS then enables the integration of this model in probabilistic risk assessment. However, this method incorporates the organization but still focuses on the operator.

2.3.4 System Actions Management SAM

The System Actions Management (SAM) approach is based on an influence diagram describing the interaction among three levels – basic events, decisions and actions and organizational factors – and an analytical approach (Paté-Cornell and Murphy, 1996).

The principle is as follows: a traditional diagram for the event is drawn at the lowest level. Then the decisions and actions that led to the events are added at an intermediate level. Finally the management factors that influenced those decisions and actions are represented at the upper level. The conditional probability failure is achieved from this decomposition (Paté-Cornell, 1997):

$$p(F|M_k)=\sum_i \sum_j p(F|IE_i,DA_j)\,p(IE_i|DA_j)\,p(DA_j|M_k)$$

where:

$p(F)$ probability of system failure F

$p(IE_i)$ probability of the initiating event i

$p(DA_j)$ probabilities of the decisions and actions of the different actors

M_k relevant management factors

2.3.5 Accident Map (AcciMap)

Svedung and Rasmussen (2002) have proposed a graphic representation model called AcciMap in order to describe the complexity of accident scenarios. In fact, it consists of a set of representation tools:

- the AcciMap represents a particular accident scenario
- the generic AcciMap, created by putting together several AcciMap in order to identify the decision bodies involved in a particular hazard domain
- the ActorMap identifies organizational bodies, individual actors and decision makers
- the InfoFlowMap represents the information flows

The mode of representation of an AcciMap is illustrated in Figure 2-2. This modeling technique helps to identify influences on physical process and actor activities at different levels of the system, and enables to represent complex accident scenarios through direct and indirect consequences.

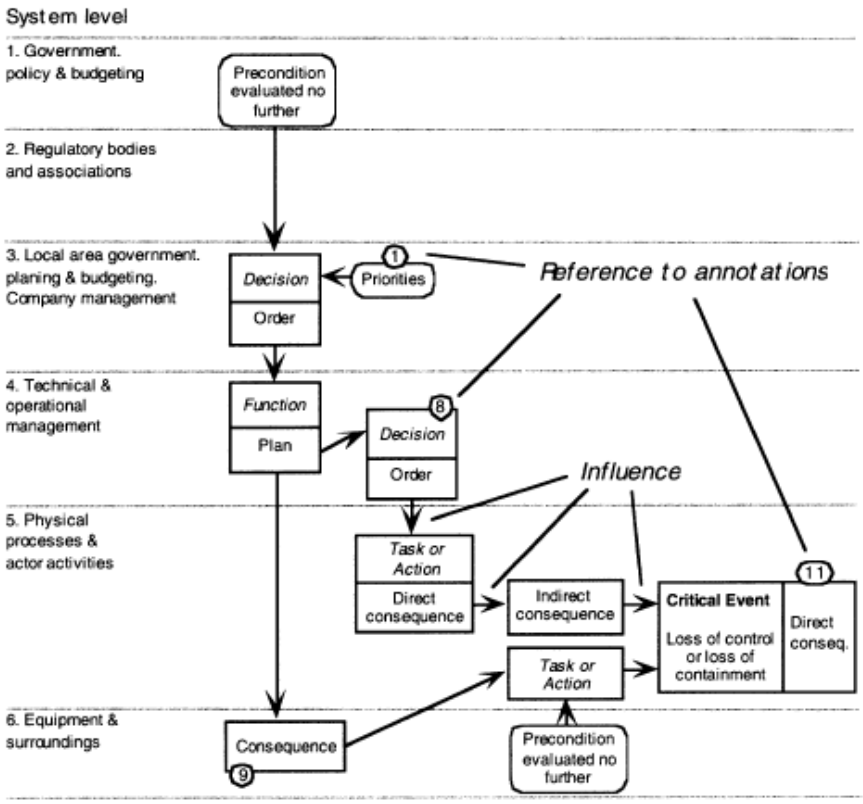


Figure 2-2 Illustration of the structure of an "AcciMap"

(from Svedung and Rasmussen, 2002)

2.3.6 Defence-in-depth

Presentation of the concept

As defined by Valancogne and Nicolet (2002), the concept of defence-in-depth relies on the installation of several levels of protection solutions, which will be called barriers, in order to reduce the aggressions on the system or their consequences. Such barriers can either be technological, procedural, human, or mixed.

In order to improve the safety of the system, the barriers not only protect the system against the aggressions, but also protect one another, in order to improve the overall defense, as depicted on Figure 2-3.

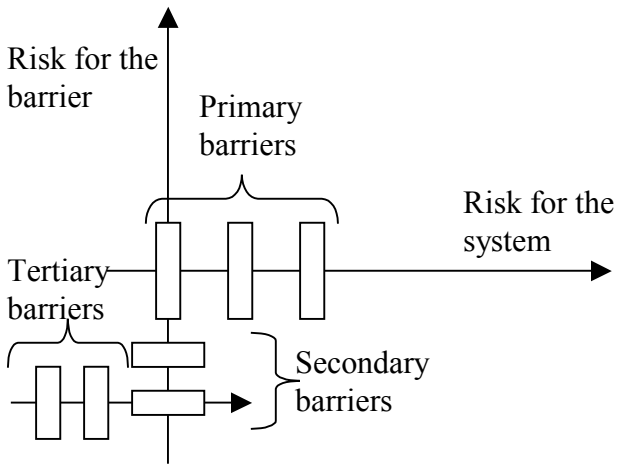


Figure 2-3 Illustration of Defence-in-depth

(from Valancogne & Nicolet, 2002)

This approach presents many interesting perspectives:

- it gives an overall picture of the risk management mechanisms protecting the system
- it is very intuitive, as it is based on simple models, and does not require specific knowledge
- it helps evaluate better the influence of modifications brought to the system on its safety
- it ensures a global coherence in the defense mechanisms, from technological to organizational ones
- it shows to every actor in the system his possible impact on safety

The fallacy of defence-in-depth

Defence-in-depth has helped make nuclear plants safe to isolated failures. However, its efficiency as a risk management approach presents some flaws. As discussed by Reason (1990), in the "real world", the various barriers are not intact at a given time, but they possess gaps and holes created by combinations of active failures and latent conditions. This can be represented with the "swiss cheese model" shown on Figure 2-4.

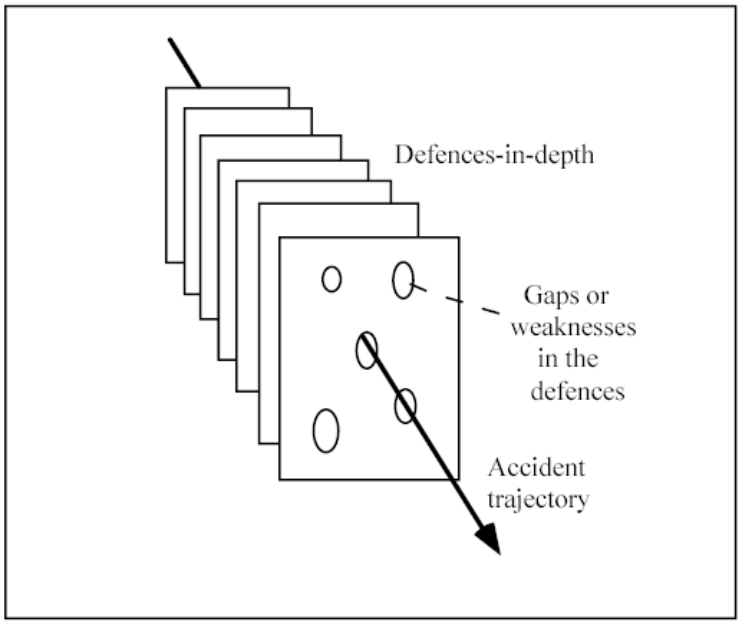


Figure 2-4 The Swiss cheese model of organisational accidents

(from Reason, 1990)

These holes constitute "windows of opportunity" which, if combined in the right manner, can lead to an accident.

These holes are the main threats for a safety management approach based on defence-in-depth. The problem is that the holes are dynamic, they can move, expand or decrease, so that it may be difficult to evaluate the level of safety of a system at a given time, and to know in detail what is right or wrong. Safety issues may then be hidden from the workers and supervisors, which may prevent them from being proactive in the case of an accident scenario.

2.3.7 Second generation HRA techniques

In order to overcome the problems linked with the simplicity of the first HRA methods, some second-generation HRA methods were developed.

Hollnagel (1996) proposes with CREAM a method to include the influence of the context in

the analysis. Unlike THERP, it considers those aspects not as performance shaping factors (PSF), but as direct consequences for human cognition. However, this method is mainly qualitative, which can be seen as one limitation when compared to first generation HRA techniques.

Another interesting method is proposed by Richei et al. (2001). HEROS – Human Error Rate Assessment and Optimizing System – is an expert system based on fuzzy variables. Hence, it does not need databases like THERP. It is based on fault trees, and includes the evaluation of management, as well as of the PSFs of the task profile. HEROS can be used both for qualitative and quantitative evaluation of human error. Its main interests lie in the incorporation of management in the model used, and the use of a fuzzy set theory, so that the uncertainties linked to the evaluation are better assessed.

Chapter 3 - Methodology

Note: Since the subject of this thesis is the development of a method, Chapter 3 is called "Methodology" and describes the process by which the method was developed and tested.

The previous chapters presented the problem and associated research questions and a literature review on the subject. In this third chapter, the methodology used to answer those research questions and reach the research objectives is described. First, an overview of the methodology is given in Section 3.1. The approach used to design the researched framework is explained in 3.2. Finally, Section 3.3 defines how this framework was evaluated.

3.1 Overview of the methodology

3.1.1 Introduction

An iterative process was used to conduct this research. The framework was developed using existing approaches and research findings and following the global structure shown in Figure 3-1, but also users' ideas and feedback as well as a formal test/evaluation.

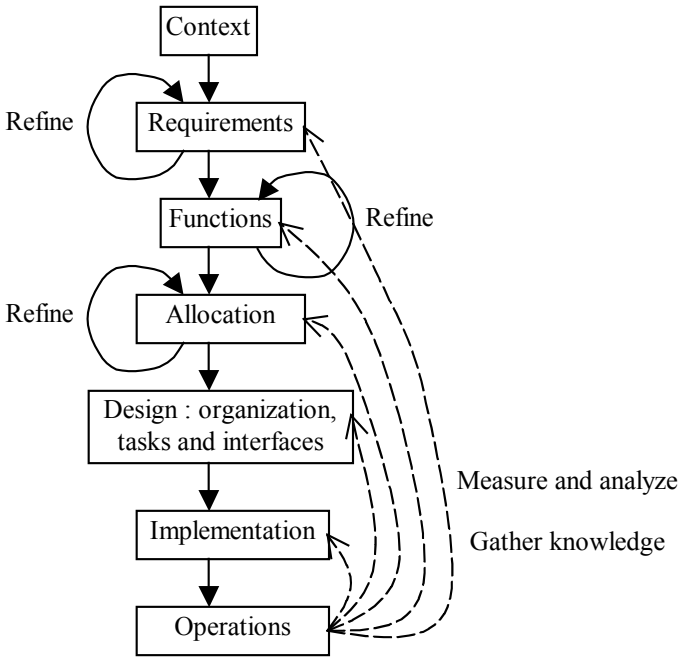


Figure 3-1 Global Structure

The method was designed and evaluated based on a "case" which consisted of a large project in the company. The idea was to apply the method to this project. First, this enabled a test of the method while it is being developed by providing a concrete case. Then, the results obtained could be compared to the actual design and the results of previous risk assessments to evaluate the researched method. A complete comparison was not possible of course, as this would imply to redesign the whole system, however thanks to this approach it was possible to see what new aspects the researched method helped in identifying.

The framework was developed using a top-down approach, going from the general process to the specific tasks. Each major phase used the comments and ideas of future users, and the output was tested on the case and thanks to the results of the tests and the feedback. Finally, the framework was evaluated based on its application on the case, by evaluating its effectiveness, the quality of the resulting designs and the user acceptance. This way of proceeding enabled the answers to the three

research questions while respecting the time and resources constraints. The case supplied both a good tool to motivate potential future users as well as the company top managers, an evaluation of the framework efficiency and the assessment of its possible acceptability.

3.1.2 Planning

Ideas and comments of some future users (how, who were they etc.) were first collected, as well as data from the literature, in order to constitute a first set of requirements for the researched method.

The development of the method then started, while various project managers were met in order to identify an appropriate case for the evaluation. Those were introduced to the objectives of the research and overall structure and principles of the method, so that they could evaluate if one of their project was suitable for an application of the method. This helped identify the project described in 3.3.

The method was then developed progressively, going from the general framework to the detailed tasks as explained in 3.2. It was regularly presented and checked by the two initiators of the research (respectively delegate director of HF in the safety division, and expert in the safety studies center), as well as to the project manager of the case.

Once the method had attained a certain level of completion, the evaluation on the case started, which helped evaluate and improve the method. It was then finalized.

3.2 Design of the framework

This section presents how the researched framework was developed. First the approach is introduced, and then each important part of the development process is presented.

3.2.1 Introduction

The framework was designed using a all three directions of the macroergonomics approach: top-down, bottom up and middle out. The top-down approach helps structure the framework and ensures the right integration of the systemic aspects. Lower stages can induce changes at the upper level, so that the bottom up dimension is very important. The middle-out approach ensures the consistency of the whole.

For each step, the objectives were first defined. Current practices and research findings were reviewed and the most adequate ones were used as a starting point.

The major steps were the following:

- Define the objectives and the methodology: This is the purpose of the first and third chapter.
- Define the global framework: In this step, the structure of the framework was researched, in terms of main phases and activities.

Then, for each major phase identified in the framework, the two following activities were performed in parallel:

- Define the processes and tasks: The previous framework was refined. Activities were described in terms of processes and tasks.
- Define the models: One or several models were researched in order to enable an efficient collaborative work. Those help understand the purpose of some tasks and provide a first simple tool to perform those tasks.

3.2.2 Objectives

In this section, we focus on specific objectives and requirements of the researched framework. These criteria come from the needs expressed by the future users of the method.

In terms of main features, this framework needed to be:

- Clear and simple: The framework and base models must be understood by all team members to ensure an efficient cooperative work.
- Detailed: Some points require specific attention, as only a thorough description of the tasks will enable their efficient use. These include among others, the definition of roles, the cooperation modes, the model creation and analysis processes and the risk assessment part. This is also true for models, which should be usable for detailed design and risk assessment.
- Adapted: One major problem with existing practices is that they are not adapted to the context. For example, human behavior evolves in a dynamic environment, contrary to traditional reliability assessment, which is often based on architectural static models. Hence, the framework was to address the needs and not try to fit some existing methods to some problems.
- Focused on safety: Existing frameworks have demonstrated their efficiency to design a system. The researched framework should focus on safety. This implies incorporating in design activities some important aspects of human reliabilities, like the concepts of barriers and redundancy. Risk assessment activities were also addressed specifically and tightly linked with design activities.

3.2.3 Global framework

The global framework can be seen as the "skeleton" for the researched method. It defines the main activities to be performed in the different phases of the project.

The proposed framework was constructed according to several usual approaches that seem well fitted to our problem. The Systems Engineering approach constitutes the base. The integration of organizational aspects uses the macroergonomics analysis and design of work systems process. For aspects dealing with human aspects, HFI methods represent a good source of inspiration. Two

approaches were of interest: the one developed in the Manning Affordability project (SC-21 S&T MAI, 1998), which is very complete and detailed and the one proposed through the HIFA project (European Organization for the Safety of Air Navigation, 2000), for the emphasis on the coordination between the project members.

Those are the core approaches used. A set of other methods or research findings was also used to complement and improve the framework.

3.2.4 Processes and tasks

The previously defined framework was then refined.

The approaches cited in Section 3.2.3 provided interesting ideas for this step as well.

The points already addressed largely in the literature are not detailed. This research focused on the following aspects:

- Design of the organization: The organization has a great impact on efficiency and safety. Designing the organization during the project to maximize those two measures is one main features of the researched method. One major difficulty lies in manipulating the complexity of all aspects that need to be taken into account.
- Function allocation to optimize RAMS: Function allocation is one major step in the design of a system. Different approaches were developed (Cook and Corbridge, 2000 and Johnson et al, 2001). This research focused on the minimization of risk, and on producing a coherent and efficient function allocation method.
- Risk assessment: As said previously, risk assessment was one major focus of this research. An efficient method to integrate organizational and human aspects was researched. Two major points of focus are: how to give the best possible representation of influencing factors and how to study the dynamic behavior of the system.

3.2.5 Models

The objective was to define models simple enough to be used by all project members, but powerful enough to enable an efficient design and risk assessment. The idea was to obtain some evolutionary modeling method adapted to the top-down approach. The first models should give a holistic view of the system, while the latest ones should be adapted to specific tasks like simulation for dynamic risk assessment.

The models used during the first phases were inspired by functional analysis (Cole, 1998), as well as other models used in SE and cybernetics. Models used for risk assessment are inspired from methods like AcciMap or cindynics (Deschanels, 2001), and quantitative assessment used approaches like the Bayesian networks.

Given that human performance and reliability strongly depend on the dynamics of the system, it seemed appropriate to think of models representing adequately the dynamic aspects of the system, like process modeling (Zakarian and Kusiak, 2001). These models could then be used in risk assessment thanks to process analysis (Kusiak and Zakarian, 1996) and simulation, for example by using Petri nets (Jampi et al., 2001).

Those models should be able to represent various aspects related to reliability like barriers and redundancy used for defence-in-depth (Valancogne and Nicolet, 2002), as well as the impact of interfaces with the technical, organizational and environmental sub-systems.

3.3 Evaluation of the framework

Evaluation refers to research questions 2 and 3. The aim was to check that the framework is functional and integrates efficiently human and organizational factors and that the company employees accept it.

3.3.1 Case

The researched method was evaluated based on its application of a specific case, which is described here.

Company

Some information about the company that hosted this case may be useful to better understand the case, as well as some results of the evaluation.

The SNCF is a state-owned company employing over 180.000 persons in France. Its activites are centered around the railway system, and include the operation and maintenance of the trains, signals, tracks and stations. It is self-controlled in terms of safety, and its main aspects and directions are defined by state decisions.

Labor unions are very strong in the SNCF, so that many attempts of evolution in the organization have ended up in strike days, which paralyze the country. This is one reason why the SNCF organization evolves at a slow pace, and this also requires many projects to adopt a "diplomatic" approach.

The organization of the SNCF is very complex, with up to fourteen levels between the top and the bottom of the organization chart. Hence, there are many departments, which sometimes have to a certain extent overlapping roles. This profusion of departments also creates tensions, given the contradictions between the objectives of some and those of others. The top management recently tried to make a shift to a management by objectives, which is likely to have strengthened this tensions. This is why the SNCF can be compared to a political organization, where influence mechanisms and "diplomatic actions" play a big role among the "Dept heads" at the various levels.

Infrastructure Maintenance System

The Infrastructure Maintenance System (IMS) of the SNCF is in charge of the maintenance of all elements composing the infrastructure: rail tracks, signals, catenaries, and bridges etc, which enable the circulation of trains controlled by the exploitation branch.

It is a complex system, important both for the safety and efficiency of circulations. Indeed, the quality of the work performed by the IMS will determine the quality of the infrastructure, and hence of the exploitation. Furthermore, the various activities performed by the IMS impact directly the circulations. It is usually necessary to stop them on a given part of the track during the maintenance work, which requires good coordination. Then, maintenance work can also cause perturbations on the signal and power lines of tracks where trains are running. Finally, maintenance trains need to move on exploited tracks to reach the maintenance site. The stakes in terms of safety and efficiency are therefore extremely high, both for the components of the IMS and those of the exploitation branch.

The IMS is currently regulated by the RG S9 referential, which serves both as documentation of the system, procedure for the workers and rules.

The IMS was conceived in the 80s, but the French railways context has evolved since that time. Moreover, the use of the IMS in its current form has highlighted many points on which improvements could be made both for safety and efficiency.

Objectives

The project studied is STORP, which stands for "Sécurité Travaux Organisation Réalisation Protection" (succession of words that can be translated as Safety Maintenance Organization Execution Protection).

A survey performed on the current personnel of the IMS has helped identify several points to improve. It appears that these points are linked rather to systemic problems than to specific ones. Hence, it was decided to adopt a systems approach in order to rethink the IMS in its whole – concepts, principles, referential, documentation.

This represents a major and complex evolution, in that it will affect more or less directly the 50,000 employees of the Infrastructure branch, can have a large impact on safety, and will have short and long-term effects.

Current status

STORP is planned in two phases. The first one consists in documenting a new IMS, while testing in parallel some improvements compatible with the current system. The second one is an accompaniment phase in order to deploy the new IMS across the SNCF.

The project is currently in this first phase and is planned to continue until 2004-2005 for an operational system in mid-2006.

Innovative approach

STORP differentiates itself from traditional projects carried out at the SNCF, especially those concerning the referential, by adopting a systems approach and focusing on human factors.

3.3.2 Methodology of evaluation

Introduction

A formative evaluation was conducted based on the information made available for the project until yet. The results achieved by the project were compared with the outputs of the application of the method.

Information used

Here are the sources of information used for applying the method to the project:

- an initial project survey, conducted by the SNCF before the beginning of the project to identify facts about the current IMS and ideas for improvements.
- project presentation documents
- project work documents
- meetings with the project team

Approach

The following approach was used:

1. First meeting with the project manager and gathering of data about the project
2. First quick application of the method, identification of the main interests of this evaluation and of the possible modalities
3. Presentation of the method, interests, modalities and results of the first application to the project manager. Discussion and gathering of data for further application
4. Global more detailed retrospective application, meetings to obtain new information
5. Identification of interesting areas, and prospective application on those
6. Synthesis. Report and oral presentation to the interlocutors.
7. Meeting with the interlocutors to evaluate the results, gather their feedback on the method, and define plans of actions to reorient the project.

Interlocutors

Various SNCF employees were met during this evaluation, either to gather data for applying the method or to give feedback on the method and its results. These interlocutors were:

- The project manager, member of the "Safety & Rules" department, with a background in engineering. He is interested in systemic approaches and motivated to take into account human factors.
- The project supervisor, also Head of the "Safety & Rules" department.
- A project member, employed by the "Safety & Rules" department.
- The first initiator of this research, Associate Director of Safety for Human Factors.
- The second initiator of this research, expert at the Center for Safety Studies, which is composed of seven experts representing each branch of activity of the SNCF, and treats specific safety projects. He is also leader of the "Methods, tools and standards for Safety & Reliability" and "Safety" working groups at the IMDR-SDF (French Institute for Risk Management, Safety and Reliability). He was vice-president of this association composed of researchers and industrials in the domains of Risk Management, Safety and Reliability.

Outputs

Several qualitative outputs were generated during this evaluation.

First, the use of the method enabled the identification of some of the advantages and disadvantages of the approach. The disadvantages identified have led to improvements.

Then, the quality of the results produced by the method was examined qualitatively, by comparing these results with the actual outputs of the project, thanks to a heuristic evaluation. This comparison highlighted some aspects that the project had missed and that were identified by the method. The results were first presented to the interlocutors, then these aspects were discussed with them during a meeting. Some of these aspects were identified as "very important for the project". An aspect was considered as such if the two following conditions were met:

- The application of the method identified it as very important for the future system
- The project supervisor or the project manager confirmed its importance and initiated specific

actions on these aspects.

Finally, an interview with the interlocutors enabled to obtain their feedback on the results produced by the method and their opinion on the method itself.

Chapter 4 - Proposed framework

This chapter describes both the framework and the way it was developed. The reader is invited to refer to the documentation of the method in Appendix 1. The various development steps are first presented chronologically, starting with the needs and resources, and then moving on to the development of the structure. Then come the main modifications brought to the original HFI approach, that is the integration of the organization, other major modifications and the development of risk management activities. The way some important ideas were integrated is then presented before the final improvements.

This chapter does not cover the aspects already addressed by the initial HFI approach. It explains the rationale of the modifications introduced, and gives an overview of the logic behind the new developments. For a detailed description of the various activities, the reader should refer to Appendix 1.

4.1 Analysis of the needs and resources

The various requirements that complement the major ones – that is the integration of human and organizational aspects and the focus on safety – are presented here. The rationale for developing the framework the way it was performed is then explained.

4.1.1 User ideas and requirements

Exchanges with future users of the developed framework helped identify some various requirements and ideas, which drove the development. Although those requirements are specific to the SNCF given the context of the research, the previous literature review proves that many of them are actually faced by a large number of companies:

- Focus: The initial need concerned a method or set of methods to integrate knowledge from human sciences into risk analyses. This was then the core need to be met by the framework.
- Integration: Previous attempts of using HF in projects failed due to a lack of integration with current practices. First, project managers and engineers believed they could easily do without HF, and actually did. Then HF inputs to the project gave information that was not reused efficiently as there was no "structure" to integrate that kind of knowledge in the project process. Lastly, by lack of integration, the exchanges between engineers and HF specialists are rarely beneficial because they do not know the inputs and outputs required by their counterparts.
- "Unexpected" scenarios: One major failure cause in projects is the inability to take into account "unexpected" scenarios of the future system. "Unexpected" covers both scenarios in degraded mode and scenarios driven by non-prescribed behaviors.
- Impact: Another cause of failed projects is the lack of understanding of the possible impacts of the project, that is the consequences of the project on the various subsystems that constitute the company.
- Improper understanding or insufficient knowledge of basic human and organizational reliability notions: Some notions were considered as essential by the main stakeholders, and appeared not to be well understood or known by the future users. Those notions include: redundancy, prescribed/real, recovery
- Improper understanding of systemic approaches: Many engineers or project managers in the SNCF have spent most of their carrier "on the field", managing groups of technicians. Furthermore, SE is not commonly used in France. Hence, many engineers have not been used to systemic thinking nor to some simple tools – some even believe that safety can only be done with texts and that models are dangerous for dealing with this aspect.

4.1.2 Derived requirements

The previous user ideas and comments and the literature review led to the following requirements, which can be seen as the chosen solution among the possible ways of solving the problem:

- Introduce SE: Many projects deal with systems, so a systemic approach can be profitable. Aside from the "systems" aspect, SE also encourages a structured approach, which is required to overcome the traditional "fuzzy" project management practices that lead project teams to miss many important aspects, especially the ones related to HF.
- Underline the main notions: The framework must be built so that users cannot miss the essential notions, even if they lack background in systems safety and HF.
- Use proven methods: Many potential users are already reluctant to HF. Bringing a new untested method is unlikely to generate a good acceptance. Hence, the framework needs to be based on methods that proved their worth to a certain extent.

4.1.3 Choice of resources

Systems engineering

Systems Engineering was chosen as the basis for the framework. It is indeed the best-recognized systemic approach and presents interests both in its principles and structured process. Users of the researched method can also benefit from the tools developed for SE. Furthermore, using it at the base will help extend and improve the framework over the years as the discipline progresses.

Human Factors Integration (HFI)

The structure of the proposed framework was then developed based on HFI. There are several interests to proceeding like this:

- HFI is a solid approach. It is based on systems engineering and is the result of major research projects both in the military and civil sector. It was used in several cases and proved its efficiency. As stated by Angus et al. (1998, p4), "Recent U.S. Army projects illustrate well the return on investment due to HSI, such as the 'cost saving to investment ratio' of 44:1 for the Comanche helicopter (cost savings of $3.29B, HSI investment of $75M), 22:1 for the Apache helicopter (cost savings of $269M, HSI investment of $12M), and 33:1 for the Fox NBC Reconnaissance vehicle (cost savings of $2-4M, investment of $60k)."
- HFI is an open approach. It can be easily extended – one example is the integration of the new domain "survivability" in the U.S. MANPRINT program. It is also open in terms of form, content and level of detail. Hence, it is suitable for the various evolutions required by this research.
- Future evolutions in HFI can be reutilized. For example, in the context of the Manning Affordability project, the HFI framework serves as a guide to drive human factors research. Those researches lead to the identification or development of methods and tools that will also be usable with the proposed framework. Another example is the recent development of HFI add-ons: HFI Capability Maturity Model (CMM) (Earthy et al., 1999) and HFI Cost Effectiveness Assessment (CEA), which can be used with the framework. HFI CMM helps evaluate the level of practices regarding HFI. HFI CEA covers the cost aspects of HF and hence represents an interesting add-on.

4.2 Structure

4.2.1 Development of the structure

As introduced in 4.1.3, the structure of the framework is inspired from Systems Engineering and HFI. More specifically, the frameworks proposed in the HIFA and Manning Affordability

projects were used. Various aspects account for this choice:

- These are the HFI projects whose results are the most accessible.
- Both methods are inspired from the MANPRINT project. They are therefore compatible.
- Both methods are complementary:
    - The Manning Affordability method presents activities and tasks in a very detailed way, and relies on a clear structure. It covers various aspects of SE, going further than HF alone. However, it does not cover the whole lifecycle of a system and lacks information about the management of the project team.
    - The Human Factors Integration in Future ATM Systems (Hifa) method concentrates more on the composition of the project team and responsibilities within it. It covers the same steps as the Manning Affordability method, but goes further and covers the production, pre-operational and operations phases. However, it is less detailed and also less structured, which makes it more complicated to use. (It gives a list of activities for each phase, whereas the Manning Affordability method is structured in phases composed of activities, each represented by a process, and details each task of this process).

In the context of this research, one objective was to offer a method detailed-enough to guide efficiently the users. Furthermore, it seems that good HF integration depends on the way the project team will analyze problems and drive the project. Most of the project managers or engineers at the SNCF are technical people with a very good knowledge of railways, but who lack skills in systemic approaches. In this case, integrating HF requires more than simply telling at each step of the project what human aspects to take into account. It requires to modify the way people work in projects, and make them apply SE. The Manning Affordability approach goes further than other HFI approaches as one of the main goals of their HFI process is to "define a generalizable process for human engineering that is compatible with systems engineering practices" (SC-21 S&T Manning

Affordability Initiative, 1998, p4). Hence, the Manning Affordability approach served as the first structure of the method.

This structure was adapted to fit the project management guidelines used in the SNCF (Table 1-1 p4).

As studies showed that one major obstacle to the integration of human factors lies in the management of the project team, it was then decided to integrate activities related to these aspects thanks to the Hifa approach. Finally, in order to ensure the necessity to take into account human factors during the whole lifecycle, the obtained framework was extended using also this approach.

4.2.2 Proposed structure

The main structure is described in Figure 4-1.

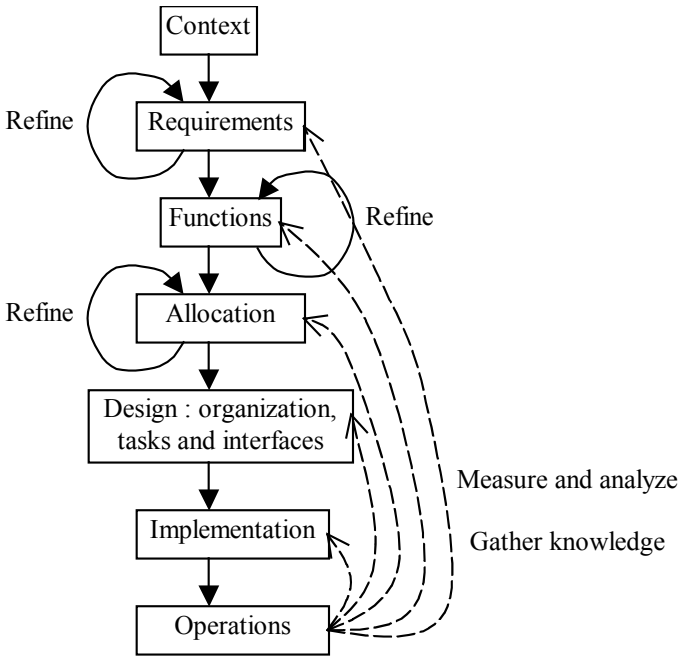


Figure 4-1 Main Structure

It can be observed that it is inspired from the SE framework.

The context of the project and of the future system is first studied. This enables to elicit at best the requirements, which are then allocated to functions. These functions are then allocated to elements or groups of elements of the system. Afterwards, the main elements are designed. Finally, the design is implemented and the system can be put into operations.

The reader is invited to consult Appendix 1 for a more detailed synthetic view of the method ("Overall view of the method" on page 6 and 7).

As underlined previously, the proper integration of HF depends on the good management of the team. Figure 4-2 illustrates the corresponding activities.

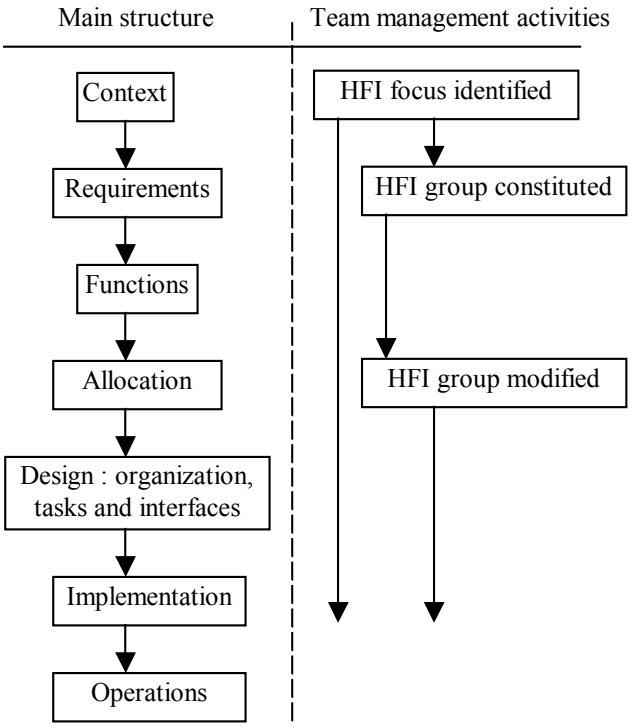


Figure 4-2 Team management activities

At the beginning of the project, an HFI focus is identified among the project team members. It is chosen for its sensibility regarding HF and its previous experience of HFI. Once the requirements for the various HFI domains were identified, a HFI group is constituted, based on the aspects identified for each domain. The members of this group will focus more precisely on their domain, and eventually be specialists of that domain if necessary. At the allocation stage, the group can be modified if its constitution seems unsuited to the composition of the designed system.

4.3 Integration of the organization domain

4.3.1 Introduction

The second step consisted of including a new domain covering the various organizational aspects. Those were already partly covered in HFI thanks to the personnel and manpower domains. However, thinking the organization goes beyond the scope of defining its structure, even more as one objective of the method is to construct the organizational reliability as explained in 4.5.

Hence, it was chosen to develop this aspect. The first activities were of major interest to enable then a "natural" propagation to the other activities thanks to the top-down approach. The MEAD process was a good source of inspiration for this purpose, in that it presented a given number of similarities in its structure and activities with the HFI process.

It is to be mentioned that a major part of the integration of organizational aspects was conducted during the development of the risk management activities.

4.3.2 Evolution of the structure

Here is a presentation of the main modifications brought to the structure. The reason for carrying out these specific modifications lies in the needs and resources identified previously. These modifications werethen refined thanks to the evaluation detailed in Chapter 6.

4.3.3 Study of the context

This context activity was extended by integrating the notion of vision and principles, in order to focus on the goal the system must reach and the values it communicates. The identification of the relationships with the environment was extended to integrate outgoing relationships and enhance the integration of dynamics.

The identification of the existing system seems essential, as a project in a company like the SNCF often modifies an existing system rather than designing a whole new one. This also implies to analyze more closely the organization in which the system integrates. Hence, specific tasks were added to the activity in order to cover these points.

Two tasks were also introduced to enable the specification of organizational dimensions in two steps. Those tasks cover the various questions related to the organization, among others its structure, level of integration and formalization, the handling of communication and coordination, organizational learning, culture, etc, inspired from NEA (1999). As the method defines a framework and gives the user freedom about the tools he chooses, other sets of characteristics can also be used. For example, an approach such as that proposed by Majchrzak and Borys (2001) is of interest for a more complete organizational analysis, furthermore as it benefits from a computer tool support.

This initial organizational specification will allow and generate automatically a better integration of organizational aspects in the following activities:

4.3.4 Requirements analysis

The new domain "organization" was introduced. It is then necessary to identify requirements about it and define associated guidelines. These requirements are identified based on the initial organizational specification.

Functional analysis

Requirements are allocated to functions, so the addition of the organization domain to the requirements enables functions related to the organization to be studied. Furthermore, the notion of resources, objectives and behavior was strengthened to ensure that these aspects – essential to a good understanding of human and organizational aspects – are well addressed.

Function allocation

The function allocation activity was extended. The original approach consisted of allocating functions to human or machine or the combination of both. It was changed to start from the whole view of the system and its main mission, in order to allocate first between entities of the organization, until the final allocation of tasks.

Design

A new activity was developed in parallel of the task and interface design activity. It does not only cover the various aspects – structure, flows, objectives, resources, constraints – but also invites the user to take into account the possible evolutions of the organization as well as its integration with the existing organization and the associated risks. The notion of performance management is also emphasized, as well as the definition of rules required to ensure organizational reliability.

Operations

The organization's health is to be analyzed and its evolutions are studied, in order to reduce risks like the "normalization of deviance" (Vaughan, 1996).

4.3.5 Synthesis about the organization

The organizational factors were integrated so as to ensure that this major aspect is not missed in projects, nor forgotten within the project. The whole method is based on the principle that a project creates or modifies an organization, so that users understand within their project the worth of taking the organization into account. By forcing the users to think about various characteristics of the organization of the system concerned by the project, and those of the organization in which this system integrates at the beginning, the method helps to identify important issues or potentials, as well as fix some guidelines about the organization. This will help to construct the technical system around the organization, and not the contrary as it often happens. The organization then remains a constant concern through the project and the system's lifecycle.

It can be noted that SE provides a good base for addressing organizational aspects, in that it considers the system as a whole. By integrating the organization in the various models and activities – which mainly comes to enlarge the focus usually taken in projects – the method benefits from the SE approach to ensure a good repercussion of those factors.

4.4 Main modifications

The activities, which existed in the original method but were significantly modified, are now described.

4.4.1 Further changes to the function allocation activity

A further literature review enabled the highlighting of many different approaches to the function allocation activity. Among the most recent ones can be cited Dearden et al. (2000), Wright et al. (2000), Cook and Corbridge (2000) and Older et al. (1996).

The method used in the Manning Affordability approach is very close to the one proposed by Older et al. (1996). Johnson et al. (2001) propose a new framework based on the comparison of this approach and the one by Dearden et al. and the identification of their respective pros and cons. This framework served as a base to modify the function allocation activity in the proposed method. This framework has indeed some advantages on its predecessors, in that it combines the following characteristics:

- it is scenario-based
- it supports the "iterative refinement of the organizational structure and the allocation of function" (Johnson et al., 2001, p183). Hence, it is compatible with the previous evolution (see chapter 4.3.4) to integrate more significantly the organizational aspects.
- it is based on a more "human-centered" design, unlike the approach by Dearden et al., which invites the users to think first in terms of total automation.

After this changes, one major disadvantage still appeared in the function allocation activity. Hence, all methods mentioned the need to address dynamic allocation – i.e. an allocation evolving depending on the context of use – but none of them provided an approach for it. A specific approach was then developed. One major concern was to make it fit with the other activities, and also to have it underline the main principles and notions of the proposed framework. Among those notions, that of prescribed/real and the associated risk seems really important in this context.

Here is the general approach behind the developed activity:

1. the functions that can be allocated dynamically are identified
2. they are categorized depending on the interest of a dynamic allocation, and on the risk of such an allocation to develop or evolve even if unwanted
3. the possible allocations and transition modes are identified
4. the acceptability of the allocations is evaluated (requirements / measures met?)
5. for unacceptable allocations, barriers and ways of recovering are designed. For acceptable ones, triggers are developed
6. the allocations are integrated into the design

4.4.2 Other modifications

It was decided to simplify the process for the function analysis activity. Here are the reasons for this choice:

- the process in the Manning Affordability method was very complex. It is likely to frighten future users, and make them deviate from the original objective of the activity.
- there exist many documents and norms on function analysis, which can be used for further information
- the intent was to focus on one major requirement for this activity, which is to not only describe the function structure, but also their behavior (Zakarion and Kusiak, 2001) and the goals related to those functions (Modarres and Cheon, 1999; Jalashgar, 1999). This is why a simpler process focusing on those aspects was designed.

Other modifications were brought to the method. Those essentially concern the integration of notions and are described in 4.6.

4.5 Development of risk management activities

4.5.1 Introduction

The major improvement of the proposed framework over the previous approaches is its emphasis on risk management and more specifically safety management. Hence, specific activities had to be developed for this purpose, using various concepts from the disciplines dealing with risks and safety (cindynics (Deschanels, 2001), RAMS, human reliability, organizational reliability).

Safety is considered an inherent part of the method. Hence, a risk management activity is associated with each major activity of the method. The safety of the system is then designed progressively in a top-down manner, in parallel of the system itself and depending on the current knowledge about it, as illustrated in Figure 4-3. Safety is built on the concept of "defence in depth" (Valancogne and Nicolet, 2002) with barriers developed at each level of detail of the system.

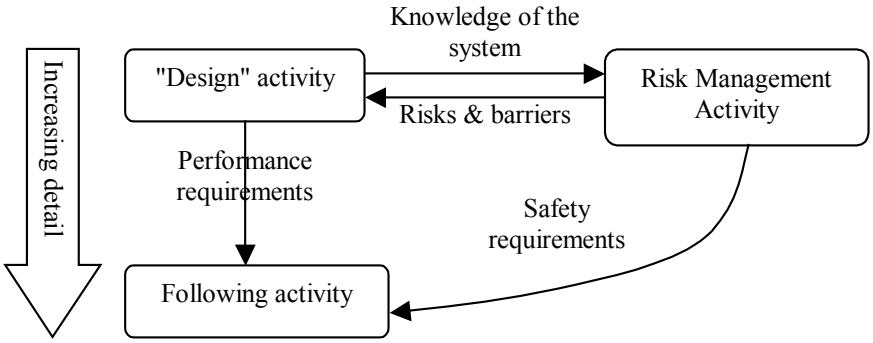


Figure 4-3 Organization of Risk Management activities

It is considered that the reliability of the system depends upon several aspects, which are focused on in the different activities:

- ability to perform correctly relevant tasks (and hence avoid system malfunctions)
- ability to limit consequences of a system malfunction through barriers

- ability to limit impact from other sources of hazards and the possible consequences through barriers
- ability to sustain all the Important for Safety (IFS) elements through an appropriate organization and management
- ability to cope with variances. As defined by Hendrick and Kleiner (2001, p76), “a variance is an unexpected or unwanted deviation from standard operating conditions, specifications, or norms”.

The identification of IFS elements throughout the project enables one to know upon what the safety structure of the system relies. This is a good and simple approach to help focus on the correct points during the project, but also to avoid modifications that could endanger the system during its lifecycle. It also helps to evaluate the "health" of the system based on those IFS aspects, eventually using methods like the one currently developed by the Institut National de l'Environnement Industriel et des Risques (Le-Coze et al., 2002), or the one by Norm and Cetop ("FHORTE" method, stands for "Méthode d’analyse et de développement des performances de la Fiabilité Humaine, ORganisationnelle et TEchnique d’un système socio-technique"), which both identify and check the IFS aspects of a running sociotechnical system to evaluate its safety.

Such an approach enables the handling of the various types of risks, from easily predictable ones to ones that cannot be predicted, and offers defense mechanisms at all levels, from the appropriate design of the organization to safety management, barriers and the design of the tasks.

4.5.2 Risk management activities

Management of risks linked to the context

This activity is inspired from the cindynics approach, and especially the cindynics analysis matrices (Deschanels, 2001). Traditional risk analysis methods are rather intended for technical

systems. Cindynics proposes an approach that fits better with our concerns, in that it studies the global risks of a system, and was developed for large industrial systems or "public systems" (railway stations, towns, etc).

An investigation of the context enables us to define four major elements: the objectives and missions of the system, its relationships with the environment, the system in which it integrates and its initial organizational specification.

Hence, the reliability of the system will be studied through its ability to fulfill objectives that are "Important for Safety" (IFS) while creating no unwanted effect on itself and the systems with which it interacts. This ability will depend of its "inner" components, especially its organization, as well as outer systems that have an impact on it.

This will lead to the identification of unwanted events and IFS aspects of the system. A first level of barriers can already be developed, which will constitute new IFS aspects. These IFS aspects will then be transformed into requirements, leading to concrete elements or tasks of the system during the remainder of the project.

Risk management related to the requirements

Previously identified IFS aspects were turned into IFS requirements. From the analysis of requirements on the system, and more specifically on the HFI domains, some new IFS requirements may be identified.

The safety of the system depends on the availability and reliability of those IFS requirements, that is, on the following elements:

- capacity of the project to meet these IFS requirements
- reliability and availability of the IFS requirements during the life of the system
- infrastructure required to support these IFS requirements

Barriers are also identified to ensure the reliability of the IFS requirements, leading to new IFS requirements.

Risk management related to the functions

IFS requirements are turned into IFS functions. The reliability of these functions is studied using two approaches. First, a quite traditional approach based on the reliability of the functions itself, as well as that of the flows between them and their behavior. This helps to identify possible degraded scenarios. Then, a more original approach based on the notions of prescribed/real and redundancy. In this way, the various ways an objective may seem to be reachable are studied. Acceptable scenarios will be used for optimization, by identifying a better way to reach an objective (which the human in the system will naturally try to do) or for process redundancy, in order to keep several solutions to reach IFS objectives in order to improve reliability. Barriers are developed in order to avoid entering an unacceptable or previously identified degraded scenario. Functions are also developed to enable the identification of these unacceptable scenarios, and the way to recover from them.

Risk management related to function allocation

The reliability and safety of the system depend on the ability to choose the most appropriate allocation, as well as ensure the right allocation will be chosen at the right time during the operations if multiple allocations are possible. Allocations are evaluated based on their ability to satisfy the IFS requirements and avoid non-recovered unacceptable scenarios, especially by making the best use of human and technological capacities and limits.

At this point, tools to enable a quick assessment of interfaces and tasks like THEA (Pocock et al., 2001) can be useful.

The dynamic function allocation activity described in 4.4.1 handles the reliability linked to the choice of the right allocation.

Risk management related to the design

It is considered that the safety/reliability of the system depends upon two aspects:

- the good execution of IPS activities: The predictable risks can be avoided if activities with a big impact on safety are well performed, as well as those constituting the barriers. More specifically at this level, the reliability of the tasks can be studied using human reliability approaches. The previous activities can be reused here efficiently, as a better understanding of the context enables a more accurate study of a task.
- appropriate safety management: Indeed, it contributes to the IFS activities, and also represents the major barrier against unpredicted risks. More specifically this includes the ability to identify, study and respond to variances, and to maintain IFS organizational dimensions during the lifecycle of the system.

During this design phase, some activities included in the design activities are directly related to risk management, concerning both the organization (Appendix 1, tasks 2.7.8, 2.7.9), the tasks (2.8.8,2.8.9, 2.8.10), interfaces (2.9.7, 2.9.13, 2.9.19) and the workload (2.10.14).

Once this point is reached, before the production of the system, previous studies will be used together. Indeed, until yet, a top-down approach was used with deductive analyses in parallel. The user is now able to build a complete picture of the safety of the system and to analyze it in a deductive and inductive manner. Given the good knowledge of the system acquired, it is possible to use methods such as AcciMap (Svedung and Rasmussen, 2002) or SAM (Paté-Cornell and Murphy, 1996).

Risk Management related to production / implementation

Modifications are studied to ensure that they do not alter the safety of the system. Tests are also performed to verify some assumptions.

Risk Management related to the operations

Safety of the system is ensured through continuous checks of its "health" through the measures. Variances are studied and appropriate measures are taken over time. This enables the gathering of data for additional projects, especially in the fields were little quantification is available like organizational risk indicators (Øien, 2001).

4.6 Principles integration

The previous sections described the method quite generally through its main functions. It seems interesting to cross these major functions with the integration of various notions, which appear in different activities and are linked to the various aspects of the framework and development process.

The activities and tasks mentioned in this section by their numbers refer to the documentation of the method in Appendix 1.

4.6.1 Prescribed versus actual behavior

This principle is underlined all along the process as it is a major one when taking into account human behavior. A human will not necessarily behave as it was planned during the design phase (prescribed behavior), for various reasons – improper understanding of the instructions, search for an easier solutions are some examples. When dealing with safety, this becomes very important. Planning those possible evolutions during the project may help identify some scenarios where the

real behavior is likely to be different from the prescribed behavior, and scenarios where such a variance can be hazardous. Further than human behavior, this notion is also enforced at the organizational level, to take into account the fact that the organization may not be as it was planned – for example for acceptance reasons, or evolve to a very different one.

This notion is first underlined in Task 1.1.12 concerning the organizational design. Highlighting the possibility of an organizational variance early may help keep that aspect in mind during the project. The identification of IFS aspects in R1 ensures then that the important aspects are known. Those are the ones to be maintained even if the system evolves. Task R2.3 contributes to this effort.

The activity R3 then plays a big role for this notion. Indeed, the possible alternative behaviors are identified and analyzed (R3.2, R3.7). The idea is to turn that possible weakness of the system if ignored into a potential, as illustrated in Figure 4-4.

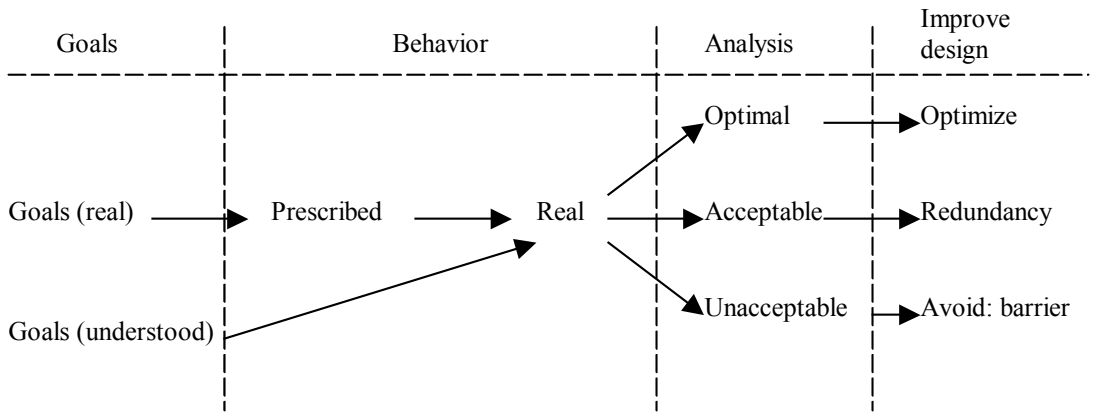


Figure 4-4 Process for prescribed/real functions, tasks and allocations

A non-prescribed scenario may be optimal, in which case it is better to make this scenario directly the prescribed one. It may also be acceptable, in which case it can serve as a redundancy scenario if the prescribed scenario cannot be achieved. A large number of acceptable behaviors may

also imply that the function was defined with too much detail, with the consequence of producing heavy procedures, in which important aspects may not be seen. Identifying that may help optimize this too. Finally, some "real behaviors" may not be acceptable; in this case some barriers can be developed to avoid them.

The allocation process also takes into account this notion through the dynamic allocations. Possible reallocations during operations are identified in Task 2.4.3, then the same process as for functions (Figure 4-4) is repeated to find the optimal allocation, ensure the best allocation is chosen at the right time and hazardous allocations are avoided.

At the design stage, the notion is strongly enforced. Concerning the organization, the possible evolutions are analyzed (2.7.11) as well as the associated risks (2.7.9). This helps to design a measurement system, which restricts the occurrence of hazardous deviances (2.7.10) as well as rules (2.7.11) to make sure that no dangerous evolutions is driven by managers. Similarly, the possible (no-prescribed) tasks are identified (2.8.2) and studied using the same approach (Figure 4-4) as for functions.

Finally, during operations, the resulting design, barriers and measurement system help continuously optimize the performance and safety of the system.

4.6.2 Degraded modes

Taking into account states of the system identified as hazardous is essential to design a safe system. Indeed, it helps design the right barriers to avoid entering these states or scenarios, and embed the functions required to identify the presence of a hazardous scenario and recover from it in the design. Although it may seem obvious to risk professionals, taking this into account is either forgotten by some project managers by lack of experience, or done partly only at one given level of the design.

Degraded modes are addressed all along the project process, depending on the level of detail with which the system is currently known. Task 1.1.9 first encourages the identification of degraded scenarios that can be faced by the system. Those are then translated into requirements. R1 and R2 help identify possible causes of degraded modes, and a more complete analysis is performed in R3. The system is strengthened by developing barriers to avoid entering a degraded scenario, and the ways to recover from such scenarios are designed. Thinking of those scenarios is essential, as those are usually the cases where the users feel "lost", loose understanding of the system and hence need very accurate guidance on what to do. The various causes for entering in degraded mode and the consequences are assessed during function allocation (including the possibility of a bad choice of dynamic reallocation), as well as through the design. Indeed, degraded modes can initiate in the long term from the organization, or on the short term from tasks; and associated interfaces will tell the user that the system is currently in a degraded mode and help him/her recover.

4.6.3 Defence-in-depth

The concept of defence-in-depth was presented in 2.3.6. Its interest for this research is that it can help give a global view of the safety mechanisms involved in the system. However, defence-in-depth presents a fallacy and as such shall not be over-used, but crossed with human and organizational reliability studies.

The idea is not to build a system relying heavily on defence-in-depth, but to consider that any system presents some kind of defence-in-depth. Rather than observing the various barriers independently, the defence-in-depth theory helps get a systemic and "easy to understand" vision of the interrelationships between these barriers. Especially, this shall remind non-specialists that some organizational factors have an impact on safety, and as such should be handled carefully. The second idea is to build this global picture of the barriers, and then provide workers and supervisors with it.

The appropriate measures of the health of these barriers shall also be provided to them, in order to avoid the development of unknown "windows of opportunity" (Reason, 1990) and help these actors of the system to be proactive.

During activity R1, important elements and hazard sources are identified, in order to know what needs to be protected, and from what to protect. Barriers are associated to ensure the protection of these elements and from the sources, which constitute the first level of barriers (those can of course be redundant, against a single cause / for a single element or by protecting "at the source" and "near the element"). Those barriers then become requirements in the system, and are tested in R2 against possible failures, either from the project, or from the system in operations and its infrastructure. This helps to design new second-level barriers to protect the first level barriers. Other first-level barriers are also identified by R2. The barriers are then turned into functions. R3 helps to identify new barriers and protect the existing ones. This recursive process then goes on, with some checks about common modes, until the detailed task design is complete. Every source of hazard and important element of the system then have various barriers of various natures, themselves protected by other barriers to ensure the overall safety of the system, thus leading to the concept of "defence-in-depth" as one single problem is not going to ruin important elements.

4.6.4 Redundancy

Redundancy constitutes one kind of barrier that can be implemented in a system. If technical redundancy is usually well understood, the way to implement such a redundancy when humans are concerned is not so obvious. Some people not proficient with HF in safety – that is, the main users of the method – tend to think it works the same way: put two humans in parallel doing the same task. Such a redundancy would not only be resource-consuming, it may also have the contrary effect, if

every operator comes to rely on its "redundancy", or does not know what this "redundancy" has just done.

In the method, redundancy is considered at the function and process level. Hence, redundancy is achieved when there are multiple acceptable ways to perform a function / meet an objective. This redundancy can be either in the tasks performed, in the process, or in the resources allocated. Redundancy alone is not sufficient however to improve the safety. This redundancy should be analyzed by the designer, and made available to the users.

The notion first appears in R3, where the various scenarios are studied (R3.2, R3.7), the bridge between scenarios identified (R3.8) (for example how a scenario may move from the normal state to a degraded one, and what bridge can bring it back in a redundant acceptable scenario) and finally the modes of recovery analyzed (R3.10) (how to drive the "jump" from a degraded scenario to a redundant one). This is for the function / process redundancy.

Then, as a cause of failure may be the unavailability of system elements in charge of performing a given function, redundancy is studied again in the dynamic allocation activity 2.4. Given the safety requirements (among other possible requirements), the functions that could benefit from a dynamic allocation are first identified (2.4.2), as well as the existing associated resources (2.4.4). The possible allocations are then studied (2.4.5) as well as the bridges between those allocations (2.4.6). The acceptable allocations are kept as possible dynamic reallocations, and reallocation activators are identified (2.4.9). This includes activators in case a redundancy allocation needs to be chosen.

Those redundancies can then be studied qualitatively or quantitatively in R4 and R5. Finally, redundancies are also taken care of in Task design 2.8, by identifying possible non-prescribed tasks and using them for recovery modes.

4.6.5 Recovery

Recovery is an essential part of safety, especially in the method where the idea is really to design the safety of the system. Hence, a specific focus is put on this step. It is of course strongly related to those of redundancy and barriers.

Recovery modes are identified at the function level in R3.10, where the idea is to avoid a system in a degraded state remaining in this state or entering an even more degraded one, and putting everything in place so that it can come back to a normal state.

Then, concerning the dynamic allocations, the possible allocations are studied. The reallocations that are not suitable are identified, and appropriate recovery ways are studied to ensure that the system can come back to an acceptable allocation for a function.

Recovery modes are addressed at the lower level during task design (2.8.10) to improve the probability of recovering from a badly performed task.

4.6.6 Dynamics

As it is introduced by Forrester (1991, p5), "System dynamics combines the theory, methods, and philosophy needed to analyze the behavior of systems in not only management, but also in environmental change, politics, economic behavior, medicine, engineering, and other fields. System dynamics provides a common foundation that can be applied wherever we want to understand and influence how things change through time". System dynamics are even more important when it comes to human and organizational aspects. Indeed, the human user needs to understand those dynamics in order to cope with the situation, and it cannot be studied as a technical element in a static view. Of course, dynamics is not easy to address quantitatively for example, given the current limitation in tools and computing power. However, keeping in mind that the system is not static may drive a better design.

Dynamics are first studied globally around the notion of mission phases and mission scenarios in 1.1. This knowledge will be kept along the project through the requirements and functions.

During the function analysis activity, the importance of not only defining the structure of functions, but also the behavior is underlined. In R3, possible failures in behaviors are also identified, as well as the ways to move between scenarios.

The dynamic aspect of the system is also studied during function allocation, with the dynamic allocation activity 2.4 that was specifically developed. This appears as an essential aspect that was not dealt with properly in the Manning Affordability and HIFA methods.

Dynamics of the organization are also taken into account, through the internal dynamics (behaviors) and global ones (evolutions). Task design covers the same need with durations, frequencies and sequence.

Overall, the practice of working with clearly defined scenarios is a major element to ensure that system dynamics are well understood and addressed.

4.7 Development and improvement

The method was then checked to ensure its coherence and to complete or reorganize some activities if necessary. The various tasks were detailed to ensure an easy and efficient use of the documentation. A presentation of the major principles of the method and of its general functioning was also included.

Some remarks from future users led to further improvements. In order to handle at best the training and constitution of project teams, mandatory and optional skills and knowledge were defined for each main step.

A "guide" was also added to the documentation in order to help the users identify at the beginning of the project which activities are important and require a specific focus, so they can

"customize" the method. This guide is comprised of a set of six main questions, refined through sub-questions, which cover the main dimensions of a project related to the organization and human factors. Depending on his/her ability to answer the questions, the likelihood of an evolution of the answers during the projects and the type of answer given, the user is advised on which activity need to be performed in greater detail.

Chapter 5 - Results

This chapter presents the results obtained by evaluating the method on the case introduced in Section 3.3. First the modalities of the application are defined. Then, the results of the application are presented. Finally, the outputs of this evaluation are presented, both in terms of improvements made to the method and quality of the results produced.

This evaluation concerned essentially the first activities of the method, which deal with macro-aspects and global safety concerns. Those are the activities to which the most changes were made from the original HFI methods, and which required testing.

Detailed design activities are more directly inspired from the Manning Affordability method. They are mostly concerned with microergonomic design, and were tested on large military projects involving many microergonomic concerns. Hence, not testing them in detail does not reduce significantly the interest of the evaluation. The method was extended, so that the information available when carrying out those specific components is at least as detailed. Hence, previous test results of those components still apply for the method.

5.1 Overview of the evaluation

5.1.1 Introduction

The project chosen for this formative evaluation and introduced in 3.3.1 is a complex and large-sized project, which has the goal to redesign the Infrastructure Maintenance System of the SNCF. There are some advantages and disadvantages of choosing this project for evaluation.

The following are some of the primary advantages of choosing this project:

- The project implies an organizational change over a large number of employees. This makes it suitable for testing the organization portion of the framework.
- The project can have a major impact on safety. It is then appropriate for evaluating the researched method aimed at projects in an very safe context.
- Given the current state of the project, the results obtained with the method can be compared with the results of the project.
- This project is in itself innovative compared to other SNCF projects, as the project managers have chosen from the beginning to adopt a systems approach and to integrate HF. For this purpose, they used more a general philosophy and some basic knowledge than a method like the one developed. . Hence, the evaluation shows what benefits can be obtained from applying the method itself rather than simply using some SE and HF notions and tools.

On the other hand, a few disadvantages are related to this way of proceeding:

- Given the size of the project, a full evaluation of the method is not possible.
- In order to make the most out of the method on such a complex project, it should have been applied by a skilled SNCF team.

However, it seems that those disadvantages could hardly be avoided: a full test would require a much smaller project, in which case only the micro-aspects of the method could be tested. This was not desirable as the initial HFI methods have already been tested on those points. Then, the limitations caused by the lack of knowledge about the IMS may be used positively. To a certain extent this represented a challenging test, as the project was led by personnel with excellent knowledge of the SNCF and especially the IMS, whereas the evaluation of the method is performed mostly by the author, who has no background in railway systems and little experience in project

management. In this situation, obtaining good results with the method shows even more clearly its superiority. Furthermore, this helped reduce experimentor bias.

5.1.2 Scope of the application

As introduced in 5.1.1, given the size of the project and its current state, the method could not be tested completely. The following is a description of the extent to which the various activities were tested. Refer to Appendix 2 for the application of the method.

Conceptual design

Activities 1.1 to 1.4, R1 and R2 were tested in detail on the whole project. Activities 1.5 and R3 were also tested in detail, but the application was restricted to two functions: the maintenance work preparation, and the realization. Activities 1.6 and 1.7 did not present an interest in the context of evaluation.

Design

From this point on, the evaluation was restricted to the two functions introduced previously, and to one of the action modes of the project: the way preparation of maintenance work is performed (and of course the impact on other elements).

The activities related to function allocation were applied partially, as the allocation was mostly fixed for the project. Indeed, the current structure was to be kept, and the new or modified tasks could hardly be allocated to a different group of people given their skills. The evaluation focused more specifically on reallocation of the "preparation" activity between the workers and their managers.

Starting from activity 2.7, the application was used to identify some points on which the project should focus on later.

5.2 Results of the application

This section covers the various steps of the method performed during this evaluation. For each task it illustrates the outputs that could be obtained by applying the method to the STORP project. Interesting points raised through this application are highlighted. A more synthetic overview of the benefits of this application is presented in 5.3 and 5.4.

5.2.1 Conceptual design

Study of the context

Identify mission, vision and principles

The goal of the STORP project is to redesign the Infrastructure Maintenance System (IMS).

The mission of the IMS is to enable the realization of maintenance operations required for the good health of the railway system, while enabling the continuation of circulations and without putting in danger SNCF employees and passengers.

The vision of the IMS is to continuously improve its productivity (and by extension the quality of the exploitation) and its flexibility as well as the safety of its personnel while maintaining the level of safety of the exploitation, especially thanks to a better dynamics of the "documentary referential".

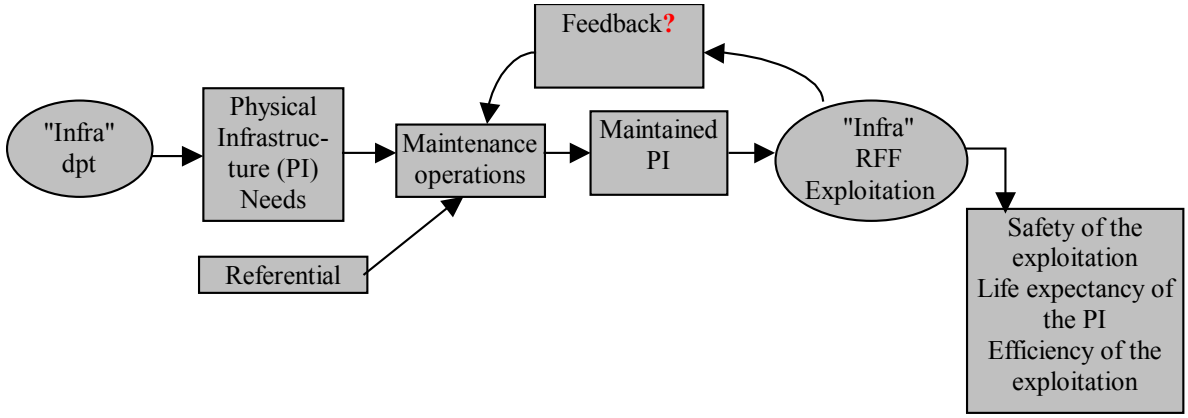
Based on this mission and vision, some interesting points can already be identified:

- the IMS has to meet 2 major requirements: efficiency and safety
- those requirements are both internal and imposed by the exploitation

- based on the vision, the project shall improve the efficiency and the "internal" safety, while maintaining the "external" safety.

This helped strengthen the project along a given orientation and keep it in focus, whereas the original project had progressively lost its unity to become a superposition of subjects, and more risky, it had lost the notion that the failure of one aspect of the project would mean the failure of the whole project.

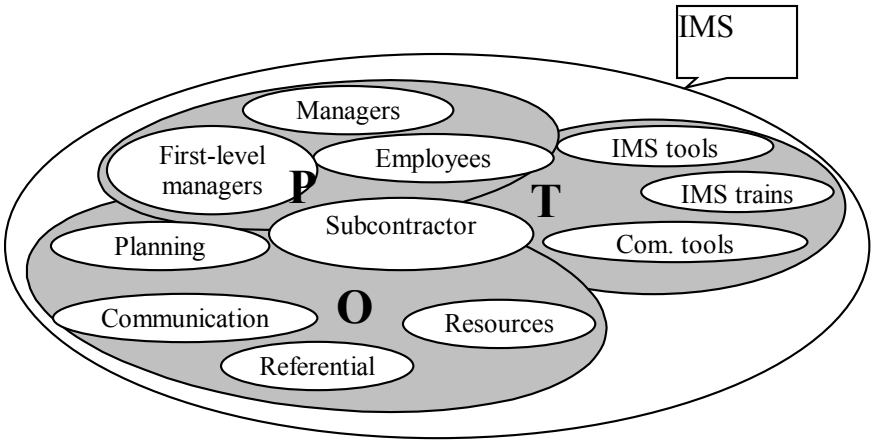
Identify the system



(Remark not included in the original document: RFF stands for "Réseau Ferré de France". It is the organism created in 1997 that now possesses the railway infrastructure in France, as well as the debt of the SNCF).

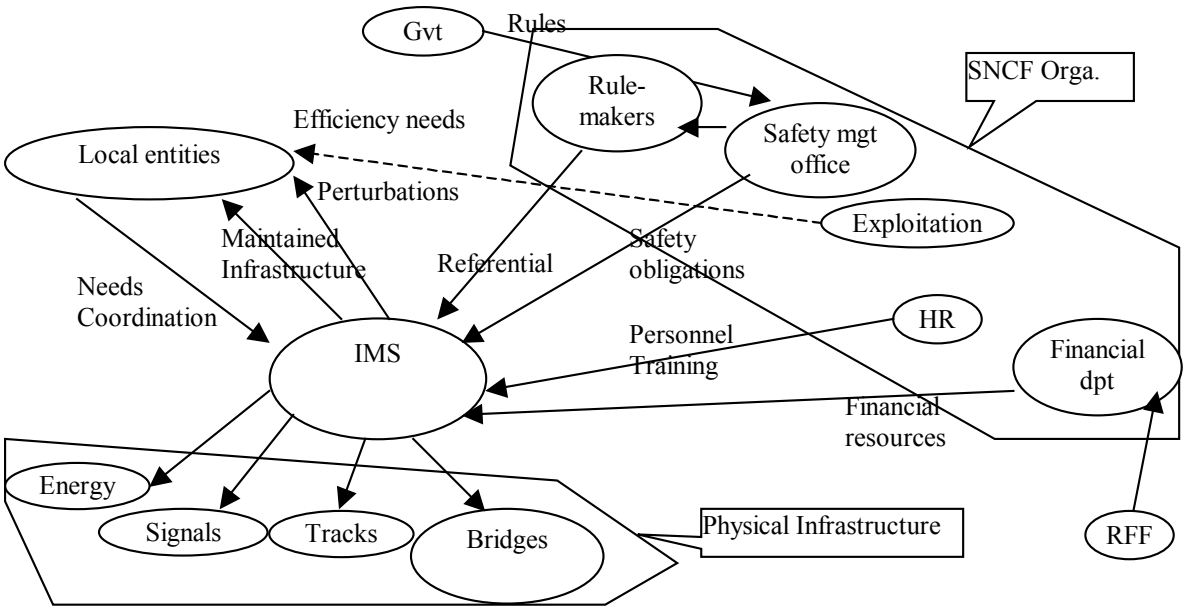
Identify the limits of the system and its environment

Here are the limits of the IMS:

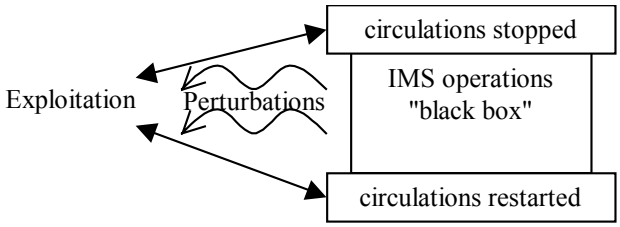


It can be observed that there does not exist a precisely defined IMS yet. Hence, we consider as elements of the IMS the elements in strong correlation with the realization of the maintenance operations, which the STORP project can modify.

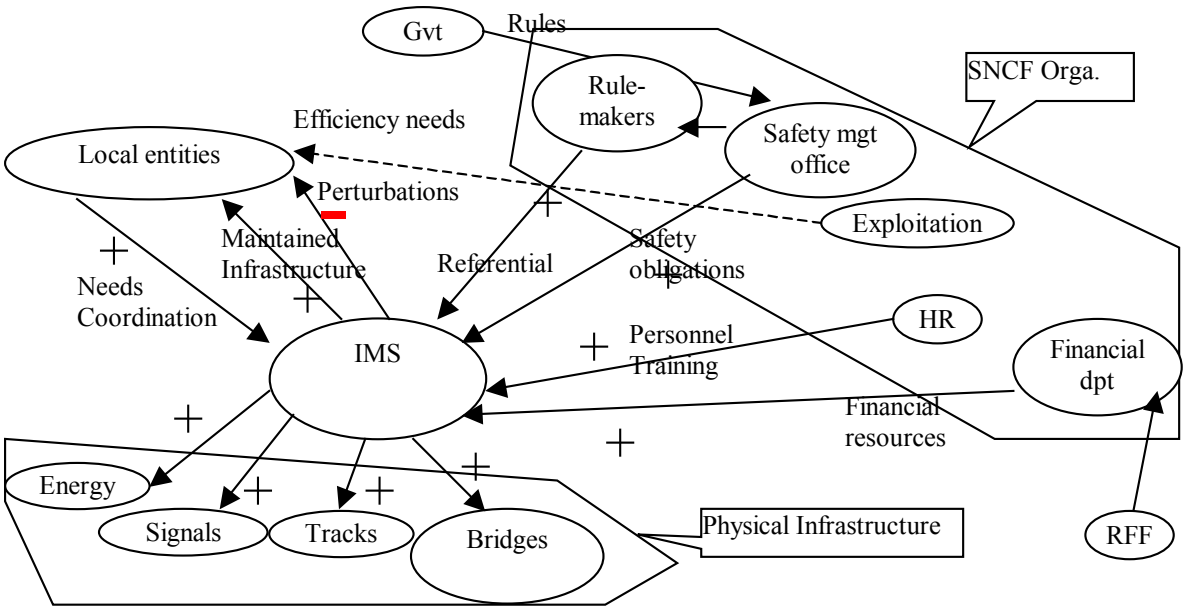
Also note that the element the project can modify the most easily is the referential, as the project initiated from the department in charge of it. Modifications on the other elements will be done indirectly, either thanks to the referential, either through actions of other entities, especially the Human Resources (HR) department.



It is interesting to note that currently, the "realization" activity of the IMS appears as a "black box" in the referential. This is one rationale to precise it in order to increase its performance.



Identify the relations with the environment



The most interesting relationship is probably the one with the local entities (Note: in French "établissements", those are in charge of the management of the tracks and circulations on one geographical section of the railway system). The difference in objectives will generate tensions that are normal and probably beneficial to the reliability of the system. One of the challenges will be to maintain the balance between those elements and to make them cooperate at best.

We are now going to identify more precisely the relations with those local entities as they are concerned in first instance by the project.

<u>IMS → local entities:</u>

+ IMS in good "health"

- Personnel on or near the tracks

- Vehicles on or near the tracks

- Temporary modification of the infrastructure

- Perturbation of the signals and automatisms

- Demand of intervention

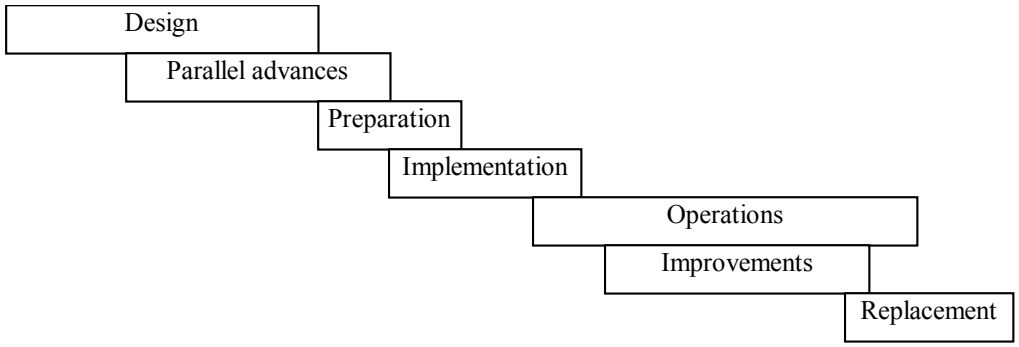
Local entities → IMS:

+ Need of maintenance

+- "time window" depending on the circulation schedule

It is necessary to identify what elements the project can affect – voluntarily or not, and what elements can have an impact on the project. Identifying the major role of the HR department, for example, lead the project team to improve their communication toward this department as well as their cooperation.

Identify mission phases



Design: Design or evolution of the referential, organization, processes and training.

Parallel advances: Progressive modifications on the current system for test and evaluation purposes

Preparation: Communication, beginning of the training sessions

Implementation: Training sessions, replacement of the referential, evolutions in the organization

Operations

Improvements: Evolutions depending on the IMS needs and evolutions in related systems

Replacement: Major evolution in the organization and referential (the successor of STORP ?)

Initial organizational specification

< Remark: This step is quite experimental. There is an experimentation of various theories related to STS, which explains the "chaotic" aspect. Furthermore, some points would require a further study. The main purpose is to demonstrate possible analyses concerning the organization. >

First, we will analyze the organization globally and concerning its main activity. The study of some objectives (especially efficiency and safety) comes next, in order to highlight possible conflicts. It is then necessary not to stop at the intermediary observations but to read until the final conclusions that take into account the various aspects.

"Technological" subsystem: We start by examining the system under the Woodward classification. The technological mode can be considered as unit production: each intervention is quite specific and relatively independent in its execution from other interventions. A low level of organizational complexity it then expected, with a low vertical and horizontal differentiation, broadly defined tasks, and low levels of centralization and formalization.
Furthermore, the IMS must integrate into a broader system, which is more related to mass production, hence with a high level of complexity, formalization and centralization.

We now use the Perrow scheme. Tasks variability in the IMS sub-system is quite important: it concerns various techniques (automatisms, mechanics, electricity, electronics…), represented under the form of various technologies (on the various kind of tracks). However, problems are easily identifiable. It is then an engineering typology, characterized by a low level of centralization, and which requires an important flexibility enabled by a low formalization.

"Personnel" sub-system: We start with the demographical factors. The required level of professionalism is high. Specific and complex technologies are concerned. This implies a low level of formalization.

In terms of demographics, we find an aging population on one side, and on the other side a debuting population to replace them. Those are two aspects to take into account.

The aging population implies a high level of professionalism, and hence a tendency to ask for a lesser formalized and lesser centralized system. The arrival of a young population requires a certain level of formalism to guide them. This formalization must be "pragmatic", as rules that do not seem to be justified (for examples related to older behaviors of the railway system or put in place after an incident that occurred many years ago) will not necessarily be understood and applied.

We must also take into account an evolution in what the employees ask for: better designed jobs, more important participation in decision taking and less formalization.

We now focus on psychosocial factors. Those concern essentially the managers. The current population is experimented, and characterized rather by a "concrete" functioning. Those are rather technical people, who have had training focused on how the elements concretely work. They work better in a mechanist organization characterized by a low vertical differentiation, high centralization and formalization, non-ambiguous structure and processes and few changes.

Given the evolution in training and culture, the new generations have a more abstract functioning, and prefer an organic organization characterized by low level of differentiation, formalization and centralization.

"Environmental" sub-system: We start by covering the five kinds of environments that affect the organizational functioning:

- *socioeconomic*: there is no competition (it may be perceived internally between the SNCF maintenance workers and subcontractors, however the IMS itself has no concurrence). If we adopt a larger viewpoint, the upcoming entry of new companies on the rail freight transportation is likely to add a productivity requirement that may affect the IMS.
- *educational*: the personnel is being renewed at a high rate. To be further studied.
- *political*: current instability, caused by Europe and the possible will of privatization.
- *cultural*: distance taken from the jobs, increasing mobility of the personnel
- *legal*: French and European laws. Controls may be strengthened with the arrival of new actors for freight transportation.

An increase in environmental incertitude must be mentioned. The environment is increasingly changing and complex (Europe, separation of SNCF and RFF, "industrial" logic, new competition, impacts of world economy). However, the IMS remains "protected" by the organization in which it integrates.

Anyway, those aspects plead for a better reactivity and flexibility, and so a more organic organization.

Importance of safety: Note that some of the previous observations were based on the functioning of the system as a "production" system. Safety is the main requirements of the IMS, and the IMS integrates in a high-reliability organization.

Organizational reliability requires a given level of formalization and integration, as well as a clearly defined organization, which is often linked with a high differentiation.

Organization specification: From the previous points, we can identify the following organization characteristics:

- Complexity - differentiation: Given the activity, reduced vertical and horizontal differentiation. For safety purposes, need of a clarification in the roles and of a well-defined organizational structure.
- Complexity – integration: Need of reduced integration mechanisms internally for the very experimented current population, but a high level of integration with the environing organization. Furthermore, with the renewing of the personnel, the experience that enables to face the low level of integration will disappear, hence a need of more developed integration mechanisms. To ensure the safety, need of an "efficient" integration, which minimizes "black boxes" and contradictions.
- Formalization: Low formalization given the activity, but high formalization given the safety requirements. Hence, formalization based on the objectives in terms of productivity and safety – that defines the limits of the acceptable operations – thus enabling a sufficient level of flexibility.
- Centralization: Low for the reasons mentioned previously. Tactical decisions very decentralized, strategic decisions centralized.

Those characteristics are not necessarily the best for the system. However, they are the ones that the system may try to reach. If the designed system opposes those characteristics, there is a good likelihood that the real organization and activities will deviate from the prescribed ones, or that an organizational "misbalance" occurs, noticeable by personnel dissatisfaction.

It is interesting to note a certain opposition between the organizational characteristics related to the operations of the system and those required for safety reasons.

One of the challenges for the IMS is to manage balancing those characteristics, i.e. to enable sufficient flexibility and ability to address the various events, while being sufficiently integrated to

guarantee the safety. It seems essential to have a concise and efficient formalization, which means that it should clearly highlight what is essential – what is required for safety – and this without possible misunderstanding. It should not be complicated with non-essential elements that would reduce flexibility and be in any case violated (with the risk that essential elements, considered as such, are also violated).

Anyway, we can note that the safety phase (which concerns essentially the time-lapse when circulation are stopped and that when they are started again) and the "productivity" phase (realization of safety operations) are differentiated chronologically. It may be interesting to use this aspect.

Identify equivalent systems

Not very applicable here. The main equivalent system is the IMS in its current state. Possibility to take inspiration from railway systems in other countries, or from aviation and nuclear power plants.

Refine the relations with the organization

The IMS integrates into a machine bureaucracy, which furthermore is increasingly productivity-oriented. This probably has an impact on it.

The interest of STORP, and one point on which is should bring improvements, is to generate an optimization of efficiency by integrating safety into the practices, that is satisfying the "productivity " requirement while ensuring the required level of safety.

Define mission scenarios

Here are the main missions expected from the IMS:

- Realize standard maintenance operations
- Realize non-standard maintenance operations
- Maintain itself in operational condition

Define measures of effectiveness

The main measures, as they can be deduced from the objectives and mission, are safety, efficiency and health of the IMS.

The safety measure can be divided into two measures: safety of the exploitation, and safety of the maintenance operations. The safety of the exploitation can itself by divided, as it concerns safety in normal time (which depends on the quality of the IMS) and safety while maintenance operations are performed.

Efficiency concerns various aspects. First there is the customer satisfaction – RFF/"Infra" and "Exploitation" – which requires meting the needs. There is then the efficiency in terms of time and cost.

The health of the IMS is linked to the safety culture, how the personnel and machines are "maintained", and its finances.

Define high-level functions

Direct functions:

Identify the need

Find agreement with exploitation

Prepare the maintenance operations (includes the planning, definition of needs in personnel and skills, procedures)

Move to the site

Interrupt exploitation

Perform operations

Restore exploitation

Evacuate the site

Indirect functions:

Maintain the tools and maintenance trains

Ensure personnel availability and training

Write and maintain referential and procedures

Temporary functions:

It seems important to take into account the functions that will be meaningful when implementing the system:

Implementation of the organization

Implementation of the referential

This early identification of functions helps ensure that no function is forgotten during the latter phases of the project, which was happening in the original project.

Refine organizational specification

The study of the current system (see below) helps analyze better some aspects:

- Formalization: It must indeed be modified. On one side it needs to be adapted to the real work "on the field", be less complicated and more usable. On the other side, concerning the managers, some lacks must be corrected.
- Integration: To improve for the managers.

In fact, the current system is very formalized and integrated at the worker level, and should be redesigned to be more usable. On the other hand, little attention was paid to the managers and the organization, which now require specific attention.

Here are some further thoughts concerning some aspects of the organization.

External influences

There is a strong influence coming from the environing organization, that is the SNCF itself. It is through it that many external influences will go before reaching the IMS.

Goals and strategies

The strategy must reflect clearly an engagement for the 2 objectives of the IMS – productivity and safety – as they are in many points contradictory.

Management functions

As said previously, it is important to improve the integration and formalization at the management level.

A good understanding of the safety responsibilities of managers is also required.

An action of mobilization and follow-up is recommended for the transfer to the new IMS.

Implementing a performance management system is to study, in order to allow manager to be conscious, feel responsible and manage at best the health of the IMS.

Resource allocation

A good balance must be found between productivity and safety objectives. The various objectives must be prioritized so that the essential one always goes first.

Allocating resources to HF activities would enable, in addition to the direct advantages, to insist on the importance of this aspect for the safety and success of the system, and to initiate progressively the members of the system to this way of thinking.

Human resources management

There are requirements in terms of skills, due to the conditions of realization of the tasks: reduced time, importance of the outputs, respect of safety rules.

The impact of the change brought by the new IMS should be evaluated before and after.

Evaluation of the practices, motivations and behaviors and of their evolution.

Training

To redesign and broaden for the managers (especially first-level ones), in order to integrate more significantly safety and systems aspects.

Training sessions to be planned for everyone to ensure a good evolution to the new IMS.

Co-ordination of work

This is an especially important aspect given the requirements (speed, efficiency, safety). This requires a good coordination, especially thanks to a good integration, an efficient analysis of organizational aspects during the project, and then an efficient measurement during the operations (especially of the "mechanisms" that could develop to violate the system).

Improved coordination also required with the subcontractors.

Need of a systemic coordination, both for main and support functions, and at all levels (from a global coordination to interpersonal coordination on the field).

Specific aspect to study: coordination with the exploitation (it does not belong to the IMS and its operating modes cannot be modified by the project).

Organizational knowledge

In order to improve the efficiency, all the personnel must understand well the system and its mechanisms. This will be even more important with the arrival of new personnel (need of knowledge transfer).

The transparency of the system can be a determining factor for its safety.

Proceduralization

Importance of a good balance between formalization and flexibility. Need to take into account the real activity and to integrate the future users (at all levels) in the design of procedures. Importance of a global coherence of the formalization (thanks to the referential).

Think about the level of decentralization of the formalization.

Need for a formalization, which covers the whole spectrum of missions of the IMS (and not 1 mission covered in too much detail while the others are "black boxes").

Organizational culture

Maintain or improve the safety culture at all levels, and ensure it is recognized. The "collectifs" (informal but organized group of worker) must accept and enforce voluntarily the safety requirements.

Organizational learning

Importance of the return on experience (REX), as the referential must be based on the real activity. Enforce the REX, incite employees to report and establish good analysis mechanisms.

Establish exchanges or even benchmarking between the regions / local entities so that the IMS can be more decentralized (one aim of the STORP project and of another project) and efficient.

Communication

Importance of the communication at all levels and with the exploitation, as the planning must be very precise.

For communications involving safety, design some verification and/or redundancy.

Furthermore, at a more systemic scale, communicate on the importance of safety, and on the IMS itself, to enable a good organizational transparency.

Study the current system

This study concerns three aspects: the identification of the prescribed functioning, the understanding of the real functioning, and the evaluation of strengths and weaknesses.

For the identification of the prescribed functioning, refer to page 9 of the document "Integration of HF in STORP". Page 8 of the same document gives information about the real functioning. So does also the report on the S9 survey. This report also analyzes the strengths and weaknesses. (all confidential documents)

The pertinence of the S9 survey must be underlined. Indeed, the interviews "on the field" seem to be an efficient approach to evaluate the real functioning of a system, both concerning the technical, organizational and human aspects.

Here are some important results of the survey:

- The situation is sane at the operator level. The main progress actions must now concern the system and the organization – top-managers, first-level managers and rule-makers.
- The "System referential" does not sufficiently take into account the role of the organization. It is based on outdated concepts and is too complex.
- There is a lack of information concerning the preparation and organization of maintenance operations

We will keep in mind essentially a problem in term of formalization, perceived as repressive and not adapted. An evolution is required. Formalization (especially the referential and the procedures) must be a tool that enables an efficient and safe realization of maintenance operations.

The second main problem relates to the integration. The system in itself is considered as very integrated, with strict and inflexible processes. Such a system can appear as easier to manage "on the paper", however in reality it requires an efficient integration, which is not the case (incoherence between the documents, lack of integration and "fuzzy" processes at the first-manager level).

Study of the risks related to the context

Identify IFS measures

		human accident	environ-mental accident	financial loss	customer loss	loss of know-how	loss of mastery	Destruction of material	Material stolen
Safety	Safety of exploitation normal time								
	Safety of exploitation maintenance								
	Safety of maintenance operations								
Efficiency	Realization								
	Time								
	Cost								
Health	Safety culture								
	Personnel maintained								
	Material maintained								
	Economic health								

Hence, all the measures, at the exception of the respect of the cost and the economic health, are Important for the System and especially Important for Safety. A ranking of importance can be seen in the table below, the most important measures being red.

Here is a preliminary grid of analysis concerning high-level functions, which indicates the level of importance and some barriers (note S9x corresponds to one section of the referential):

		Safety			Efficiency		Health		
		Safety of exploitation normal time	Safety of exploitation during maintenance operations	Safety of maintenance operations	Realization	Time	Safety culture	Personnel maintained	Material maintained
Direct functions	Identify the need								
	Find agreement with the exploitation		- RG S9A						
	Prepare maintenance operations		- S9C	"	"	"			
	Move to the site		- S9B - Itinerary of maintenance trains (S9C) - Planning (S9C)			- Itinerary (S9C)			
	Interrupt exploitation		- S9A	- S9A					
	Perform operations								
	Evacuate the site		- S9B - Itinerary of maintenance trains (S9C) - Planning (S9C) - Verify state of the site						
	Restore exploitation		- S9A						

		Safety			Efficiency		Health		
		Safety of exploitation normal time	Safety of exploitation during maintenance operations	Safety of maintenance operations	Realization	Time	Safety culture	Personnel maintained	Material maintained
Indirect functions	Maintain the tools and maintenance trains								
	Ensure personnel availability and training								
	Write and maintain referential and procedures								
Temp. func.	Implementation of the organization								
	Implementation of the referential								

Identify IFS organizational dimensions

	Safety			**Efficiency**		**Health**		
	Safety of exploitation normal time	**Safety of exploitation during maintenance**	**Safety of maintenance operations**	**Realization**	**Time**	**Safety culture**	**Personnel maintained**	**Material maintained**
External influences		Phys. env. Coordination Finance	"				Social context RH management	
Goals and strategies						Safety motivation		
Management functions								
Resource allocations								
HR Management								
Training								
Coordination								
Organizational knowledge								
Formalization								
Organizational culture								
Organizational learning								

	Safety			Efficiency		Health		
	Safety of exploitation normal time	Safety of exploitation during maintenance	Safety of maintenance operations	Realization	Time	Safety culture	Personnel maintained	Material maintained
Communication								

The most IFS organizational characteristics are formalization, which is the main subject of STORP, coordination / communication, related to the importance of the interaction between the IMS and the exploitation as well as the complexity of interventions (different teams, steps between the expression of the need and its realization), and the training.

Identify IFS incoming relations

	Safety			Efficiency		Health		
	Safety of exploitation normal time	Safety of exploitation during maintenance	Safety of maintenance operations	Realization	Time	Safety culture	Personnel maintained	Material maintained
Rule makers								
Safety mgt office								
Exploitation								
Financial department								
HR								
Local entities								

Identify IFS outgoing relations

The main relations are the one that consist to provide the local entities with a maintained infrastructure, and the one that consists in causing perturbations for those local entities. Both of those relations are clearly IFS.

If we use the more precise previous definition, this corresponds to the following relations for which we will identify some barriers:

+ Maintained infrastructure: Track monitoring, planned operations, capacity of reaction for unplanned operations following an incident

- Personnel on or near the tracks: protection of maintenance operations, special rules (ex: interval)

- Vehicles on or near the tracks: protection of maintenance operations, rules of circulation for maintenance trains

- Temporary modification of the infrastructure: Preparation, protection and know-how

- Perturbation of the signals and automatisms: Preparation and know-how

- Demand of intervention: written or oral "contract"

(remark: the "referential" barrier was not been forgotten, it counts for all those relations and is not repeated)

We can notice here an interesting aspect: the capacity of reaction for unplanned operations. The new IMS indeed relies more on the preparation, this should not reduce this capacity.

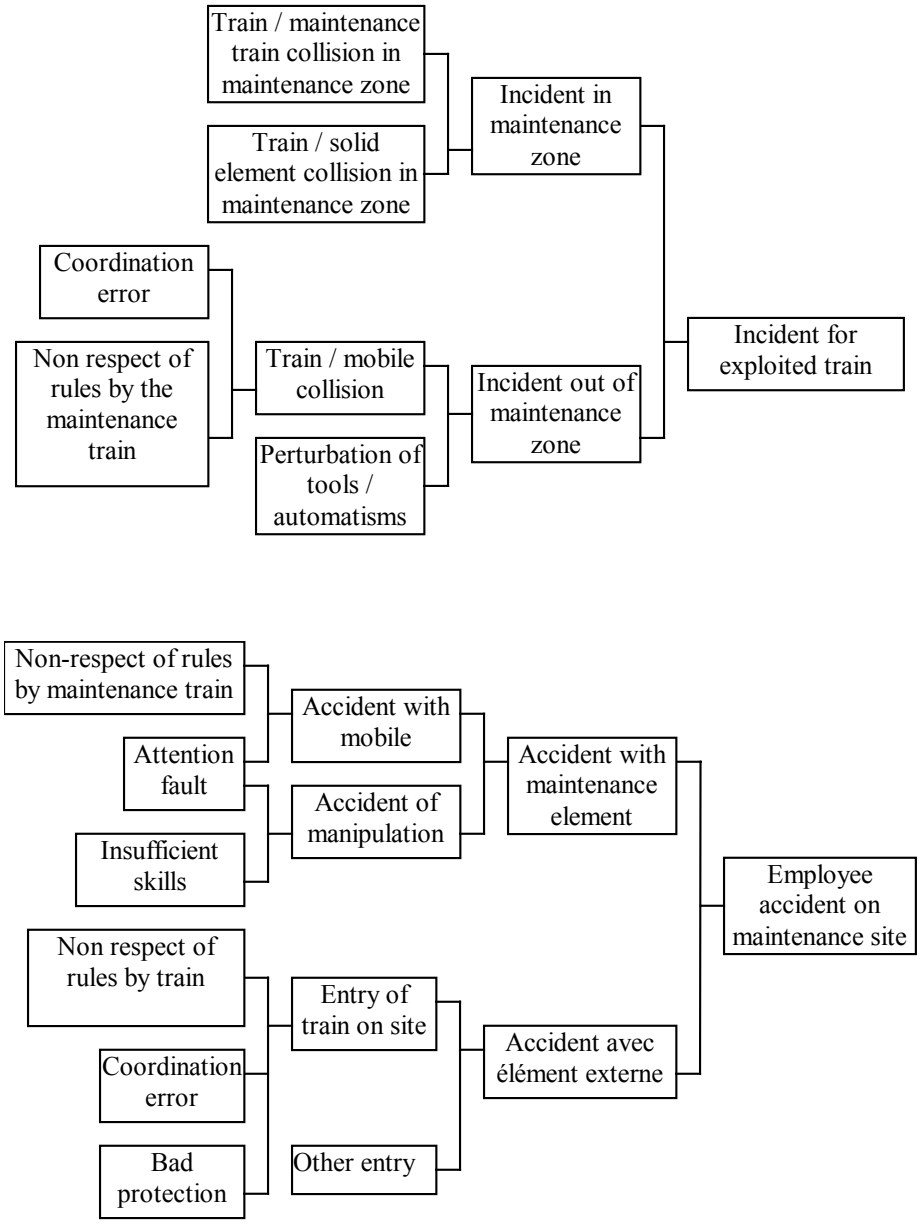
Identify mutual impacts with existing organization

There is a strong opposition against change in the domain of infrastructure maintenance at the SNCF top-management level. This represents on one side risks for the success of the project, but also risks for the future IMS. Indeed, this opposition may destabilize a system that has acquired efficiency and safety partly thanks to implicit rules of functioning.

Identify failure modes

We already know a given number of possible incidents and failure modes. Here are some examples, to detail further in the context of a complete study.

It should be controlled that the new IMS does as good in treating those modes as the current one.



Define IFS requirements

Currently, the majority of barriers are constituted by the referential and its respect. So, the first IFS requirements are the quality of this referential and its capacity to ensure the required level of safety.

The other major barrier is constituted by the employees and their skills, which then need to be maintained and enforced. Preparation of maintenance operations must enable an optimal use of those. In particular, given the various incoming relations and their importance for coordination, unplanned events may occur during the operations, with an impact on safety. It is then required from the system to be able to adapt to these events.

Remarks concerning the HFI focus and working group

We can notice that it was decided at the beginning of the project to integrate in the project team a HF specialist in charge of HF aspects and responsible of interacting with the required HF experts. Specific skill profiles of those experts had also been defined.

As this did not happen correctly, it is the project manager who became the HFI focus, which will be the case in many projects. We can underline the efforts made by this project manager to integrate HF and to train its team on systems approaches and HF integration.

Requirements analysis

Identify required functions

The high level functions identified previously are:

Direct functions:

Fd1: Identify the need

Fd2: Find agreement with exploitation

Fd3: Prepare the maintenance operations

Fd4: Move to the site

Fd5: Interrupt exploitation

Fd6: Perform operations

Fd7: Restore exploitation

Fd8: Evacuate the site

Indirect functions:

Fi1: Maintain the tools and maintenance trains

Fi2: Ensure personnel availability and training

Fi3: Write and maintain referential and procedures

Temporary functions:

Ft1: Implementation of the organization

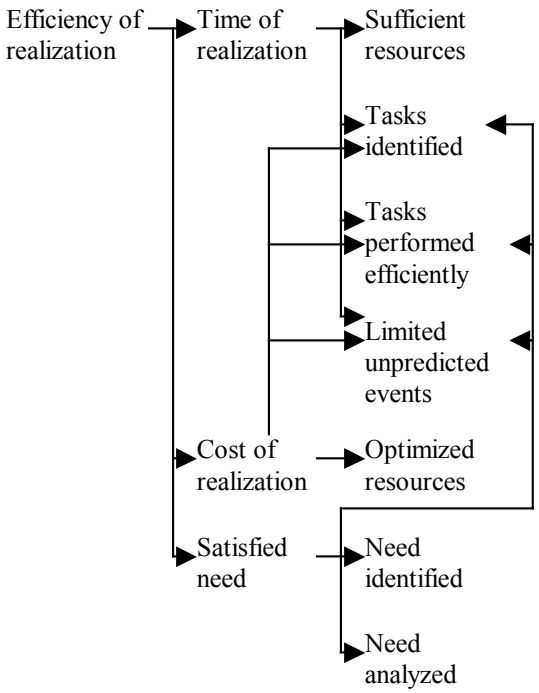
Ft2: Implementation of the referential

STORP will concern more precisely the redaction and maintenance of the referential and procedures, as well as what it inside the "black box", that is the realization of maintenance operations. Hence, we will focus more specifically on functions Fd3, Fd6 and Fi3.

Identify required performance

Global performance

It could be interesting to deduct progressively the requirements starting with the objectives and measures, as shown in the following example showing a "branch" of the "tree" that could be obtained. However, in the present case, we adapt an existing system whose main functions are already defined, and whose functioning we do not want to modify. Hence, it seems more appropriate to start from these functions in order to deduct the requirements as we do next.



Functions performance

Fd1: Identify the need

Respect of a given level of coherence between the real need, the need expressed by the customer and the need understood by the IMS

Fd2: Find agreement with exploitation

Respect of a certain formalization of the agreement

Traceability of the agreement

Required time to conclude the agreement should not be more than a given value

Fd3: Prepare the maintenance operations

Respect of a given ratio preparation time / operations

Respect of a given ratio preparation cost / operations

Allocation of resources in a given interval (sufficient for an acceptable safety and efficiency level, while optimizing the costs).

Coherence between the skills and the operations

Coherence between the material and the operations

Quality of procedures

Fd4: Move to the site

No danger for the personnel

No danger for the exploitation → respecting the circulation rules

Respect of durations

Fd5: Interrupt exploitation

Respect of the planning

Respect of the duration planned for the intervention

Fd6: Perform operations

Realization of tasks corresponding to the needs if no unexpected event makes obstacle

Respect of a given ration realization time / tasks

Respect of a given ratio realization time / task

No unacceptable perturbation on the exploitation

Safety of the personnel

Capacity to adapt to unexpected events

Fd7: Restore exploitation

Respect of the duration planned for the restoration

Restoration at the right time

Fd8: Evacuate the site

No danger for the personnel

No danger for the exploitation → respecting the circulation rules

Respect of durations

Fi1: Maintain the tools and maintenance trains

Material available sufficient to meet the demand

Material meets safety criteria

Material in good state

Fi2: Ensure personnel availability and training

Skilled personnel available sufficient to meet the demand

Personnel capable of realizing the tasks

Personnel guarantees the safety

Fi3: Write and maintain referential and procedures

Respect of the referential

Procedures usable

Procedures enable a given level of safety

Procedures enable the required efficiency

Ft1 & Ft2

Acceptance of the new IMS by a large majority of employees

No major loss of safety caused by the transition

No major loss of performance caused by the transition

One issue faced by the project team was its inability to design a good measurement system. The method helped overcome this obstacle.

Requirements analysis requires a structured approach. It seems appropriate to start classifying those, in order to ensure traceability.

Code	Description
E1	**Identify the need**
E1.1	Respect of a given level of coherence between the real need, the need expressed by the customer and the need understood by the IMS

E2	**Find agreement with exploitation**
E2.1	Respect of a certain formalization of the agreement
E2.2	Traceability of the agreement
E2.3	Required time to conclude the agreement should not be more than a given value
E3	**Prepare the maintenance operations**
E3.1	Respect of a given ratio preparation time / operations
E3.2	Respect of a given ratio preparation cost / operations
E3.3	Allocation of resources in a given interval
E3.4	Coherence between the skills and the operations
E3.5	Coherence between the material and the operations
E3.6	Quality of procedures
E4	**Move to the site**
E4.1	No danger for the personnel
E4.2	No danger for the exploitation → respecting the circulation rules
E4.3	Respect of durations
E5	**Interrupt exploitation**
E5.1	Respect of the planning
E5.2	Respect of the duration planned for the intervention
E6	**Perform operations**
E6.1	Realization of tasks corresponding to the needs if no unexpected event makes obstacle
E6.2	Respect of a given ration realization time / tasks
E6.3	Respect of a given ratio realization time / task
E6.4	No unacceptable perturbation on the exploitation
E6.5	Safety of the personnel
E6.6	Capacity to adapt to unexpected events
E7	**Restore exploitation**

E7.1	Respect of the duration planned for the restoration
E7.2	Restoration at the right time
E8	**Evacuate the site**
E8.1	No danger for the personnel
E8.2	No danger for the exploitation → respecting the circulation rules
E8.3	Respect of durations
E9	**Maintain the tools and maintenance trains**
E9.1	Material available sufficient to meet the demand
E9.2	Material meets safety criteria
E9.3	Material in good state
E10	**Ensure personnel availability and training**
E10.1	Skilled personnel available sufficient to meet the demand
E10.2	Personnel capable of realizing the tasks
E10.3	Personnel guarantees the safety
E11	**Write and maintain referential and procedures**
E11.1	Respect of the referential
E11.2	Procedures usable
E11.3	Procedures enable a given level of safety
E11.4	Procedures enable the required efficiency
E12	**Organization implementation**
E12.1	Acceptance of the new IMS by a large majority of employees
E12.2	No major loss of safety caused by the transition
E12.3	No major loss of performance caused by the transition
E13	**Referential implementation**

Define performance measures

Previously identified measures of effectiveness are refined.

Safety of the exploitation in normal time

- Proportion (number / traffic, eventually number * gravity / traffic) of incidents related to a failure of maintenance operations (failure of operations = operations have been carried out, but have not brought back the infrastructure in an acceptable state)
- Proportion of incidents related to operations not performed timely (demand of intervention made, but maintenance operations not carried out)

Safety of the exploitation during maintenance operations

- Proportion of incidents with mobiles going to and coming from the site
- Proportion of incidents related to the entry of a passenger or freight train into the site

Safety of maintenance operations

- Proportion (number / number of operations (or number of hours spent in operations)) of personnel accidents
- Proportion of incidents on the material (if possible with a cost estimation)
- Safety feeling by the personnel (survey?)

Efficiency of the realization

- Proportion of interventions carried out a second time
- Proportion of interventions that had to be stopped once the personnel was on-site

Time efficiency

- Proportion of interventions starting with a delay

- Proportion of interventions that took too long

Cost efficiency

- Average preparation cost / type of operations
- Average realization cost / type of operations

Safety culture

- Safety culture "grade" (interview / questionnaire)

Personnel maintained

- Number of unexpected events caused by a lack of skills
- Number of accidents caused by a lack of skills

Material maintained

- Proportion of unexpected events caused by a material failure
- Proportion of accidents caused by a material failure

Economic health

- Ratio between the sum given by RFF and the sum spent by the IMS

Define human role strategy

The project shall not require quantitative modifications in personnel. It should not either increase the workload of the workers during maintenance operations.

The project will act on the organization and training. However, it shall not require too many new skills. The organization, if modified, must be quickly accepted and operational.

The part of automation of the system is not supposed to be modified (eventually for the referential maintenance and the preparation?)

Identify the required infrastructure

Human resources management

The operations of the IMS rely largely on HR. Indeed, the manpower must be sufficient and skilled.

HR will be in charge, among others, of the following activities important to the IMS:

- training of the operators and managers
- skill evaluation
- manpower management
- communication to enhance the acceptance of the new IMS
- communication on important messages (efficiency / safety)

Rule-makers

The operations of the IMS depend in a large part on the referential. It is then important that this referential is well organized, coherent and maintained.

Exploitation

The communication with the exploitation must be good.

Identify HFI requirements

We will study the previous requirements and identify related HFI requirements.

O: organization - P: manpower - C: personnel - F: training - S: safety - E: ergonomics

Code	Related system requirements	Description
EO1		More adapted formalization
EO2		More adapted integration
EO3		Referential implemented by HR
EO4		Training organized by HR
EP1		No significant increase in manpower
EP2		No significant diminution in manpower
EC3	E3	Definition of a new skill "preparation"
EC4	E6	Operators capable of performing the required tasks
EC5	E6	Operators capable of using the referential and procedures
EC6	E4, E8	Maintenance train drivers capable of driving on exploited track
EC7	E6	Maintenance train drivers capable of driving on maintenance site
EC8	E4, E6, E8	Maintenance train drivers capable of distinguishing those two modes
EC9	E2, E5, E7	Personnel capable of cooperating efficiently with the exploitation
EC10	E3, E11	Managers capable of writing their own part of the referential and procedures
EC11	E3	Managers capable of preparing maintenance operations
EC12	E3, E11	Managers capable of using the referential
EF1	E4-8, E10	Training of the operators to the new referential / procedures
EF2	E3, E11	Training of the managers to the referential
EF3	E11	Training of the managers to the methods used to create parts of the referential
EF4	E3	Training of the managers to the preparation of maintenance operations
EF5		Training of the managers to any new technique or modification related to STORP
ES1		Improvement in the exploitation safety
ES2	E4-8	Improvement of the IMS personnel safety
EE1	E3	Usability of procedures

Code	Related system requirements	Description
EE2	E11	Usability of the referential
EE3	E6	Reduced workload for workers
EE4	E3, E11	No significant increase in managers workload

Feasibility and compatibility analysis

Acceptance of the project

One interesting requirement (that conditions alone the success of the project) is " Acceptance of the new IMS by a large majority of employees". We can study the related risk (and also the characteristics to be aimed at by the new IMS in order to minimize this risk) by using Rogers' work on the diffusion of innovations:

- Relative advantage: The advantage of the new system when compared to the current one is quite clear, however it is not sure that this advantage is perceived by the users. There is a large communication work to be carried out.
- Complexity: Theoretically the project should not increase significantly the complexity of tasks to perform. However, this requirement should be controlled, especially concerning the new skills required for the preparation function.
- Compatibility: The new IMS should be compatible with the practices of the operators. Concerning the managers, we can wonder if they will accept the new referential and its implications (indeed, the managers will have a much greater responsibility concerning safety, which may displease many – or even be misunderstood).
- Triability: This possibility is in a way given through the parallel advances. However, when putting in place the final system, it will not really be offered.

- Observability: It is important to communicate on the results obtained during the parallel advances, and to ensure that we can quickly evaluate the positive impact of the new system once it is implemented, in order to accelerate and improve its acceptance.

Conflicts between requirements

The success of a project and of the concerned system depends on the coherence between the requirements and its ability to handle the possible conflicts among them.

We can notice that a given number of requirements are in conflict, especially:

- E3.1 and E3.2 with E3.3 to E3.6
- E6.2 and E6.3 with E6.1, E6.4 and E6.5

We find again here the conflict between efficiency and safety. But, further than this one, a more important conflict is the one between the time allocated to the preparation, which must not be too high otherwise the system will become unusable or not be accepted, and the improved efficiency and safety which are consequences of a good, detailed preparation.

The preparation function must be designed so as to handle at best this conflict.

Feasibility

(Remark: The activity of study of the risks related to the requirements is used here.)

Here are synthesized the main observations on the feasibility of the project:

Importance of the support from the HR department: the project designs, but it is the HR department that will communicate, train and control the system, i.e. ensure its life. Consequently, this department must be convinced of the interest of the project and be ready to take part in it.

- Thoughts on the acceptance: the success of the project relies upon its acceptance by future users. This implies that they understand its interest (to change one's uses, which requires an

effort, one must be convinced of the utility to do so), but also that the future IMS is adapted, at the referential level and in some modified functions, and especially in the balance between preparation and realization.

- Thoughts on the balance: We just underlined the importance of handling the balance between preparation and realization. We can also highlight the necessity to balance correctly safety and efficiency. It the new system appears as "over-safety" and degrades efficiency, it will be rejected, and it is not acceptable to reduce safety. Then it is important to see improvements in both domains, and to balance the activities accordingly.
- Necessity of the project: An evolution of the IMS seems necessary. On one side some limits appear already (complexity of the referential, points not or badly covered, insufficient preparation that leads to violations), on the other side some limits can be anticipated (need of a better integration and transparency, need of more adapted procedures and good documentation of the IMS to support the renewing of the personnel, risk of increase in complexity if the functions, referential and organization are not redesigned), and finally there is a possibility to gain in safety and efficiency (especially thanks to a better organization and a better preparation of maintenance operations). An evolution is therefore required, and the action modes chosen by the project seem appropriate. Now they must be well studied, and the objectives and requirements must be kept in focus.

Define human requirements baseline

Human aspects appear under various forms:

- "execution" tasks (realization, maintenance train driving, communication)
- preparation tasks, which can be cognitively complex
- referential writing task
- general documents (referential, job documents)

- locally written documents (definition of maintenance operations, local referential)
- training
- the organization and the transition
- the acceptance

The required HF skills are of various types:

- ergonomics: task analysis, linguistics, estimation of cognitive workload
- estimation of required skills
- training
- organization
- communication on the project

Further than these skills, which require specific profiles, we can underline the importance of a good cooperation with the HR department, as well as the quality of the design required for the various activities and tasks; design activities should involve the cooperation of "technical" members of the project team, HF specialists and future users.

Also keep in mind the previously identified HFI requirements.

Study of the risks related to the requirements

Identify Ifs requirements

Here are the requirements that can be considered as IFS. Of course we use here the work performed on the functions during activity R1.

Code	Safety	Efficiency	Health	IFS?
E1				
E1.1				
E2				
E2.1				
E2.2				
E2.3				
E3				**X**
E3.1				
E3.2				
E3.3				
E3.4				X
E3.5				X
E3.6				X
E4				
E4.1				X
E4.2				X
E4.3				
E5				**X**
E5.1				
E5.2				
E6				
E6.1				
E6.2				
E6.3				
E6.4				X
E6.5				X
E7				**X**
E7.1				

Code	Safety	Efficiency	Health	IFS?
E7.2				
E8				
E8.1				X
E8.2				X
E8.3				
E9				
E9.1				
E9.2				X
E9.3				
E10				
E10.1				
E10.2				
E10.3				X
E11				**X**
E11.1				X
E11.2				X
E11.3				X
E11.4				
E12				
E12.1				
E12.2				X
E12.3				
E13				**X**

Identify risks of non-fulfillment of IFS requirements

Code	Proba	Gravity	Risk	Observations
E3				Skill to modify
E3.4				Already done
E3.5				"
E3.6				New method to prepare procedures
E4.1				
E4.2				
E5				
E6.4				

Code	Proba	Gravity	Risk	Observations
E6.5				
E7				
E8.1				Referential to improve, but until yet no problem
E8.2				
E9.2				"
E10.3				Depends on HR + acceptance of the referential + capacity to use
E11				Modification of the practices
E11.1				
E11.2				
E11.3				
E12.2				

The systems requirements can be translated as the following requirements on the project, given the points on which it will act:

- the designed referential is adapted: The referential, if well used, covers the previous requirements concerning how the new IMS should function.
- the designed referential is accepted: see observations in the feasibility / compatibility step
- the designed referential is well used: this is where HF appear the most clearly. This represents a major risk for the project
- the organization is adapted and accepted: Modifications should not be too important, which reduces the criticity, however the probability is relatively high as this requirements will be allocated to the HR department not directly implied in the project

In all cases, the project must ensure its objectives about safety and efficiency. Otherwise, it may be criticized for "over-safety" and not accepted.

Identify risk of degradation / loss of an IFS requirement

Code	Proba	Gravity	Risk	Observations
E3				Risk of inappropriate use of the newly designed preparation function
E3.4				
E3.5				
E3.6				The procedures, outputs of the preparation, ensure good operations. Hence, this preparation must be performed as well as possible.
E4.1				
E4.2				
E5				
E6.4				
E6.5				
E7				
E8.1				
E8.2				
E9.2				
E10.3				This is an essential barrier
E11				
E11.1				
E11.2				
E11.3				
E12.2				**!!!**

Identify problems in the infrastructure or interfaces

The two main risks are related to the interface with the exploitation and that with the HR department.

Define new IFS requirements and functions

STORP will modify the organization: role of the referential, preparation, use of the referential and procedures during operations (and the balance between those 3 elements), role of the employees,

modification of the structure (DPx (new local managers), new responsibilities on the maintenance sites).

It is necessary to find a good balance in order to progress (and not progress on one point and loose on the other), i.e. ensure that the proposed modifications are beneficial, but also that they will be accepted and implemented. Indeed, given the level of dependence between the various modifications, the failure of one of them is likely to drive the failure of the whole project.

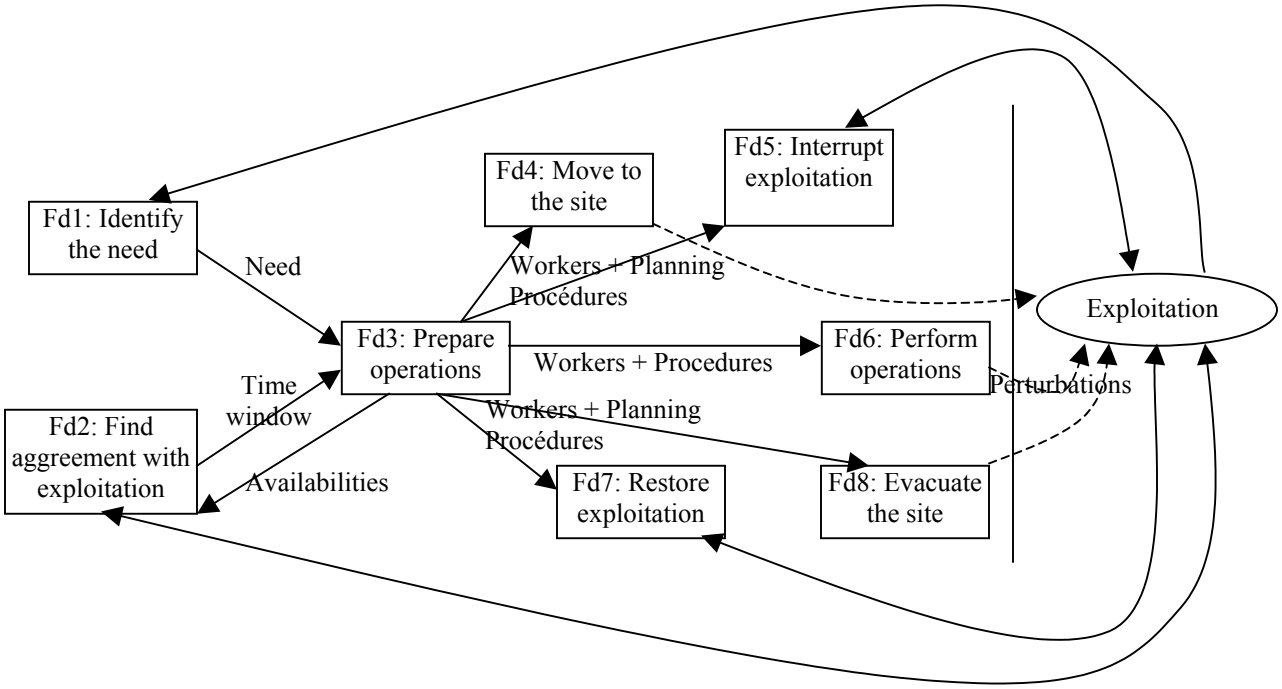
Function analysis

Architecture of functions

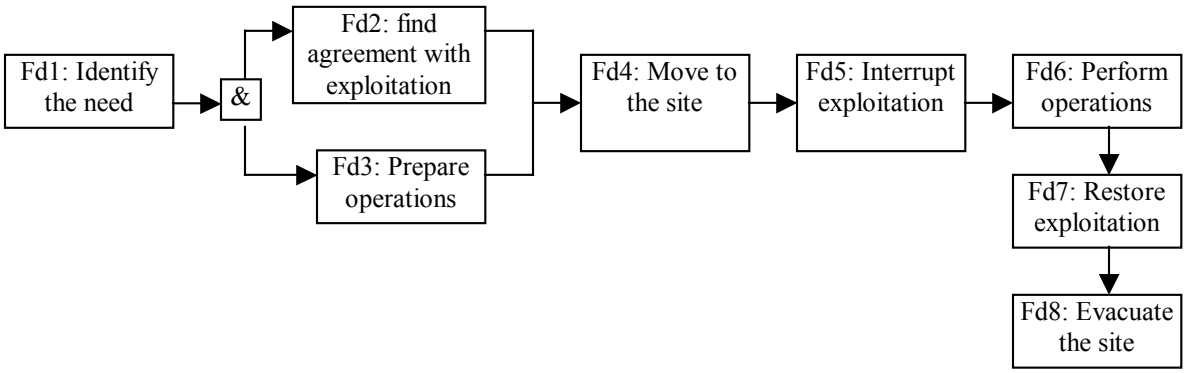
Level 1

From now on we will focus on Fd3 and Fd6. This is why we represent only the Fd here. Of course, for a complete analyze, the Fi and Ft must also be taken into account, especially for risk analyses.

Flows

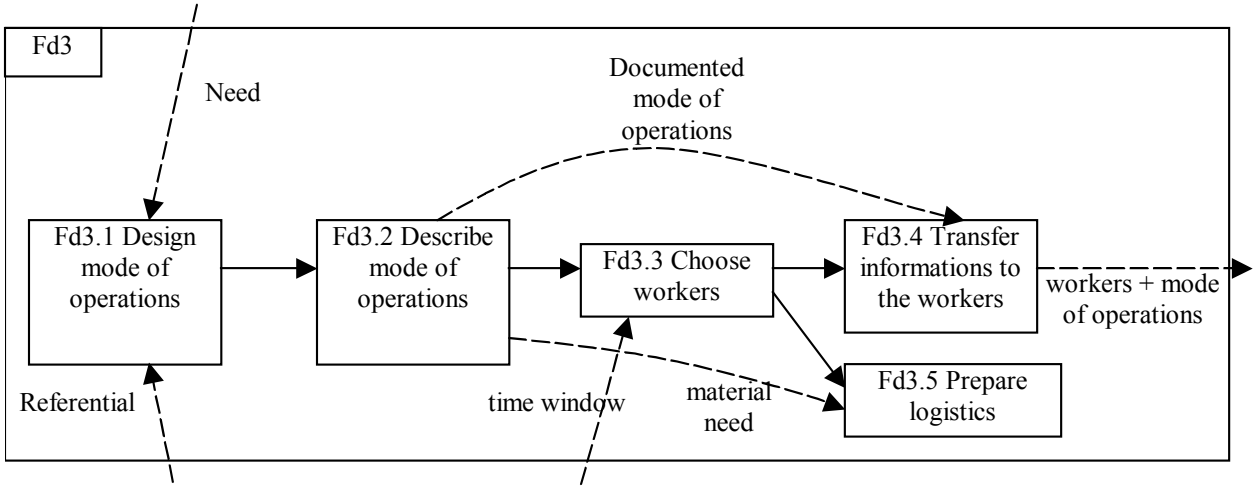


Behavior



Level 2

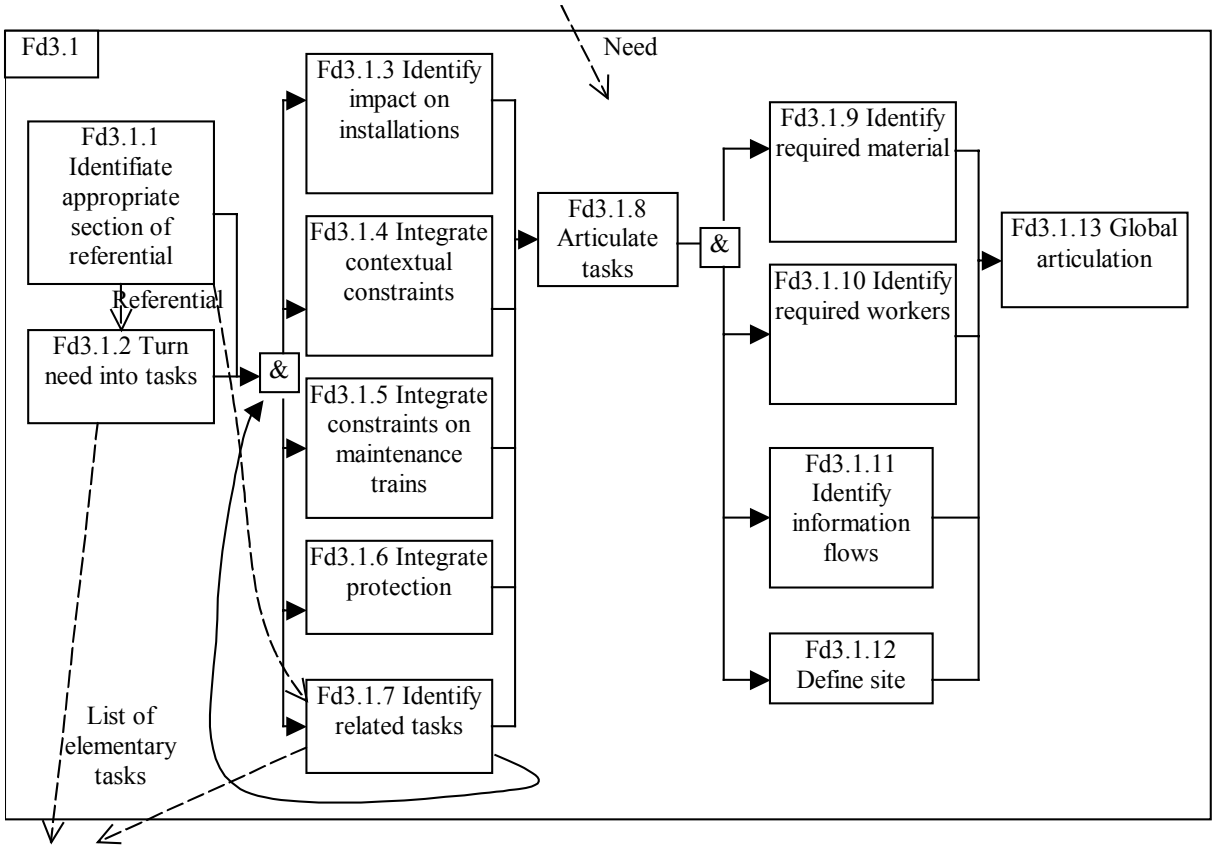
From now on, only Fd3 (prepare the operations, and in fact more specifically the sub-function that aims at defining the operations process) and Fd6 (perform operations). Those functions were chosen because they will be modified significantly by the project.

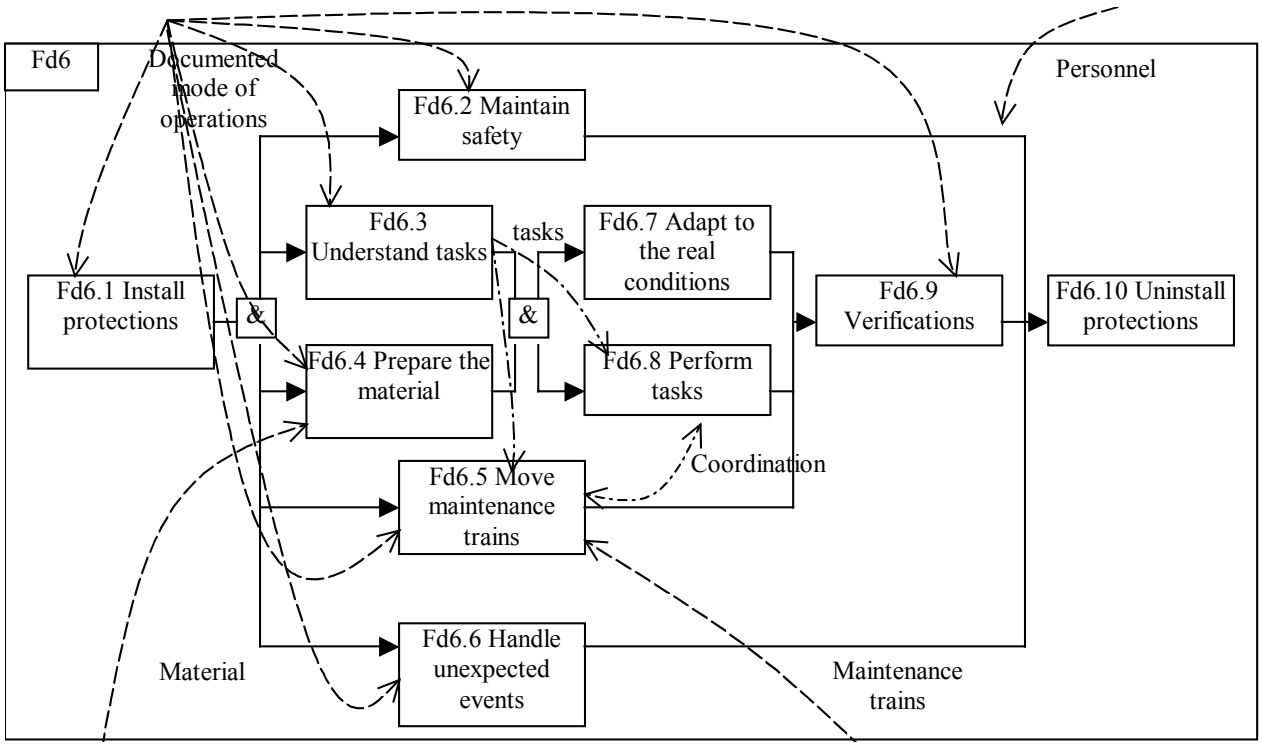


We can notice that this function has similarities with the issues treated by the HFI method (context, task definition, allocation, workload balance). It may be interesting to get inspiration out of the method to design this function.

Requirements met:

Function	Requirement directly concerned
Fd3	E3
Fd3.1	E3.1, E3.2
Fd3.2	E3.6
Fd3.3	E3.3, E3.4
Fd3.4	Indirectly E6.x
Fd3.5	E3.5





We can observe clearly on the flows the importance of Fd3 for Fd6.

Fd6

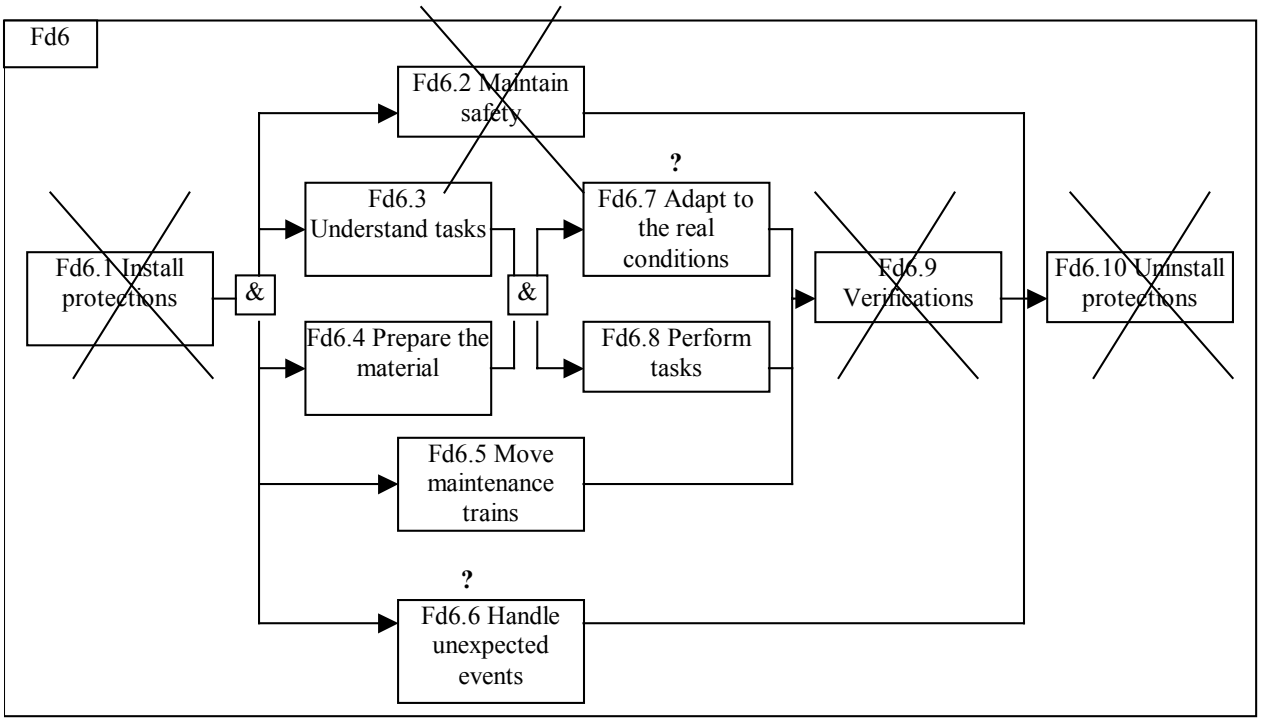
We start by focusing more specifically on Fd6.

Identify IFS functions

Functions related to requirements E6.4 and E6.5 can be seen as IFS. We can consider that all sub-functions Fd6.x meet partially those requirements, with a stronger importance for safety on functions Fd6.1, Fd6.2, Fd6.5, Fd6.6, Fd6.9 et Fd6.10.

Identify alternative behaviors

The main objective (in the sense: objective that seems the most obvious and whose results are most easily observable (in fact, safety shall be the main objective)) of Fd6 is that operations are performed. In order to reach this objective, the following functional architecture is sufficient (for a better understanding, we crossed the functions that do not belong to this minimal architecture, and indicated by a question mark those which only need to be performed partly).



We can also notice that the functions, which are the most likely not to be performed, are Fd6.2 and Fd6.9.

Analyze function failures

Function	Failure	Consequence
Fd6.1	Forgotten protections	To study (use return-on-experience)
	Installation at the wrong place	
	Bad activation of protection	
Fd6.2	Safety actions not performed	
Fd6.3	Tasks not understood	
Fd6.4	Error of manipulation	
Fd6.5	Error of movement in the zone	
	Error of protection crossing	
	Error when moving out of the zone	
Fd6.6	Modification of scenario not identified	
	Bad reaction to unexpected event	
….	….	

concerning Fd6.6: the new system implies a better definition of the mode of operations, input of Fd6. It this better definition may improve safety and efficiency, we may wonder if there is no risk of loss of skill for the workers. Indeed, as they will not be used to handle so many tasks and unexpected events by themselves, it is possible that they lose reactivity in case of an unexpected scenario.

Analyze flow failures

Flow	Failure	Cause	Consequence
Documented mode of operations	Inappropriate documentation	Failure Fd3, Fi3, Ft2	Risk of failure of functions Fd6.1 to Fd6.6, increase of workload for functions Fd6.6 and Fd6.7
	Documentation hard to understand	Failure Fd3, Fi3, Ft2	
Personnel	Insufficient manpower	Failure Fd3, unexpected events on personnel Failure Fi2	
	Inappropriate skills	Failure Fd3, unexpected events on personnel Failure Fi2	
Material	Inappropriate material	Failure Fd3 Material "forgotten" Material unavailable	
	Not maintained	Failure Fi1	
Maintenance trains	Inappropriate trains	Failure Fd3, Fd4, Fi1, other unexpected events	
	Not maintained	Failure Fi1	
Tasks	Failure of Fd6.5 and/or Fd6.8		
Coordination	Incident between personnel and train		
…	…		

We can observe the importance of the other functions, especially Fd3, for this function. The failures of those functions should also be analyzed.

Analyze behavioral failures

The main possible failure is that Fd6.1, 6.2, 6.9 and 6.10 are not carried out.

This can be due to a violation (deliberate choice not to carry them out, for example because of productivity requirements), or an involuntary action (function forgotten, or fault, caused for example by a workload too important for functions Fd6.3, 4, 7 or 8) or even a bad coordination.

We can add further failures: violation of time windows to finish earlier, etc… REX must be analyzed. This could be especially useful for designing Fd3.

Analysis of possible accidents

Inside the zone: Material / personnel, maintenance train / personnel, train / personnel, train / material or mobile.

Outside the zone: Personnel / train, train / maintenance train

See the failure modes identified in R1.

Identify non-prescribed scenarios

We are here in a particular case. Indeed, we must think not on precise maintenance scenarios, but more generally on the operations, as the IMS must cover all possible cases. We consider then as non-prescribed all scenarios that do not follow what was prescribed during Fd3 (the case of a bad preparation is treated later on).

Identify bridges between scenarios

Entering a non-prescribed scenario may be caused by:

- a bad definition of the prescribed, so that workers who want to do the operations have to violate the prescribed
- an unexpected event, which obliges the workers to modify the prescribed scenario

- a voluntary violation of the prescribed, to make the task easier, shorter

Coming back to a prescribed scenario may happen:

- voluntarily, once the non-prescribed task was carried out
- with the intervention of another actor of the IMS or of the exploitation

It is suitable to prepare the maintenance operations so as to enable the easiest and safest possible return to the prescribed scenario.

Identify barriers

In order to prevent from entering dangerous non-prescribed scenarios, some barriers already exist or are planned by the project:

- handling of the unexpected events: a new specific function must be created in Fd3 to ensure that all unexpected event can be treated safely
- rules: there must be an evolution in this barrier, especially to enable a better usability
- safety culture: this barrier contributes to the respect of the rules and to a better handling of unexpected events
- protection mechanisms: the various elements and procedures make a barrier against some unexpected events (train near the zone, maintenance train reaching the limit of the zone for example).

Identify recovery modes

Hazardous scenarios should be quickly identified (by including symptoms and risks in the preparation documents), as well as the way to recover safely (to be done by the "unexpected event handling function").

Fd3

We will now focus on Fd3.

Function	Failure	Consequence
Fd3.1	Mode of operations not adapted to the need	Problem Fd4->7
	Mode of operations does not respect the referential	Problem Fd4->7
	Mode of operations insufficiently analyzed	Problem Fd4->7
Fd3.2	Description cannot be understood	Problem Fd4->7
Fd3.3	Error in the manpower	
	Error in the skills	
	Error in the availabilities	
Fd3.4	Information not transmitted	
	Missing information	
Fd3.5	Logistics insufficiently prepared	

Function	Failure	Consequence
Fd3.1.1	Bad identification of the type of maintenance*	Insufficient mode of operations
	Use of inappropriate section of referential	to be further analyzed
Fd3.1.2	Inappropriate tasks	
	Forgotten tasks	
Fd3.1.3	Important repercussion not identified	
Fd3.1.4		
Fd3.1.5		
Fd3.1.6	Insufficient protection	
	Inappropriate protection	
Fd3.1.7	See Fd3.1.2	
Fd3.1.8	Inappropriate behavior	
	Prescribed behavior can cause a dangerous real behavior	
Fd3.1.9	Inappropriate material	
	Identified material not available	
Fd3.1.10	Inappropriate skills	
	Inappropriate number	
	Allocation can cause dangerous unprescribed scenario	

Fd3.1.11		
Fd3.1.12	Inappropriate zone	
	"Fuzzy" zone	
Fd3.1.13	Bad integration of the previous work	
	Unresolved contradiction	
….	….	

*We can mention the risk that, in order to simplify their task, managers consider "non-standards" operations as the aggregation of simple "standards" operations, which prevents from creating specific documents (the local documents and the referential are sufficient for standard operations).

The project manager underlined the pertinence of this remark as this kind of deviation was already observed.

5.2.2 Design

Given the current state of the project, it is not possible to detail this part – this is actually the aim of the remaining activities of the project. However, it seemed interesting to study prospectively some parts of the project in order to provide eventual advices and observations.

Allocation

We focus on functions Fd3 and Fd6. The allocation is quite fixed. Interesting points concern the modifications of the organization of maintenance zones, as well as the allocation of task identification (between managers in charge of the preparation, and works in charge or realization). This second aspect constitutes a major action mode of the project that will determine quite significantly its success, as it must help improve safety and efficiency. Here we will evaluate the newly proposed allocation when compared to the current one.

Capacities and limits

The project will impact Fd3 and Fd6 about various capacities. Here are some of them:

Fd6:

- Capacity to transform an objective into a realization
- Capacity to handle unexpected events

Fd3:

- Capacity to anticipate
- Capacity to identify the real mode of functioning
- Capacity to produce usable procedures, i.e. sufficiently precise but that allow flexibility

Criteria

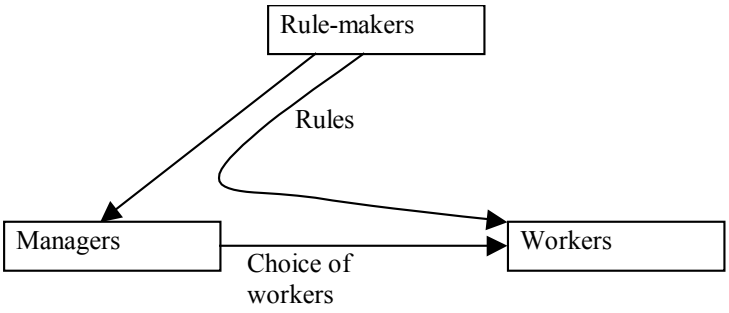
Fd6: Safety, productivity

Fd3: Used resources

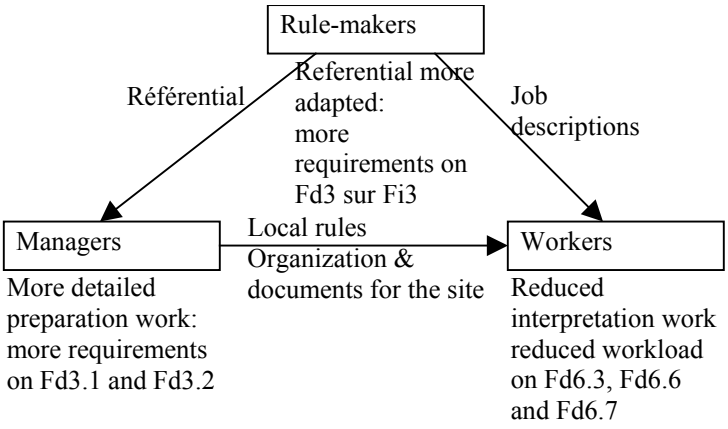
Other: Cost of modifications

Modifications

Current system:



New system:



The main modifications caused by the allocation can be clearly seen here: a reduced cognitive load for the workers, but more requirements for the rule-makers and managers.

The system is acceptable only if those new requirements do not cause a too important workload increase for those 2 job categories, which implies that they must be provided with efficient methods.

Dynamic allocation

We can be confronted to various types of dynamic allocation.

Allocation between the preparation and realization

Some functions of Fd6 cover those of Fd3. Consequently, a less detailed preparation will transfer the task of interpreting the rule and objectives to Fd6.

This allocation is completely dependant on the managers, as the workers can only cope with the documents they have once on the site.

A reallocation at the detriment of workers is not suitable; indeed it would bring the system back to the current state (but with different rules, which are maybe less adapted to this mode of functioning). This would displease the workers. Hence, it shall be ensured that managers handle their preparation role correctly.

On-site allocation

This constitutes an aspect to study for the preparation method. Indeed, it is possible that the agents are tempted (or obliged) to reallocate on site.

The unexpected events handling function can also take dynamic allocation into consideration in order to help workers choose the best allocation.

Sociotechnical aptitude

Theoretically, the new system shall result in an increase of all major functions.

However, there are some limits:

- it is not sure that the new system will not generate an increase in workload, and so a decrease in efficiency, at the manager level. This could even make managers more "administrative" and distant from the field.
- the project may have an impact on the safety culture, which is particularly important. Indeed, until yet, workers were considered as responsible of safety. Now, the role and responsibility of the managers will be underlined. We must avoid that the agents feel freed from their responsibility ("this is not our fault if operations are not efficient or unsafe, they probably were badly prepared" kind of behavior).

A more detailed analysis requires knowledge about the exact tasks involved in the preparation activity.

Here are the main strengths of the new organization:

- work on site better organized, easier to perform and manage

- strengthen manager's involvement
- better links between managers and workers (as the operations must be prepared based on the real practices)

The possible weaknesses relate to:

- large dependency on the HR department for the transition
- importance to be quickly operational and efficient in order to avoid a massive reject
- risk that a good balance may be hard to find in the preparation activity, which may either lead to time wastes (and discouragement) or to a return to the current system

5.2.3 Detailed design

As the system is more integrated, it is necessary to have a good organizational functioning and efficient interfaces between the managers and the agents (as well as between the agents, and with the exploitation of course).

Organizational design

The main structural modifications will concern the modifications planned at the site level, with the introduction of a site supervisor and of a local sites manager.

More important modifications will affect the flows. The flows with the rule-makers, as well as between the managers and the workers will be modified in their contents.

The integration requires an appropriate training. Managers must be trained to the new preparation methods and to the new referential.

The organization can evolve either by returning to the current system, or moving towards a better-organized and integrated system, where operations preparation is recognized truly as a skill.

The performance measures must be controlled in order to detect quickly a weakness in the new system or a deviance from its initial objectives. It is necessary to think how to make those measures operational.

In terms of organizational rule, it is necessary to support the preparation activity by developing and encouraging the skills and providing enough time to perform this activity correctly.

Tasks design

An essential task is the preparation. Are also to be designed the tasks corresponding to the new jobs (site supervisor and local sites manager), and to the modified activities.

Interface design

Interfaces for the site supervisor and sites manager are essential. They must be well designed.

The interfaces around the managers in charge of preparation are multiple and also important (interface with the exploitation for planning, with the HR department for the choice of agents, and especially with the agents themselves. Think especially on the form and content of the transmitted documents).

5.2.4 Implementation and operations

Ensure that a good support is provided, globally and locally, to ensure that the design is integrated as efficiently as possible.

Given the incertitude on the acceptance and possible consequences of the project, it is really important to establish an efficient measurement system. This system must be very detailed at the beginning to help identify quickly any deviance. Then, it can be lightened, but must remain regular,

in order to estimate the outcomes of the project and prevent unwanted deviances and "perverse" effects.

5.3 Formative Evaluation

This section discusses the value the evaluation brought to the method, that is the observations that can be made after using it in terms of advantages and disadvantages, as well as the points it helped improve.

5.3.1 General observations

Advantages

The following are the main advantages that appeared when testing the method. Those advantages are related to the use of the method, and not the results it generates, this latest point being discussed in 5.4.

The first noticeable point, which is mostly related to the SE base of the method, is that it is structured, which necessitates us to:

- identify and trace the characteristics of the system concerned and the context of the project
- identify and trace the goals of the project
- trace the needs and constraints

Those aspects contribute significantly to the project quality. From this observation we can assume that the method, when introduced in the SNCF, will generate better results than simply integrating HF.

Then, the human and organizational aspects are covered "naturally" thanks to the method. This means that simply applying the different steps of the method without making efforts to focus on HF is sufficient for addressing the various human and organizational aspects. This is important as the method is meant for non-HF specialists and intended to guide throughout the project in order to cover all important HF aspects.

Similarly, the method ensures that some important questions are addressed, like: "what if the system does not behave as we thought? What if employees do not follow procedures?". More generally, it ensures that important safety aspects will not be missed, even by people with little background in RAMS and risk management.

Disadvantages

Some disadvantages also appeared when using the method. The main one is that it may be "bothersome" for users accustomed to "unstructured" projects – that is, projects that lack structured problem thinking and solving as well as traceability, which appears to be the case in the company.

Then, the method may be avoided given the number of steps. Although good projects usually go beyond these steps, the first contact with the method may be difficult for some project managers. This raised the need for practical examples in the training provided to the users in order to reassure them.

Another possible problem is that the method requires a specific way of thinking. First of all, people not accustomed to SE may try to find the solution before going through the context and requirements analysis. Then, as it relies on SE, the method is more efficient if used with models, which is not guaranteed to be accepted given previous problems faced by the STORP project.

5.3.2 Improvements

The evaluation led to concrete improvements and also highlighted some areas for further research.

Actual improvements

Risk activities were modified to include more clearly the deductive analyses. Indeed, in the first version, the focus was placed on identifying causes in the system and identifying barriers. The improvements made to activities R1 to R5 now require a building a safety architecture by performing both inductive and deductive analyses. If this seems obvious to risk specialists, it may not be to some users.

In order to help the users, thanks to the better understanding brought by the evaluation, illustrations were inserted in the documentation of the method. This may help clarify the meaning of some tasks, as well as provide a starting point in terms of models or tables that can be used.

It also appeared that the method had fallen into a common "trap". Indeed, it felt as if it was meant for developing systems from scratch, whereas in many cases – especially in the SNCF – it will be used to make systems evolve. Hence, the method was enhanced, especially by adding task 1.1.13. This raised the possibility of further improvements in this domain, discussed later.

The evaluation also confirmed the need of guiding users on identifying the points of the method of major interest for their specific project. This need was also raised by the stakeholders. The evaluation helped design the "guide of use" described in 4.7.

Area for further improvement

The notion of change could be better integrated in the method. Indeed, the method will often be used on existing systems, and changes imply some specific HF aspects, as well as safety issues.

Those are partially addressed in the current method, through an appropriate identification of the existing system during the study of the context, and then the propagation of these elements with the requirements. However, new tasks could be added to address more precisely aspects like: HF issues in tasks modified by the project (or changes in technology used for example), acceptance of the changes, impact of organizational change, etc.

Another area of improvement concerns the quantification. However, it may be useful to expand on this aspect, especially by using methods taken from the disciplines of decision aiding and operations research.

5.4 Comparative evaluation

Once the application of the method was completed to the extent described previously, the results were presented to the interlocutors. After the presentation of these results, a semi-guided interview was conducted. The structured part of this interview consisted in discussing the various important points identified to ensure their pertinence, and obtaining a more general opinion on the application of the method. Much freedom was given to the interlocutors to express their thoughts. The results of this inquiry are first explained. The consequences of the application of the method on the project are then discussed, followed by a summary of the interlocutors feedback about the method.

5.4.1 Important points identified

The application of the method identified many different points. Some of these points appeared as very important for the project, by crossing the method application and the interlocutors feedback (as explained in the Methodology chapter).

This section first presents two points previously identified in the project that the application of the method highlighted and underscored. These points, although they had been identified at the beginning of the project, were not taken into account sufficiently, thus endangering the project and the future system.

The first point concerns the size and complexity of the project. The project is intended to reach several objectives through various interrelated modes of action as identified in *5.2.1 - Study of the context*. The application identified (*5.2.1 - Requirements analysis*) that the failure of one or more of these modes of action could endanger the project itself as well as the safety of the IMS, which was a major problem given that many action-modes relied on relations with other entities and human acceptance. This point was confirmed, as well as its importance, with the conclusion that a failure of one mode of action would mean the failure of the project, as underlined in *5.2.1 - Study of the risks related to the requirements.* As the project manager stated, "If one mode of action of STORP fails, this will mean the failure of the whole project. We (the project team) have a bad tendency to forget this".

Another point highlighted by the application of the method is the importance of the relationship with the Human Resources (HR) department. Indeed, the project will result in referential procedures, documents for training and "theoretical" changes in the organization, however those need to be put in application by the HR department, which will be responsible for the communication, training and establishment of the new organization and procedures. Hence, the opposition of some members of the HR departments to the project represents an important threat for it success. In this case the contextual study (*5.2.1 - Study of the context*) proved its usefulness. This point was underlined by the initiators of this research.

The application of the method also focused attention to new points that had not been identified, or not studied with sufficient detail.

The starting point concerns the new balance between preparation and realization. In the current system, preparation let much flexibility and also required a large capacity of adaptation and improvisation from the agents in charge of the realization. It is to be replaced by a system with much more precise preparation and a strict realization, where the respect of rules and preparation documents will be enforced. This points refer to *5.2.1 - Study of the functional risks* and *5.2.2 - Allocation.*

The first points are about the new characteristics of the realization: strict rules, no improvisation. The application of the method raised many questions concerning the work of the realization agents:

- Loss of skills: currently, agents gather a good knowledge of the railway system when they "improvise". With the new system, they are likely to loose those skills. The questions is: will they not require those skills when a situation not identified during the preparation phase occurs?
- Acceptance by the realization agents: agents were used to a certain degree of freedom, which allowed them in some cases to finish their work earlier or make it easier. There is a risk of non-acceptance of the new IMS.

The second series of points deals with the preparation, which needs to be more precise. The following questions require to be solved by the project:

- Risk of a "bad" preparation: as realization agents are asked to follow the instructions precisely, badly prepared instructions could lead to major problems (whereas in the current system they were simply "absorbed" by the flexibility of the agents). This raised the importance of designing the new preparation function so that it addresses abnormal situations correctly –, which in itself may be quite complicated. Among the various causes identified, some proved very likely thanks to the return on experience, like managers considering that a

large maintenance work is just an aggregation of smaller ones, and so preparing it without considering the whole system and interactions.

- Need for a well-designed preparation function: Preparation is not easy, as it requires taking into account many different aspects, plus HF and abnormal scenarios. It is not obvious to decide the right amount of detail, and many important aspects may be forgotten – especially as many employees are now retiring and being replaced by new ones with little experience of the railway systems. Furthermore, the application of the method identified that an increase in preparation may reduce the capacity of reaction for unplanned operations (after an incident). This is not acceptable, so this constitutes another requirement for this function. Hence, much attention shall be allocated to the design of the preparation function and the associated training.
- Acceptance: Some consequences of the new system may not be accepted easily, restricting the overall acceptance of the project. First, managers will be clearly considered as responsible. As they do all the preparation, if an incident happens and the realization agents have followed the instructions, it is the manager who will be held responsible. This is likely to raise many voices against the project. Then, preparing more precisely implies more work.

The application of the method even helped identify a deviance in the current system. Indeed, it raised the fact that more preparation implies a heavier workload. Actually, the new preparation function should imply better preparation rather than more preparation. So no problem in theory. However, in practice, it appears that many managers, whose role is to prepare the maintenance work (and this is their only official role), do something completely different, as preparation is not done, or not done properly. This is clearly a deviance. The project manager, a former IMS manager, had missed this aspect as he had himself been used to this deviance.

This deviance has safety consequences for the current IMS system – and may be one major reason for the need of evolution and the STORP project. It also has quite a strange consequence on the project: the new preparation function may not be accepted because it asks the managers to do … what they are supposed to – what was originally their only role now constitutes a threat to them carrying out the other tasks (task still to be identified).

5.4.2 Main results of the application for the project

The method helped identify various points. The project manager and the project supervisor agreed on the need to address those points, and a few actions were decided on order to reorient the project, which are presented here.

As a consequence of the previous points, the application of the method underlined the need for en improved and modified communication (*5.2.1 - Requirements analysis - Feasibility and compatibility analysis*). Indeed, many disadvantages can be seen by the future users of the new IMS, and the rationale for some choices may not be clear. Hence, it is mandatory to explain why this change will be beneficial, and how the new safety architecture will be built, so that every employee is aware of the role he plays and understands the implications of the changes. The three following actions were decided:

- Organize communication actions towards the HR and methods departments
- Involve some people of the HR department in the project team
- Improve the balance between the project team and the HR and methods departments. Indeed, in order for the project to remain accepted, the project team had a tendency to make modifications that were strongly suggested by the other departments. These modifications sometimes modified vital elements for the project. The objective is to identify the IFS elements and not accept to modify them on one side, and on the other

side to build a relationship based on cooperation rather than on influence and "political manipulation" (characteristic of the organization, see 3.3.1).

The importance of the preparation function was also underlined thanks to the method. Furthermore, it added some requirements to this function:

- need of addressing correctly the unexpected situations
- need of a proper design that helps managers not to fall in two pitfalls: the one related to the appropriate level of detail, and the other one related to missing importance aspects.
- need to rectify the current deviance
- need of acceptance
- need in terms of results produced

The decision was taken to develop much more precisely and differently the preparation function, and test it thoroughly. A second action that was decided was to study the deviance observed in the current system in order to avoid it happening again in the new system.

Concerning the operations, the project manager agreed on the importance of two aspects:

- need for a good accompaniment, to ensure the acceptance and successful implementation of the new IMS and avoid immediate variances that could be very harmful.
- need for a measurement system, to ensure that the new IMS functions "as it should", to verify some assumptions made during the project, and verify that the new IMS indeed reaches the objectives

5.4.3 Feedback from the company

Once the results of application of the method had been discussed with the interlocutors, they were asked for a more general opinion on the method itself.

The first response was a regret that the method could not be applied from the beginning of the project, as it would have highlighted many useful things. However, for someone who starts a project, it really seems to be a useful method given the very pertinent results it generates.

Then, another positive aspect is that it has the "look & feel" of a method. In other words, it is face valid. It is well documented, clear in the process to follow, and so deserves to be qualified as a "method". As the project manager stated: "This [the method] really feels like a complete methodology. It is certainly a more serious investments than previous so-called methods we have been confronted to". The initiators of the research also said: "We were far to expect something as detailed and usable as this. This is not some conceptual approach but a usable and interesting method."

Another interesting point is that it generates "rational" results. Unlike some direct HF-experts input, it does not reflect someone's opinion or belief about human work and humans and provide directly usable data, as the project manager expressed: "Usually, HF specialists bring us results which are far from our concerns or too subjective. The outputs of the application are objective and will be of great use for the project".

It seems very efficient given the context of the evaluation and the results obtained, as the project supervisor underlined: "I am really surprised that in such a short time, and with your little knowledge of railway systems, you were able to provide such appropriate and useful results".

The project is uncommon, so the method can be considered as very adaptable in that it can be applied on such a project, as it appears through this statement of the project manager: "This method has helped someone with little experience deal with a subject as complex and specific as our project. I really believe it can be applied to most project successfully".

Furthermore, the initiators of the research and the project managers estimated that this method would be a good help for their HF specialists.

On the other hand, the method is quite generic and the documentation may be "frightening" at first sight, so that it is necessary to teach and accompany users in their first use of the method, as the project manager expressed: "this is a generic method, and as such it has many steps. this could be demoralizing for many people. […] People need to be accompanied, at least on their first projects". The idea of including a guide of use to help focus on some points for the project is pertinent.

5.5 Conclusion

Applying the method to a concrete case was a worthy experience. Indeed, it helped identify some components to be modified or developed further in the method. Some further points will be discussed in Chapter 6. It also enabled to gain a more "practical experience". This led to better explanations in the documentation of the method, and the potential for better training. One interesting point is that it raised the need for support in the application of the method, as will be discussed in Chapter 6.

Globally, it justifies the implementation of such a method in the company – and its possible interest for other companies dealing with HF, safety and projects – both from the results it generated and the feedback obtained.

Chapter 6 - Discussion

The purpose of this chapter is to analyze further the research results. First, the initial questions and hypotheses are discussed. Then, the main conclusions of the research are highlighted. Various observations are then made on the results. Finally, the perspectives of this research are discussed as well as the various limitations it had to face.

6.1 Discussion of the questions and hypotheses

6.1.1 Question 1 – Integration of human and organizational aspects

Question 1: How can design and risk assessment integrate human and organizational aspects?

Hypothesis 1.1: Human factors integration in design and risk assessment can be achieved by coordinating and integrating together macroergonomics, microergonomics, organizational risk models and human reliability methods.

The developed method shows that it is possible to integrate human and organizational aspects in projects, and especially in design and risk assessment activities. While being based on a common approach to project and design and "usual" approaches to risk management, the method addresses the main aspects related to human and organizational aspects. Hence, it demonstrates that without a huge shift in practices, this integration can be achieved.

Hypothesis 1.1 can be considered as true; the integration was achieved thanks to a method that coordinates and integrates together microergonomics – thanks to the very good basis provided by HFI, macroergonomics, organizational risk models and human reliability methods.

However, such an integration, if the method had not gone further than this, would probably have been limited. Indeed, it can be believed that the efficiency of the method relies also on two other elements:

- its inheritance from SE: integrating human and organizational aspects probably gains much from the systems approach. Indeed, it helps to cover the various aspects and address the various needs in a structured manner – and hence can be used efficiently even by people with limited background in HF, whereas previous methods like the one used in-house (Direction des Ressources Humaines, 1997) required a good background in HF.
- the high-level approach: Simply integrating existing methods and models would have resulted in a "closed" approach, dependent on the chosen models. Integrating the various important aspects without restricting to some models makes the approach open – it is a framework on which various methods can be applied – and suitable for future evolutions.

6.1.2 Question 2 – Efficiency of the method

Question 2: Can an organization- and human-centered design methodology of safe complex systems be used efficiently?

Hypothesis 2.1: A sociotechnical project framework will enable the design of safe systems.

Hypothesis 2.2: A sociotechnical project framework will enable the design of efficient systems.

The proposed method was tested on a single case; hence it would not be appropriate to generalize too much without further research. With respect to the case , interesting results were generated as described in chapter 5, which implies that it can be used efficiently at least on certain types of projects.

The method is based on approaches that had been previously tested. SE now benefits from a wide appreciation, and HFI proved its efficiency on various large military projects and generated important savings (Angus et al., 1998). As our method extends HFI – adding activities does not restrict the efficiency of the existing ones; it does at least as good and as such can be considered as efficient.

Given the nature of the case studied and some thoughts on the content of the methods, our particular method can be considered as especially adapted for projects involving organizational design or change in a context where safety matters.

Both hypotheses were partly addressed in Chapter 5. On the evaluation project, the method helped highlight new elements to enable a safer and more efficient redesign.

More generally, here are some additional thoughts on such a method. Given it helps to better identify HF-related issues and include more efficiently safety concerns, the method may generate gains both in terms of efficiency and safety in projects where HF and risk/safety skills are low. Even for projects with a high level of expertise in HF and safety, adopting a structured and systems approach may generate some improved results. However, further research is required to confirm that there are improvements in this later case and eventually quantify them.

The main cause of possible negative findings related to the hypothesis relies in the complexity of the method. If a project starts using the method and does not benefit from proper support, the project team could get lost and focus too much on understanding the method rather than on the project and target system.

If adequate support is provided, it can be assumed that both hypotheses are true. More research is required to draw conclusive findings on this point – the HIFA approach is also currently undergoing this phase of test.

6.1.3 Question 3 – Acceptance of the method

Question 3: Can an organization- and human-centered design methodology of safe complex systems be accepted by an interdisciplinary project team?

Hypothesis 3.1: Engineers will agree on the advantages of a sociotechnical project framework.

Hypothesis 3.2: Project managers will agree on the advantages of a sociotechnical project framework.

Hypothesis 3.3: Human factors specialists will agree on the advantages of a sociotechnical project framework.

As for the previous question, the absence of statistics on a large sample prevents generalization. However, from the various potential users met during the research, many expressed their interest and need for such a method. It is relevant to discuss this question in terms of Rogers' perceived attributes of innovation (1995):

- Relative advantage: Given the current practices in many companies the method presents many advantages. It introduces human and organizational aspects, but also systemic thinking and safety design "philosophy". The most obvious results may already generate important gains:
    - better feasibility studies that enable the identification of failure-prone projects
    - a better analysis of project consequences, reducing the number of failures
    - an optimization and reduction of required resources
    - a pertinent description of designed systems, which enables more efficient training and management

  The case study used for formative evaluation of the method supported its usefulness.

- Compatibility: The method does not require a big shift in practice, as it allows the choice of models and tools. However, it implies the adoption of a systemic approach as well as a more structured behavior in projects, and to be convinced of the importance of human aspects, which may not be accepted easily for some populations.
- Complexity: The method is meant to be used by non-specialists. It may at first sight seem complex, but a short training program based on examples should help overcome this first impression. Thus, future implementation should focus on training and communication.
- Trialability: The evaluation demonstrates that the method can be applied on any kind of project involving human aspects, so that it can easily be experimented with on a small project before being applied to bigger ones if project managers wish.
- Observability: The evaluation helped make first results observable. It may not be obvious to demonstrate that a given project was a success because the method was used on it, however successful cases can easily be advertised and enhance the acceptance of the method.

Most contacts were with project managers and engineers (project managers are mainly engineers in the company). Feedbacks from those populations were very good, whatever their contact to the method was (simple presentation, detailed analysis of the method, method tested on their project).

Concerning the third hypothesis, this remains a question to be studied. HF specialists should be the first to encourage such a method, however they might not accept a method different from the ones they use traditionally (even if this is a framework that allows them to use the methods they want). Through discussion with the STORP project manager, it appeared that some ergonomists tend to focus on the "operator on the field" and are reticent to analysis of managerial jobs or more global approaches.

6.2 Contributions of the research

This section covers the contributions of this research, first by considering its modalities, and then by synthesizing its value to the company and for the more general Research Community.

6.2.1 Introduction: The context of applied research

One interest of this research is that it generates both general and applied results. While being based on general approaches, and resulting in a general method, it it was evaluated using a concrete application in a company, which enabled the testing of the method It also shows how applied research can be efficiently used in a company, even in the domain of HF where there is sometimes a gap between research findings and company practices. From an initial broad problem – taking into account HF more efficiently in risk analyses, a first analysis was performed to identify a possible action lever, in this case project management. Then existing approaches were identified and reused, resulting in quality outputs, and further developments.

6.2.2 Outputs and outcomes for industrial users

The method addresses the initial needs expressed by the test company, and solves it with the following advantages:

- healthy base: SE and HFI have been tested and have proven their efficiency. Hence, the method benefits from this experience, both in terms of quality and acceptance.
- adapted for users of various level in HF and safety: Unskilled persons will find the method useful for identifying HF and systemic issues in their projects, while the more experimented can benefit from a structured approach to exploit their skills at best.

- possibility of evolution: As it is a high-level framework, and not a method limited to one single model of human behavior or one tool, it can benefit of advances in HF and safety research. Being based on HFI, it can also benefit from the findings of projects like Manning Affordability or Hifa.
- Integrated systems approach: It goes beyond the initial need expressed by proposing an integrated systems approach, which may generate larger gains.

The second output is the application on the STORP project, which is likely to benefit from the various observations made.

In terms of outcomes, HFI already generated major savings in the Army, and it can be anticipated that such gains can also be achieved in the SNCF. Furthermore, it is not only efficiency and economic gains that are concerned, but also safety – and the whole image of the company, as well as social atmosphere. However, the application performed on the STORP project does not enable to provide measures of these benefits currently, those should be obtained through further experimentation and research.

6.2.3 Outputs and outcomes for the research

This research meets to a certain extent two directions proposed by Strain and Preece (1999). The first direction was the integration of HFI and risk management, for which this method proposes a solution.

The second one was the possibility of using HFI in a civil company. This research begins this avenue, and furthermore shows through the evaluation on a project that HFI can be used on civil

projects – and also on projects involving no technical design and/or purchase, as was the case in the Army projects.

Furthermore, it helps to extend HFI by proposing a solution to a more systemic integration of organizational aspects.

Finally, it helps to develop the emerging discipline of HFI and publicize it.

6.3 Observations

The research highlighted some interesting aspects, which are discussed here: first, the interest of using existing approaches, then observations on SE and finally a discussion on the ability of this method to help improve the cooperation between technical and HF specialists.

6.3.1 Interest of using existing approaches

The proposed method is not an entirely new one as previously discussed. It is an advancement of HFI approaches. Some observations can be made about this:

- Many methods and tools already exist concerning HF and human reliability. If this quantity demonstrates the quality work and interest of researchers, one might wonder if it does not reduce the applicability of HF in companies. Indeed, users may feel lost with all of these methods, based on various models. Companies prefer to have one or a few working methods easily identifiable and recognized. Establishing some sort of common reusable base with HFI may help improve the acceptance of HF in companies.
- Companies are often much more reluctant to invest in HF than in technical matters – this is especially true in France where human sciences tend not to be highly regarded. However, developing a method and testing it requires time and resources. Hence, focusing on improving a framework like HFI as well as the tools specific to the various activities can help

enhance the applicability and acceptability of such researches. Developing the researched method from scratch would have taken much more time, for a result that would have never been tested before, and hence of reduced acceptability.

- Reusability and evolution are important. Knowledge in HF evolves, as well as methods do. Discarding the current methods and practices is not an easy task in a company, and may disqualify the discipline itself. An approach based on HFI will benefit from findings in similar projects, and help the method evolve and improve.
- However, to a certain extent, using HFI limits the structure of the base behind the method. Indeed, keeping a very clear idea of the way the method is built is important, but requires that some time is spent understanding the existing approaches and keeping "big directions in the method". Simply adding activities to cover the whole spectrum of HF aspects may result in a n unusable method (this is what essentially happened with some HF guidelines).

6.3.2 Beyond HFI: Systems Engineering

The first intention of this research concerned Human Factors. However, it seems clear that SE had a big impact on the quality of the method produced. Requirements engineering alone helps to keep a project on track and identify the various aspects required. If the HF-related part of the method helps to focus on some aspects, the general structure ensures coherence in the project, which is essential when dealing with aspects as complex as human and organizational aspects.

SE is still an emerging practice in France, and tends to be limited to big technological projects, especially ones that involve software. However, the evaluation of the method on the STORP project proves that it can be of great use for purely organizational projects.

HFI was not specifically conceived for SE. It is mainly the Manning Affordability project, which proposes this mixed approach. The Hifa and UK HFI approaches for instance adopt a much

more "traditional" project management cycle. However, during the evaluation, it appeared that a SE based approach helped analyze and understand the system and ways of action much more efficiently, and it certainly enabled good results in the railways context where the researcher lacked experience.

6.3.3 Cooperation between engineers and HF specialists

Upon discussion with the STORP project manager, it appears that cooperation between engineers and ergonomists represents an issue for good sociotechnical design. A situation that seems to occur frequently is that few exchanges happen between both, so that both parties lack information and provide the other with valuable input.

Use of the method during the evaluation phase helped highlight a few points that would require input from an HF specialist. More generally, it can be assumed that using the method may improve the cooperation and override the limitations related to the current practices – put an ergonomist on the project and let him operate. Here are some of the observations that can be made concerning this point:

- the method, thanks to the systems and structured approach, allows a much better understanding of HF issues even for someone not expert in the subject matter. The evaluation was able to show this. As one main problem relies in the fact that ergonomists in the company are not railway experts, the method can improve their participation in projects.
- the method helps to create efficient interfaces between engineers and HF specialists. Indeed, it shows the engineers what input they could expect from HF specialists, and helps them to identify the points on which they need such input. It gives them a common basis for dialogue.
- the method helps to understand the spectrum of HF skills. Currently, project managers tend to forget that there are other people dealing with HF than ergonomists, whose input may be more appropriate, for example sociologists when organization or global consequences of a

project are concerned. As the method underscores the skills required for the various activities, and will be supported by a training supporting this aspect, cooperation may also be enhanced this way.

6.4 Prospects

This section discusses the perspectives after this research both for the company and for the Research.

6.4.1 Prospects for the company

The research consisted of developing a method and evaluating it. It is now the role of the SNCF to ensure its support and appropriate use.

Initial implementation

Distributing the documentation to the future users is insufficient to ensure a good acceptation and efficient use of the method. It is necessary to plan an adapted training and support. The training shall encompass:

- an introduction to the main aspects of HF
- an introduction to SE
- a presentation of the main principles of the method
- a more detailed presentation of the method
- an introduction to interesting methods and tools
- a sample case to test the method

It is recommended to provide the users with a support, at least on their first project. The idea it to make someone available, who is more confident with the method, in order to advise and help them. This may prevent them from being "apprehensive" of the method or disappointed by an inappropriate use of it.

Further support

Some support may be required for an optimal use of the method. Here are some possible modalities:

- return on experience: by gathering and analyzing users' feedback, improvements could be made to the method, its documentation and the associated training.
- benchmarking: putting in common the positive results of application of the method could create a databank of examples. Those examples might be used to:
    - help new users understand the method
    - inspire users who work on projects with similar points to previous projects
    - identify innovative applications to help the method improve
    - identify successes to communicate on the interest of the method and improve its rate of acceptance
- databank of methods and tools: the method proposes a framework. It is then necessary to choose the right methods in order to perform the various activities. Some databases were created in the HIFA and Manning Affordability projects. It would be interesting to provide users with a basic bank inspired from those, which they could then fill up with new methods or tools they discover or create for their projects.

The interest is also to create a "movement" around HF. Users should understand and get interested in the discipline and the method and get able to make improvements, as they did for more "technical" domains.

6.4.2 Prospects for the research

The results of this research may be used for further research.

Transfer to other sectors

This study constitutes one of the first attempts to apply HFI to a non-military domain and to non-specific projects. The method can be generalized through some minor adaptations; hence it can be transferred to other sectors. It would be interesting to study to what extend such a method is transferable and of interest for the sectors concerned.

Validation

The research enabled an evaluation of the method. However, given the limitations faced, this should be considered as a partial validation. A whole validation would imply an application of the whole method on a larger number of projects (and of course users) and the analysis of those applications.

Points to be studied concern:

- the acceptance: to what extent is the method accepted in a company, and how to improve this acceptance for eventual transfers in other companies
- efficiency: how efficient is the application of the method, and what is the quality of the results obtained

- return-on-investment: what is the cost of introducing HFI in a company (including adaptation of the method, communication, training, support) and what are the gains of such an introduction.

Constructing a common referential

There exist various HFI methods, all inspired by the same objectives and a common source, but which all present their own advantages and specificities. It would be interesting to propose a common referential using the best aspects of all those methods.

Systems Engineering and Human Factors

It appears that one strength of the method resides in its relationship to SE. Reciprocally, SE gains from a good integration of human and organizational factors. It may be interesting to pursue this to see how one discipline can gain from the other. The latest conference of the International Council on Systems Engineering (INCOSE 2002) demonstrates the relevance of this topic. Indeed, a review of paper titles indicates this trend: "Organization Safety: A systems Engineering Perspective", "Systems Engineering Approach for Modeling and organizational Structure", "Analysis of Human Factors in Specific Aspects of Systems Design". There is still work to make SE a true "total-systems" approach with the appropriate methods and tools.

Evolution of the method

The researched method brings improvements to the HFI approach. However, there is still room for further improvement. The integration of change as well as quantification was previously discussed in 5.3.2 – concerning quantification there is a need for ways to optimize the sociotechnical system.

Links between organizational design activities and other activities could also be strengthened, to define what organizational characteristic relates to which lower-level activities.

The complexity of the method could also be reduced. Indeed, the current evaluation gives a general opinion on the whole method. However, currently, there is little information available about the value of the various parts of the method. One interesting prospect would be to separate the method into pieces and study how valuable and applicable each of these pieces are. As presented in 5.4.3 and discussed in 6.1.3, the main obstacle to the acceptance is the complexity of the method, as industrial users often lack the required time for complex approaches. By focusing on the most valuable parts of the method, it should be possible to reduce its complexity, and improve its acceptance.

Other aspects to be studied

Some questions could be studied following this research:

- HFI focus: who is most suitable to become responsible of HFI activities in a project? A HF specialist, an internal consultant, the project manager, a project quality manager?
- where does the efficiency of the method really come from? HF, use of SE, the new concepts included, the background it helps to acquire?

6.5 Limitations

This research faced some limitations that should be kept in mind when studying the results:

- the input – in terms of ideas and feedback – comes from employees of the same "national" company
- the method was tested on a single project, and not on all aspects of the project nor on the whole project life

Chapter 7 - Conclusion

The focus of this research was to develop a project management framework that integrated efficiently human factors and risk management activities, and could be applied in a company. It showed that such a method can be developed and actually generates interesting results when applied to a project.

7.1 Recommendations

Several pitfalls must be overcome in order to conduct research of this kind.

The first obstacle lies in the cooperation with a company. This certainly represents a great opportunity to evaluate research hypotheses in their real context. On the other hand, it requires a good planning as well as flexibility, because the employees have their own schedules, and their projects are subject to delays, or cancellations. One must also be able to convince people to spend time on a research project, at a time where you have little information to give about the achievable results.

The second obstacle lies in the multidisciplinary dimension of this research. Indeed, it is at the meeting point between HF, project management, risk management and SE. As such, it is necessary to be able to acquire quickly an overall view of the disciplines, identify what the best starting point may be, and select carefully the sources of inspiration.

The third obstacle relates to the subject of the research, which is broad and conceptual. It is easy to get lost by trying to fit all the existing methods, extend them, synthesize them in a research project. To avoid this, it is very important to define clearly the objectives, the requirements and the methodology, and then constantly keep this focus and check regularly that you head in the right direction.

7.2 Synthesis

This research underlines the interest of adopting a sociotechnical approach to the design of ultra-safe systems. It demonstrates that Systems Engineering can be used efficiently on projects involving organizational design and safety concerns, as it helps to address the complexity of such projects and concerned systems and provides a structured approach for studying those systems. It also highlights the pertinence of the emerging approach of Human Factors (or Human Systems) Integration, which can easily be borrowed from its initial military context to be applied to much more general projects in a civil context.

Then, this research shows that HFI in its current form can still be extended to improve the success of projects and designed systems. In the context of ultra-safe systems where organizational reliability plays a major role, it is appropriate to add and enforce a new "organization" domain. HFI in itself is already adept at addressing some organizational aspects, but extending it helps to adopt a more systemic view on the organization and to better integrate organizational aspects. Then, such contexts require risk management activities to be integrated into project management practices. In ultra-safe systems, safety is largely related to the human and the way they are organized. This research proposes a solution to integrate successfully risk management activities with HFI, while underlining important notions and proposing specific activities to enable an efficient embedding of safety mechanisms in the designs or redesigns. It also highlights that the aspect of HFI dealing with the composition and organization of the project team to support HFI is essential, and asked for by users. Finally, it demonstrates that HFI is a living approach that can still be improved, for example on activities like function allocation, and would benefit from such further improvements.

This research also identified that implementing an HFI approach in a company also requires a systemic approach and especially a good analysis on the adequate support. HFI presents the quality

of being simple enough to be widely spread and of driving a good use of HF and safety skills in the company. However, users ask for a good documentation that allows them to start quickly using HFI on a project. This implies that this documentation guides them from the beginning for their specific project, and helps them to identify the appropriate skills required. HFI implementation also requires training and accompaniment of course. But it could also benefit from an architecture to make it live and evolve, through return on experience, benchmarking, tools and methods databases and user-driven improvements.

This research showed that such an approach helps to solve many issues related to the integration of HF and safety concerns in projects. Indeed, it is likely to improve the cooperation between technical and HF specialists. It helps to "demystify" HF, and shows how to take them into account "rationally", while ensuring that no important aspect is missed. It also integrates some important notions in the practices, leading to the design of better systems. More globally, it shows users how important HF is for their projects, and that a systemic approach can help them manage more successful projects.

Finally, it opens the door for further research. The method itself can still be improved, to better integrate the notion of change. It can also be analyzed in order to identify the most valuable parts, and reduce the complexity, which represents the major default of the method. Thinking quantification throughout the method, especially concerning RAMS matter may also improve the method. Of course, many activities would gain from new methods, tools and approaches. Finally, the domain of the infrastructure adapted to enhance the efficiency of HFI in a company, evoked in this research, remains to be further studied.

Methods like HFI – and the researched method – can be very beneficial in terms of improved efficiency, improved safety and more successful projects. In the same way as HF, risk management and SE gained popularity during the last decades, it can be anticipated that HFI will further develop, thus opening the doors of true total systems approaches.

Bibliography

AFAV (1997). Qualité en conception : La rencontre Besoin - Produit - Ressources. AFNOR

AFNOR (1994). X50-415: Ingéniérie intégrée.

AFNOR (1994). X50-420: Soutien logistique integré.

Amalberti, R. (1996). La conduite des systèmes à risques. PUF

Amalberti, R. (1998). Les facteurs humains à l'aube de l'an 2000. Phoebus, numéro spécial Le Facteur Humain

Amalberti, R. (2001). The paradoxes of almost totally safe transportation systems. Safety Science 37 109-126

Angus, R., Beevis, D., Magee, L., Jacobs, I., Landolt, J., Wakefield, D., Foster, K. and Vallerand A.L. (1998). Way Ahead & Investment Strategy for Human Factors Modeling & Simulation R&D in DND. Defence R&D branch.

Bahr, N. J. (1997). System Safety Engineering and Risk Assessment: A Practical Approach. Taylor & Francis

Bourrier, M. (2001). La fiabilité est une question d'organisation. in Bourrier M., Organiser la fiabilité, L'Harmattan

Buck, J. R. (1999). Ergonomic Design. Unpub.

Cole, E.L. JR. (1998). Functional Analysis: A System conceptual Design Tool. IEEE Transactions on Aerospace and Electronic Systems 34-2, 354-365

Colin, R. and Vaxevanoglou, X. (1994). L'adaptation de l'ergonomie de conception aux réalités du travail industriel. Actes du XXIXème Congrès de la Société d'Ergonomie de Langue Française, 2, 38-44

Cook, C. and Corbridge, C. (2000). Function Allocation: Optimising the Automation Boundary. Crown / DERA.

Dearden, A., Harrison, M. and Wright, P. (2000). Allocation of Functions: Scenarios, Context and the Economics of Effort. Int. J. Human-Computer Studies, 52, 289-318

Deschanels, J.L. (2001). Initiation to the cindynics. Course at the Ecoles des Mines de Nantes.

DGA (1994). Guide pour la prise en compte du facteur humain et de l'ergonomie dans les programmes d'armement. DGA / AQ / FHE 913

Didelot, A. (2001). Contribution à l'identification et au contrôle des risques dans le processus de conception. Thèse, Institut Polytechnique de Lorrain.

Direction des Ressources Humains (1997). Démarche sociotechnique : "Comment prendre en compte les facteurs humains dans les projets ?".

Direction des Ressources Humains (2000). RG-0022: Le management de projet. Référentiel général SNCF

Earthy, J.V., Bowler, Y., Forster, M., Taylor, R. (1999). A Human Factors Integration Capability Maturity Model. Proceedings of "People in Control: An Internationl Conference on Human Interfaces in Control Roooms, Cockpits and Command Centres: 21-23 June 1999", Conference Publication N.463, IEE.

Embrey, D. E. (1992). Incorporating management and organisational factors into probabilistic safety assessment. Reliability Engineering and System Safety 38 199-201

European Organisation for the Safety of Air Navigation (2000 a). Human factors integration in future ATM systems : Identification of tasks and design scenarios.

European Organisation for the Safety of Air Navigation (2000 b). Human factors integration in future ATM systems : Methods and Tools.

European Organisation for the Safety of Air Navigation (2000 c). Human factors integration in future ATM systems : design concepts and philosophies.

Fadier, E. (1998). L'intégration des facteurs humains à la conception, travaux actuels et perspectives. Phoebus, numéro special, 59-66

Fadier, E. and Mazeau, M. (1998). Les facteurs humains de la SDF. Actes de la conference Lambda-Mu 11

Forrester, J. W. (2001). System dynamics and the lessons of 35 years. In De Greene K. B. , The systemic basis of policy making in the 1990s.

Garrigou, A., Daniellou, F, Carballeda, G., Ruaud, S. (1995). Activity Analysis in participatory design and analysis of participatory design activity. International Journal of Industrial Ergonomics 15, 315-327

Garrigou A., Thibault J-F., Jackson M. and Mascia F. (2001). Contributions et démarche de l'ergonomie dans les processus de conception. Pistes 3-2

Gerard, M. (2001). Etude sur les écarts entre prescriptions et pratiques quotidiennes des agents de maintenance de la voie ferrée. Rapport de stage SNCF

Greenley M. (2000). Canadian Department of National Defence Human Systems Integration Capability : Concept Description. DRD Canada

Hamann R.J. (1999). Systems Engineering: A structured way to satisfy internal & external customer needs, lecture at the Ecoles des Mines de Nantes, Fokker Space.

Helander, M. G. (1999). Seven common reasons to not implement ergonomics. International Journal of Industrial Ergonomics 25, 97-101

Hendrick, H. W. (1996). Good ergonomics is good economics. HFES

Hendrick, H. W and Kleiner, B. M. (2001). Macroergonomics: An introduction to work system design. HFES, Santa Monica, CA

Hollnagel, E. (1996). Reliability analysis and operator modeling. Reliability Engineering and System Safety 52, 327-337

Hutchins, E. (1995). Organizing work by adaptation. Organisation science 2-1

ISdF (1996). Rôle positif de l'homme dans la fiabilité des systèmes. Projet ISdF 7/95

ISO (1997). ISO 10006: Lignes directrices pour la qualité en management de projets.

Jalashgar, A. (1999). Goal-oriented systems modeling: justification of the approach and overview of the methods. Reliability Engineering and System Safety 64, 271-278

Jampi, D., Guilhem, E. and Aubry, J.-F. (2001). Conception et sûreté de fonctionnement: Deux acitivités indissociables. Actes de la 3ème conference Francophone de Modélisation et SIMulation MOSIM01

Jensen, L. (2002). Human factors and ergonomics in the planning of production. International Journal of Industrial Ergonomics 29, 121-131

Johnson, P., Harrison, M. and Wright P. (2001). An evaluation of two function allocation methods, Crown / DERA

Jourdan, M. and Bellies, L. (1996). De l'analyse du travail à l'intervention ergonomique : l'expérience d'une collaboration à la conception d'un Système Automatisé de Production. in L'ergonomie face aux changements technologiques et organisationnels du tr avail humain, Octarès

Le-Coze, J.C., Vince, A.S., Salvi, O., Prats, F. and Plot, E. (2002). Development of the ATOS concept, analysis of technical and organizational safety. Proceedings of the lambda-mu 13/Esrel 2002 conference

Kirchsteiger, C. (2002). Workshop summary evaluation and how to proceed. International workshop on promotion of technical harmonization on risk-based decision-making. Safety Science 40, 383-395

Kirwan, B. (2000). Soft systems, hard lessons. Applied ergonomics 31, 663-678

Kusiak, A. and Zakarian, A. (1996). Risk assessment of process models. Computers & industrial Engineering 30, 599-610

La Porte, T. (2001). Fiabilité et légitimité soutenable. in Bourrier M., Organiser la fiabilité, L'Harmattan

Lagrange, V. and Fanchini, H. (1996). Intégration de l'ergonomie dans une méthode de spécification: le cas du développement d'un outil expert en fiabilité. Actes du congrès ERGO.IA', Biarritz

Lapeyrière, S. and Massip, C. (1994). De l'importance des demandes et des contextes pour la définition des modalités d'une sensibilisation des ingénieurs informaticiens au volet homme-travail-organisation. Actes du XXIXème Congrès de la Société d'Ergonomie de Langue Française

Laprie, J-C. (1985). Sûreté de fonctionnement des systèmes informatiques et tolérance aux fautes: concepts de base. TSI 4, 419-429

Lewkowitch-Orlandi, A. and Carballeda, G. (1996). Impact de la coopération entre ergonomes et spécialistes en management sur la conception d'une organisation. in L'ergonomie face aux changements technologiques et organisationnels du travail humain, 1996

Majchrzak, A, Borys, B. (2001). Generating testable socio-technical systems theory. J. Eng. Tehcnol. Manage. 18, 219-240

Modarres, M. and Cheon S.W. (1999). Function-centered modeling of engineering systems using the goal tree-success tree technique and functional primitives. Reliability Engineering and System Safety 64, 181-200

Naël, M., Poulain, G. and Damay, J. (1994). La contractualisation des interventions ergonomiques dans les projets de conception. Actes du XXIXème Congrès de la Société d'Ergonomie de Langue Française, 2, 130-137

NEA (1999) Identification and assessment of organisational factors related to the safety of NPPs : State of the art report.

Neboit M., Fadier E. and Poyet C. (1993). Analyse systémique et analyse ergonomique. Application conjointe à la reconception d'une cellule robotisée d'usinage. Rapport INRS 1993

Nikolopoulo, H. (1998). Dynamiques d'intégration et légitimité de l'ergonomie dans les projects de conception. Actes des Journées Recherche et Ergonomie, Toulouse, février 1998

NMA - Naval Manning Agency (2000). The UK MoD Human Factors Integration Programme. Presentation at TTCP - HUM 9, Toronto 5-9 June 2000

Øien K. (2001). A framework for the establishment of organizational risk indicators. Reliability Engineering and System Safety 74, 147-167

Older, M., Clegg, C. and Waterson, P. (1996). Report on the revised method of function allocation and its preliminary evaluation. Institute of Work Psychology, University of Sheffied.

Paté-Cornell, E., Murphy, D. M. (1996). Human and management factors in probabilistic risk analysis: the SAM approach and observations from recent applications. Reliability Engineering and System Safety 53, 115-126

Paté-Cornell E. (1997). Ranking and priorities in risk management: Human and organizational factors in system failure risk analysis and a maritime illustration. MIT workshop on Organizational Processes in High-Hazard Industries, May 1997

Perrow, C. (1984). Normal accidents, Living with High-Risks Technologies. Basic Books, New York, NJ

Pocock, S., Harrison, M., Wright, P. and Johnson, P (2001). THEA: A Technique for Human Error Assessment Early in Design. Proceedings Interact'01, Japan.

Pomian, J-L., Pradère, T. and Gaillard, I. (1997). Ingéniérie & Ergonomie. Cépaduès-Editions, Toulouse

Rasmussen, J. (1997). Risk management in a dynamic society: a modelling problem. Safety science 27, 183-213

Reason, J. (1990). Human Error. Cambridge University Press

Richei, A., Hauptmanns, U. and Unger, H. (2001). The human error rate assessment and optimizing system HEROS – a new procedure for evaluating and optimizing the man-machine interface in PSA. Reliability Engineering and System Safety 72, 153-164

Rogers, E.M (1995). Diffusion of Innovation, 4th Ed. New York: Free Press

Sagot, J.C., Roberty, ML., Benchekroun, M., Garret, D., Chappet, P. and Raimond, C. (1994). Intervention ergonomique dans la conception du poste de conduite du TGV nouvelle generation. Actes du XXIXème Congrès de la Société d'Ergonomie de Langue Française, 2, 12-20

Sagot, J-C., Gouin, V. and Gomes, S. (2000). Ergonomie et conception centrée sur l'homme : exemple de l'étude de la conception du poste de conduite du TGV Nouvelle Génération. Actes de la journée Ergonomie et Facteurs humains dans le transport ferroviaire

SC-21 S&T Manning Affordability Initiative (1998). Human Engineering Process. DD21/ONR

Skepper, N., Straker, L. and Pollock, C. (2000). A case study of the use of ergonomics information in a heavy engineering design process. International Journal of Industrial Ergonomics 26, 425-435

MoD Director Naval Architecture (1999). SSP11 Naval equipment procurement Human Factors Integration Technical Guide. NA145

Strain, J. D., Preece, D. A. (1999). Project management and the integration of human factors in military system procurement. International Journal of Project Management 17, 283-292

Svedung, I. and Rasmussen, J. (2002). Graphic representation of accident scenarios: mapping system structure and the causation of accidents. Safety Science 40, 397-417

Swain, A. D. and Guttman, H. E. (1980). Handbook of human reliability analysis with emphasis on nuclear power plant application, NUREG/CR-1278

UK MoD. DEF STAN 00-25: Human Factors for Designers of Equipment.

US Army (2000). MANPRINT: An Approach To Systems Integration. http://army.manprint.mil

Valancogne, J. and Nicolet, J.-L. (2002). Defence-in-depth: A new systematic and global approach in sociotechnical system design to guarantee better the timelessness safety in operation. Proceedings of the lambda-mu 13/Esrel 2002 conference

Vaughan, D. (1996). The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA. University of Chicago Press, Chicago, IL, USA

Vignes, P. (2002). Les Facteurs Humains. internal SNCF document

Wagner, D., Birt, J. A., Snyder, M. and Duncanson, J. P. (1996). Human factors design guide. DOT/FAA

Wright, P., Dearden, A. and Fields, B. (2000). Function Allocation: a Perspective from Studies of Work Practice. Int. J.Human-Computer Studies, 52, 335-355

Zakarian, A. and Kusiak, A. (2001). Process analysis and reengineering. Computers and Industrial Engineering 41, 135-150

Annex

Annex 1: Documentation of the method

SNCF HFI framework

Fabrice Delmotte – 09/03/2003

Table of contents

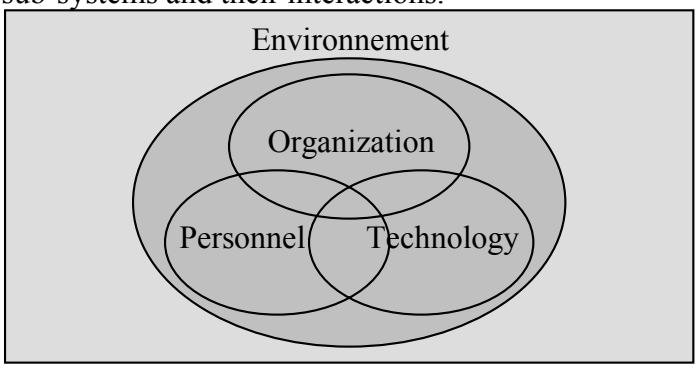
Introduction 177
General principles 177
HFI domains 179
Required skills 180
Project management framework 181
Overall view of the method 182
Guide of use of the method 184
Some links 187
Extensions 188
1 Conceptual design 189
1.1 Study of the context 190
R1 Study of the risks related to the context 195
1.2 Appoint HFI focus 198
1.3 Requirements analysis 199
R2 Study of the risks related to the requirements 203
1.4 Constitute an HFI working group 205
1.5 Function analysis 206
R3 Study of the functional risks 209
1.6 Preliminary allocation 212
1.7 Verification 212
2 Design 213
2.1 Mandatory allocations 214
2.2 Evolution of the project team 216
2.3 Possible allocations of functions 217
2.4 Dynamic allocation 219
R4 Evaluate the sociotechnical aptitude 221
2.5 Selection of the optimal allocation 224
2.6 Allocation verification 225
2.7 Design of the organization 226
2.8 Task design and analysis 229
2.9 Interface design 231
2.10 Estimate workload, performance and personnel 234
R5 Evaluate the global aptitude 237
2.11 Verification 240
3 Implementation 242
3.1 Prepare HF implementation 242
3.2 Study modifications 242
3.3 Perform part HF tests 243
3.4 Plan the local implementation 243
3.5 HF verification 243
3.6 Test 243
3.7 Finalize 243
3.8 HF check of the implementation 243
4 Pre-operational 244

5 Operations 245
5.1 Measure 245
5.2 Perform return on experience 246
5.3 Follow the evolutions 246
5.4 Perform studies on specific points 246
5.5 Update models and guidelines 246
5.6 Improve the system 246
6 Disposal 247
6.1 Reevaluate the impacts of the disposal 247
6.2 Prepare disposal 247
6.3 Dispose 247
6.4 Analyze the impact of the disposal 247
Glossary 248

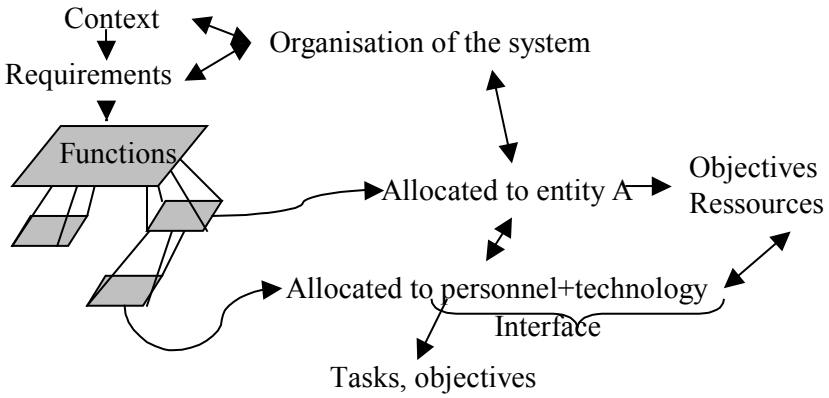
Introduction

General principles

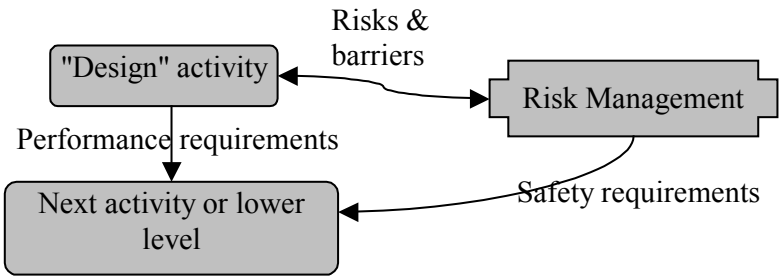
A system is considered as the interaction between three elements: the organization sub-system, the personnel sub-system and the technological one. The system is open on its environment with which it interacts. The performance (safety, efficiency, etc…) can be achieved through a joint optimization of these sub-systems and their interactions.



The present approach designs the system in a top-down matter. It starts from the expression of the whole system in its context to come progressively to the design of the tasks and interfaces. In-between it is concerned with the definition of the organization, the allocation of functions to the entities of the organization and then to the men and machines that are part of them.
A bottom-up analysis is then performed to ensure the coherence of the system.

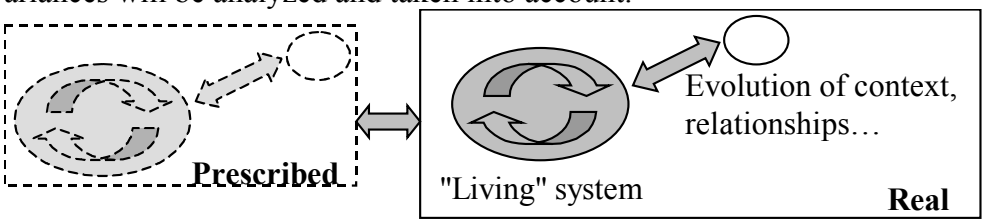


The purpose of the risk management activities is not only "verification". Those activities impact directly the design to obtain a safer system. Hence, an analysis at a given level will be translated into risks and possible barriers. That constitutes information to use for the activity performed in parallel, and to use further under the form of requirements for the next activities or levels.



Risk Management activities are spread out along the project. Indeed, safety needs to be "designed" progressively, from the global considerations to precise tasks. The earliest the IFS aspects are identified ("Important For the System", this concerns reliability – maintainability – availability – safety, safety being often the major focus, in which case IFS can be used as "Important For Safety"), the more likely the system design will take these aspects into consideration, and so the more likely it is to obtain a safer system as well as a more systemic view of the risks.

The study of the system must take into account its dynamics. On one side dynamics in the way it functions, and on the other side dynamics of evolution – especially between prescribed and real. Hence, the system needs to be analyzed in its behavior, and not only in its structure.
Possible variances will be analyzed and taken into account.



This approach is a participatory one. It is important to involve in the project the required Human Factors (HF) skills as well as the concerned persons. This involves of course the future users of the system but also people in relation with an entity modified or created by the project.

HFI domains

This method is based on six domains that it integrates to project management. Here is a short presentation of those domains.

Organization: This domain is concerned with the characteristics of the organization. This includes among others its structure, flows, level of integration and formalization, culture, communication etc. as well as the way the various support entities work.

Manpower: This domain is about the number of people concerned with the system, and the associated Human Resources management.

Personnel: This concerns the individual characteristics required for the operations of the system created or modified by the project. This includes physical and cognitive capabilities, recruitments procedures, socio-cultural factors, and experience.

Training: This domain covers the training (including "on-the-field" training) required to ensure that the personnel has the necessary skills, knowledge, principles and attitudes necessary for the operations.

Ergonomics: This domain is concerned with the integration of human characteristics in the design of the system. This covers among others interfaces and the work environment.

Safety: All aspects related to safety, including human reliability and personnel safety.

Required skills

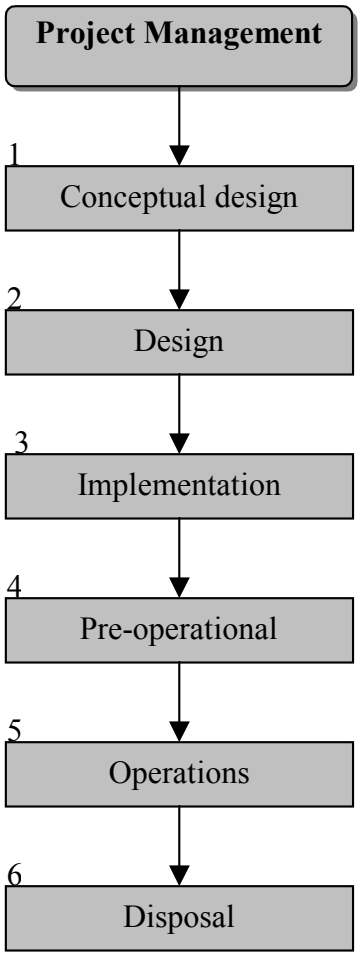
Globally, the method is open and intended for all project members, as one goal is to teach the utility of taking into account HF progressively during the projects.
The majority of the activities do not require specific skills.
The use of the method itself (managing a project with it) requires a person who knows systems engineering, has been trained to the method and introduced to the various skills required for some activities.
The knowledge and skills required for some activities (indicated in the present document for the concerned activities) are:

- Human reliability
- Organizational reliability
- Sociology of organizations and theory of organizations
- Training and skills management
- Human resources management
- Risk management and RAMS

Depending on the type of project, all those skills are not necessarily useful. A competent person assisting novice ones can normally perform the tasks for which such skills are required.

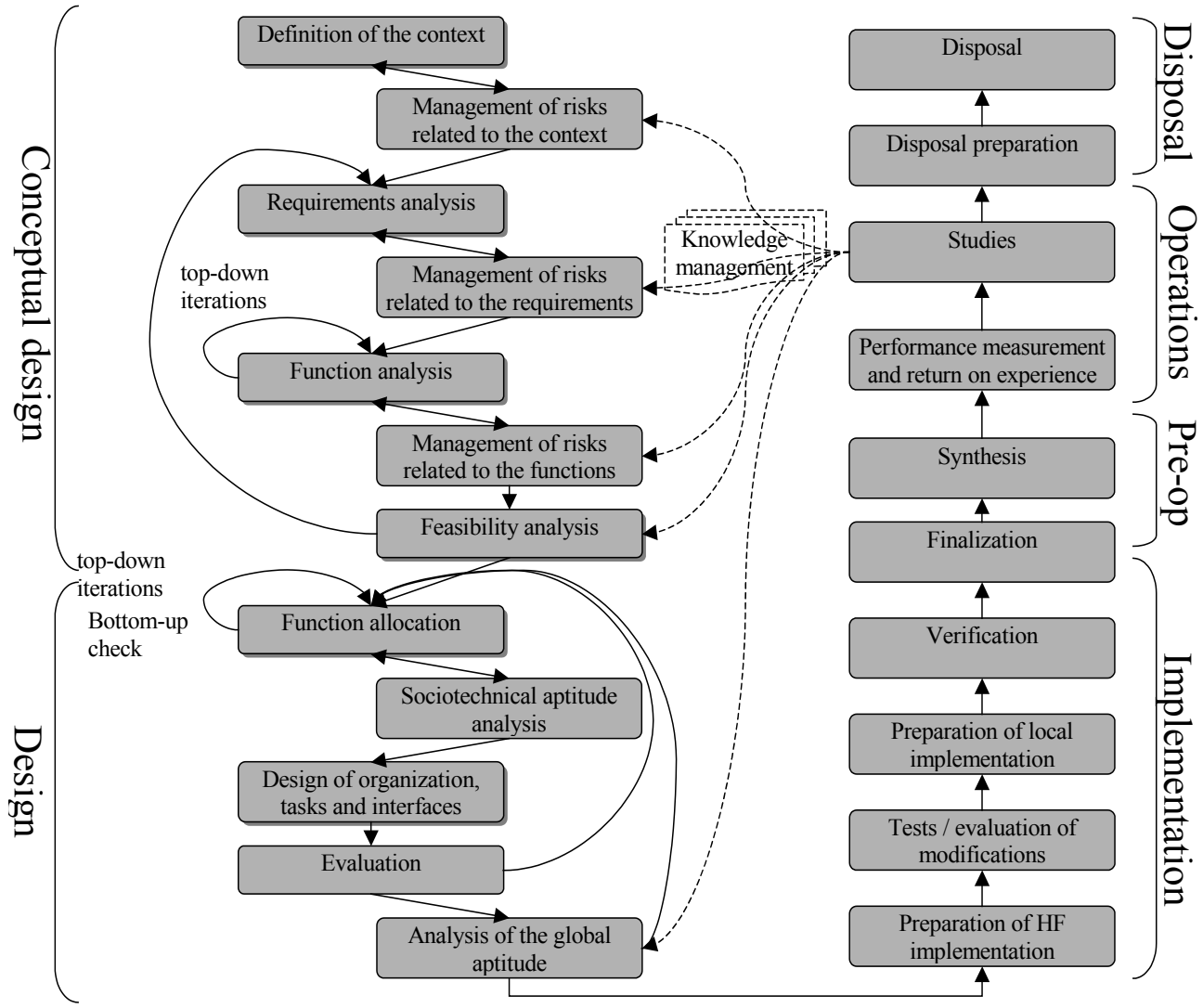
Project management framework

We consider the project management framework constituted of the six following activities as defined in the RG-0022 referential.

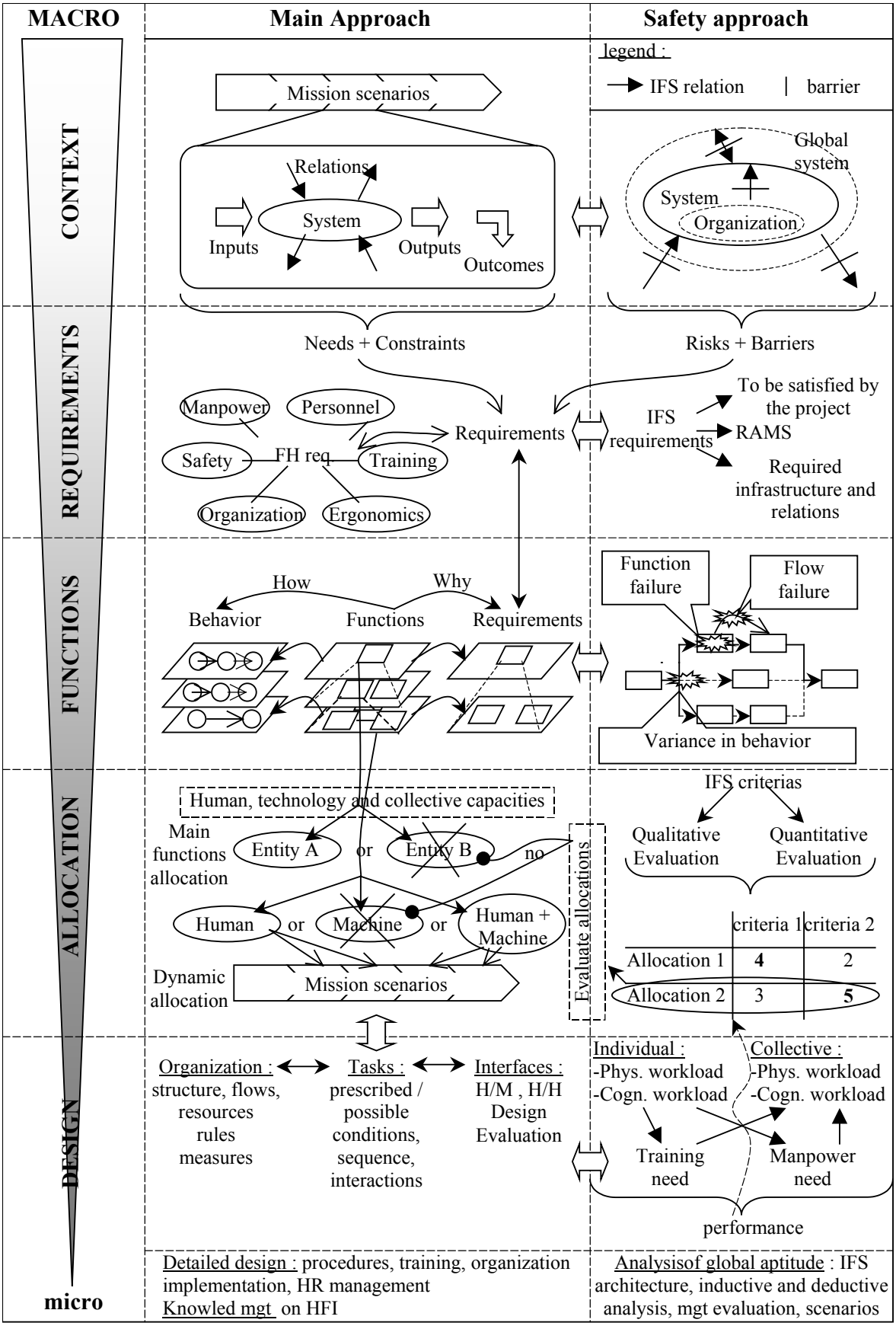


Overall view of the method

The following figure represents the main activities of the method.



The poster on next page enables a quick understanding of the overall logic of the method.


MACRO
Main Approach
Safety approach
CONTEXT
REQUIREMENTS
FUNCTIONS
ALLOCATION
DESIGN
micro
legend :
IFS relation
barrier
Mission scenarios
Relations
System
Inputs
Outputs
Outcomes
Global system
System
Organization
Needs + Constraints
Risks + Barriers
Manpower
Personnel
Requirements
Safety
FH req
Training
Organization
Ergonomics
IFS requirements
To be satisfied by the project
RAMS
Required infrastructure and relations
How
Why
Behavior
Functions
Requirements
Function failure
Flow failure
Variance in behavior
Human, technology and collective capacities
Main functions allocation
Entity A
or
Entity B
no
Human
or
Machine
or
Human + Machine
Dynamic allocation
Mission scenarios
Evaluate allocations
IFS criterias
Qualitative Evaluation
Quantitative Evaluation
criteria 1
criteria 2
Allocation 1
4
2
Allocation 2
3
5
Organization : structure, flows, resources rules measures
Tasks : prescribed / possible conditions, sequence, interactions
Interfaces : H/M , H/H Design Evaluation
Individual :
-Phys. workload
-Cogn. workload
Collective :
-Phys. workload
-Cogn. workload
Training need
Manpower need
performance
Detailed design : procedures, training, organization implementation, HR management
Knowled mgt on HFI
Analysisof global aptitude : IFS architecture, inductive and deductive analysis, mgt evaluation, scenarios

Guide of use of the method

The proposed method is modular. It can then be used on projects of different nature and size. It is important to know, depending on the project, which activities should be given more focus and which ones are of lesser use. Indeed, one given activity can be mandatory and extremely important for some projects but completely useless in other cases.
Through the following questions and the capacity to answer them precisely, the possible evolution in the answer and this answer itself, the following guide indicates how to use the method at its best on a project.

Question 1: Which systems are impacted by the project?
Related questions:
Which system is directly concerned by the project?
What are the systems in relation with this system?

Capacity to answer the question
Bad: If you cannot answer precisely, then activity 1.1 (context) is very important.
Good: In this case, check that you are able to answer the various questions raised by activity 1.1.

Possible evolution of the answer
Large: If the number or definition of impacted systems will depend on the evolution of the project, then tasks 1.1.5 and 1.1.9 must be carried out in detail. This dynamical context shall be kept in mind during the project.

Answer
Many systems are impacted: In this case, tasks 1.1.3, 1.1.4, 1.1.8 and activity R1 are very important.
The system concerned directly by the project is complex: The system should be well understood. This must be achieved through tasks 1.1.1, 1.1.2, 1.1.6, 1.1.12 and activity R1.

Question 2: How does the project affect safety?
Related questions:
Is safety important for the system directly concerned by the project?
Is safety important for the systems in relation?

Capacity to answer the question
Bad: In this case, required time will be taken to identify correctly the system (activity 1.1) as well as the related risks (activity R1).

Possible evolution of the answer
Large: In this case, performing risk management activities R1 to R5 and ensuring their traceability and integration with the rest of the project is very important. In particular, validation activities (R3, 1.7, R5) must be carried out seriously.

Answer
The project has a big impact on safety: The method must then be carried out in detail, especially activities R1 to R5.
Safety is linked to interactions between systems: Activities 1.1 and R1 are very important.
Safety depends of human tasks: Then activities R4, 2.8, 2.9, 2.10 and R5 are very important.

Question 3: Does the project affect many people?
Related questions:
Does the project concern many hierarchical levels?
Does the project impact many different categories of personnel?

Capacity to answer the question
Bad: Then the user must be sure to have well understood the system (1.1). Then, it is required to perform in detail the function allocation activities 2.1 to 2.6 and R4.

Possible evolution of the answer
Large: If the number of impacted people depends on choices in the project, then activities 1.5 and 2.1 to 2.6 require specific attention, especially concerning the high-level functions.

Answer
The project impacts many people: Tasks 1.3.4, A.3.7, A.3.18 and activities 2.7 to 2.10 are important.
The project impacts many hierarchical levels / many different categories of personnel: Specific attention required for activities and tasks related to the organization: 1.1.6, 1.1.12, 1.3.7, 1.3.13, 2.1, 2.3, 2.7, 2.10.

Question 4: Are there many interfaces in the impacted systems?
Related questions:
Do the impacted system require much cooperation / coordination?
Are there many human-machine interfaces in the impacted systems?

Capacity to answer the question
Bad: Detail activities 1.5 and 2.1 to 2.6.

Possible evolution of the answer
Large: It is then necessary to detail activities 2.1 to 2.6 in order to find the best allocation.

Answer
Many human-machine interfaces: Specific attention required for activities 2.3 to 2.5, R4 for the functions carried out by the interfaces, 2.8 to 2.10.
Much cooperation / coordination: Activities related to the organization need to be well performed. Activities 2.3 to 2.5 (especially 2.4) and R4 require attention for the functions involving coordination or cooperation. Activities 2.7 to 2.10 are then important, especially tasks 2.9.13 to 2.9.18 and 2.10.8 to 2.10.14.

Question 5: What are the objectives and constraints of the system?
Related questions:

What are the real needs and constraints?
How does the project intend to meet the need?
What is the probability that the project reaches its objectives?

Capacity to answer the question
Bad: Activities 1.1 and 1.3/R2 are very important. Then, it is necessary to ensure a good traceability of the requirements.

Possible evolution of the answer
Large: Then it is required to put in place a good traceability of the requirements and their evolutions, and be sure to identify and manage project risks thanks to activity R2.

Answer
Real needs and constraints are not well known: Take the required time to carry out activities 1.1, R1 and 1.3.
The way to answer the need is not clear / does not seem the best one yet: It is then worthy to perform well and in order activities 1.1, 1.3 and 1.5, without trying to find a solution "immediately".
Probability that the project reaches its objectives is not very high: In this case, focus on activity R2 and verification activities.

Some links

Here are some useful links. They constitute a good starting point for who wishes to acquire a culture on human factors integration, and can be useful for some aspects of the method.

www.eurocontrol.int/eatmp/hifa and **www.hifa.org**: Sites of the HIFA project, which aim is to develop a similar methodology for Air Traffic Management centers. The sites have a list and description of method and tools useful for the different activities of the method.

www.manningaffordability.com: Site of the project for HFI in the navy. This method is adapted from their method, and they also propose a list of tools, as well as some interesting articles and links.

www.dtica.dtic.mil/ddsm: List of tools for Human Factors Engineering.

www.incose.org: Site of the International Council on Systems Engineering. Some books and articles can be downloaded there to get an introduction to systems engineering. There are also many links. The French branch of the Incose can be found at **www.afis.fr**.

www.usabilitynet.org: Site on ergonomics resources. Describes among others some methods to use during the various phases of a project.

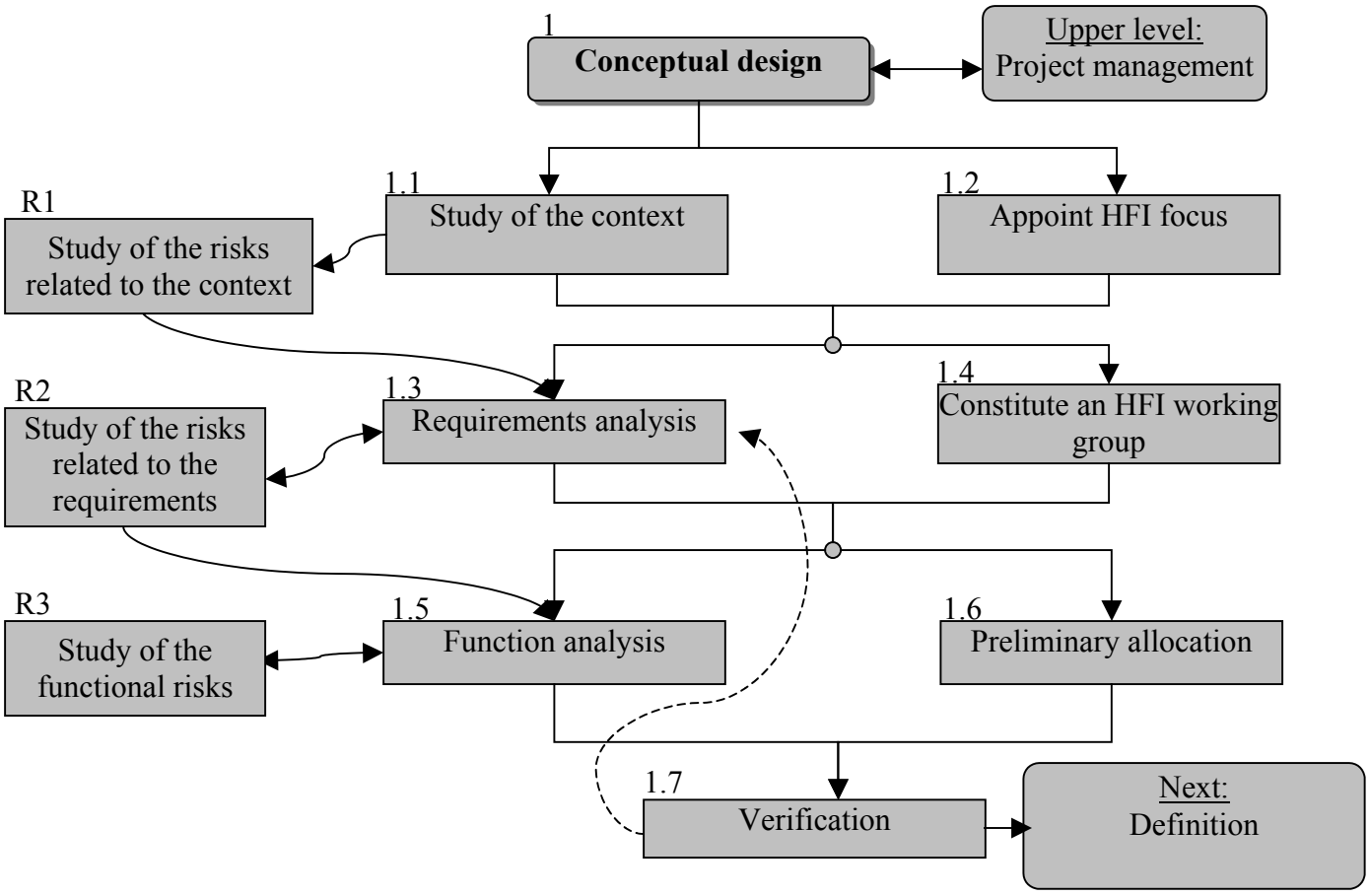
Extensions

As it is proposed in this current form, the method covers essentially the main process of the project – intended to create or make a system evolve – as well as the aspects related to risk management.

Some extensions have been researched for the other HFI projects and can be useful. Here are two of them:

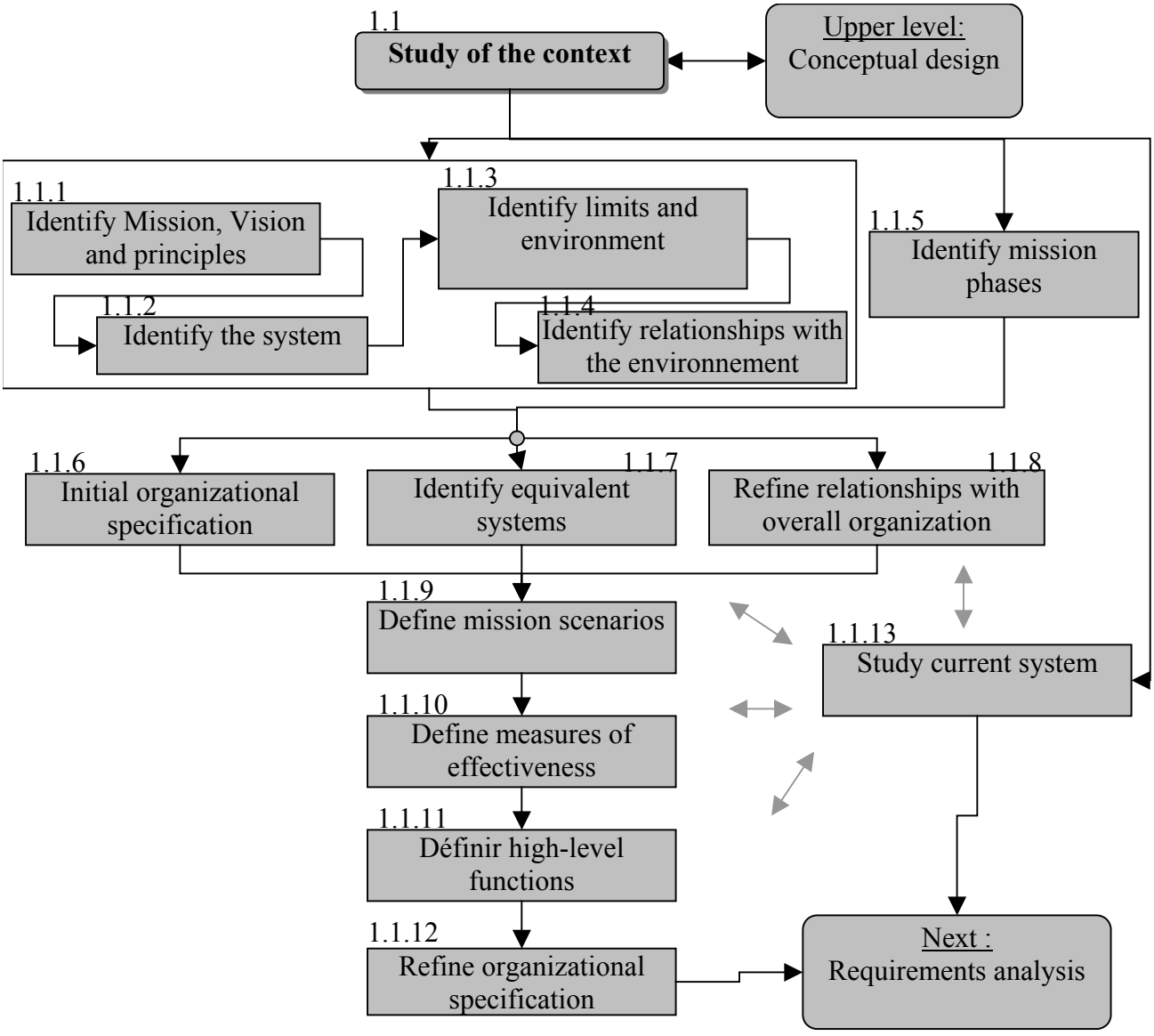
- **Cost Effectiveness Assessment**: The cost aspect is not detailed extensively in the method, as it is supposed to be done "naturally". However, it can be mentioned that a specific approach exists, aimed at integrating Cost Effectiveness Assessment with a method like this one. The reader is invited to visit: **www.ams.mod.uk/ams/content/docs/hfiweb/docs/htm**
- **HFICMM**: The "Capability Maturity Model" as it is used in systems engineering helps evaluate practices. There exists one for the HFI. Such an approach can be used to check that projects integrate human factors efficiently, and that there is progress in thee company towards this objective. Documents can be found at the following address: **www.lboro.ac.uk/research/husat/eusc/r_usability_assurance.html**

1 Conceptual design



1.1 Study of the context

During this activity, the global objectives of the system, its limits, the context in which it evolves and its main functions are identified.



All members of the project team must participate in this activity. Most tasks can be performed without specific skills. Concerning the study of the current system and of the relationships with the overall organization, knowledge in sociology of organizations can be necessary. For the organizational specification, a good knowledge of the theory of organizations is also profitable.
The input of some other persons can also be worthy: users of the existing system, users of systems in relation, users of equivalent systems.

1.1.1 Identify mission, vision and principles

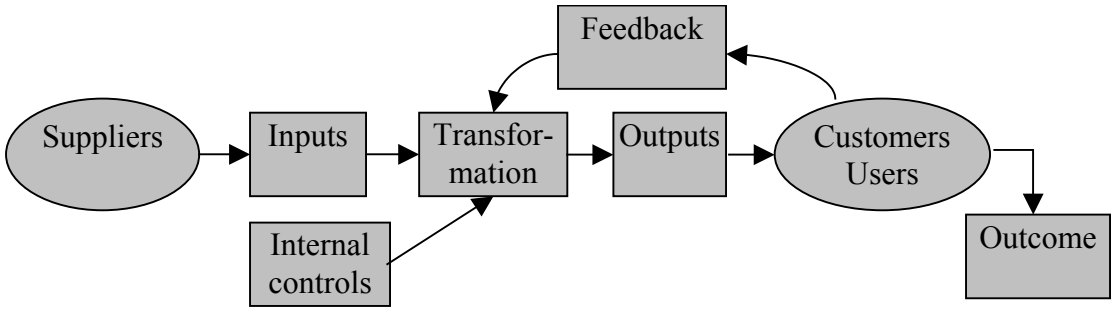
Define:

• The mission of the system: Its use, objective, what it will be defined for

• Vision of the system: How we want it in 5-10 years
• Principles: Values reflected by the system, incl. safety culture

1.1.2 Identify the system

The aim is to define more precisely the function of the system through its main suppliers, customers, inputs, outputs and processes.



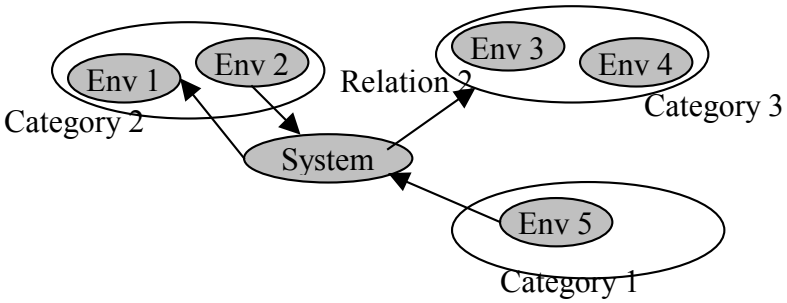
1.1.3 Identify the limits of the system and its environment

Identify what we consider as the limits of the system that will be designed or modified. Everything outside this system will become the environment. It is not always easy to identify the system; one simple rule consists in including in it all elements that can be modified during the project.

The environment includes physical, economical, regulatory, informatory elements. They are classified depending on their proximity with the system and/or nature.

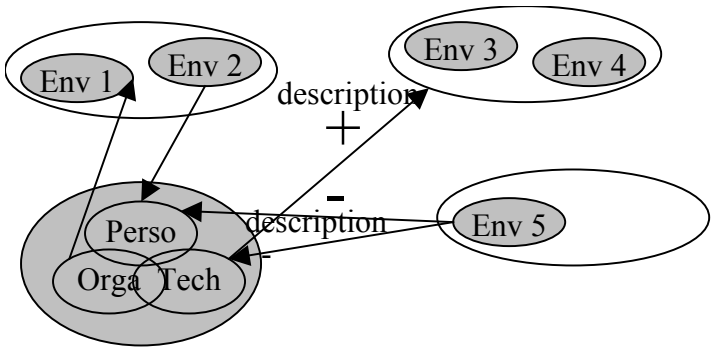
We can start identifying what links those elements to the system.

Support elements shall not be forgotten (maintenance, supplies).



1.1.4 Identify relationships with the environment

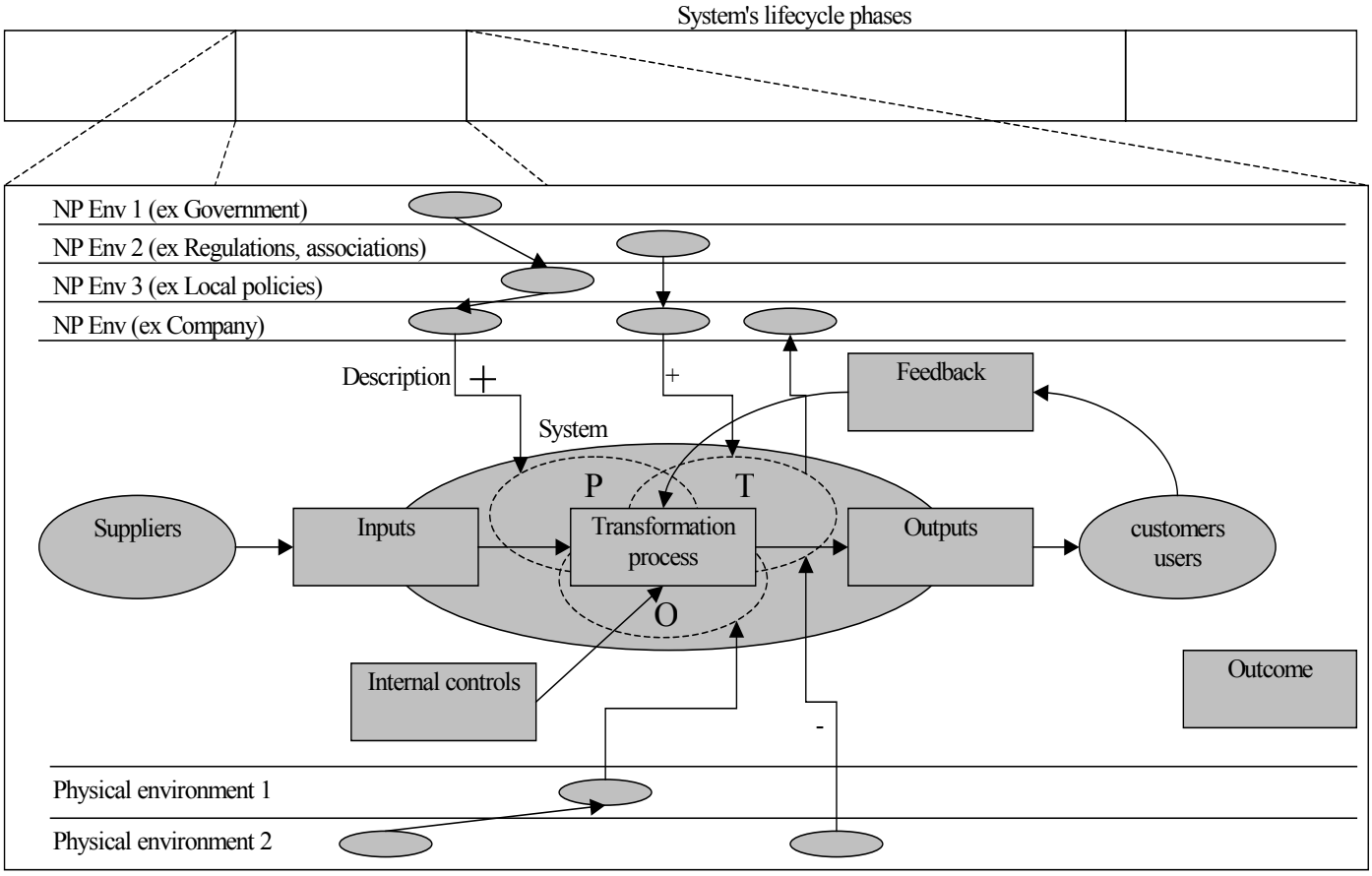
Identify more precisely what links the system to its environment, and the polarity of the relation. A positive relation is one in which the good health of the starting system improves the health of the related system; a negative one is the opposite case. The size of the polarity depends on the intensity of the relationship. This helps understand the dynamics of the whole "universe" in which our system evolves.



If a system of the environment will be largely impacted by the project, it can be further detailed at this step.

1.1.5 Identify mission phases

Define changes in system's main mission during its lifecycle. The changes concern among others operation modes, changes in the context or relationships.



The transition states between the current state (before the project) and the operations are also to be included here. This helps taking into account the notion of change.

1.1.6 Initial organizational specification

Given the initial objectives of the system, its principles and environment, it is possible to define the appropriated global characteristics for the organization.
These characteristics cover:

- the levels of complexity (differentiation and integration), formalization and centralization
- the priorities (quality, polyvalence, development, safety etc…)
- the type of organization (cf. Mintzberg)
- the characteristics of the main tasks (variability, simplicity, specificity, level of abstraction) and of the personnel (level, availability, implication)

1.1.7 Identify equivalent systems

Identify systems close to ours in terms of context and objectives.

1.1.8 Refine relationships with the existing organization

Study more precisely the relationships between the system and the organization in which it inserts or it replaces, especially between the initial organizational specification and this organization. Study how one will influence the other.

1.1.9 Define mission scenarios

Refine the phases in order to obtain the possible mission scenarios. Define as precisely as possible these scenarios in terms of modification of context and specific values and objectives.
One scenario can correspond to a normal state of the system but also (and those should not be forgotten) to a degraded state.

1.1.10 Define measures of effectiveness

Define measures that will enable an evaluation of the global performance of the system in reaching its objectives, moving towards its vision while respecting its principles, and ensuring the good operations of the specified organization.

1.1.11 Define high-level functions

Identify the main functions of the system, depending on the previously-identified mission scenarios. These high-level functions shall of course enable to reach the objectives, ensure the respect of the values, but also allow the recovery in case of a mission in degraded state, and prevent if possible from entering those degraded states.

1.1.12 Refine the organizational specification

Given the mission scenarios, measures and high-level functions, refine the initial organizational specification to ensure that it corresponds to the measures, enables the execution of functions and is adapted for the various scenarios, including the ones in degraded state.
The following organizational characteristics can be studied:

- External influences
- Goals and strategies
- Management functions
- Resource allocation
- Human resources management

- Training
- Co-ordination of Work
- Organizational knowledge
- Proceduralization
- Organizational culture
- Organizational learning
- Communication

Analyze the real organization that is likely to develop from this prescribed organization. The next analyses will also take into account these potential organizational dimensions.

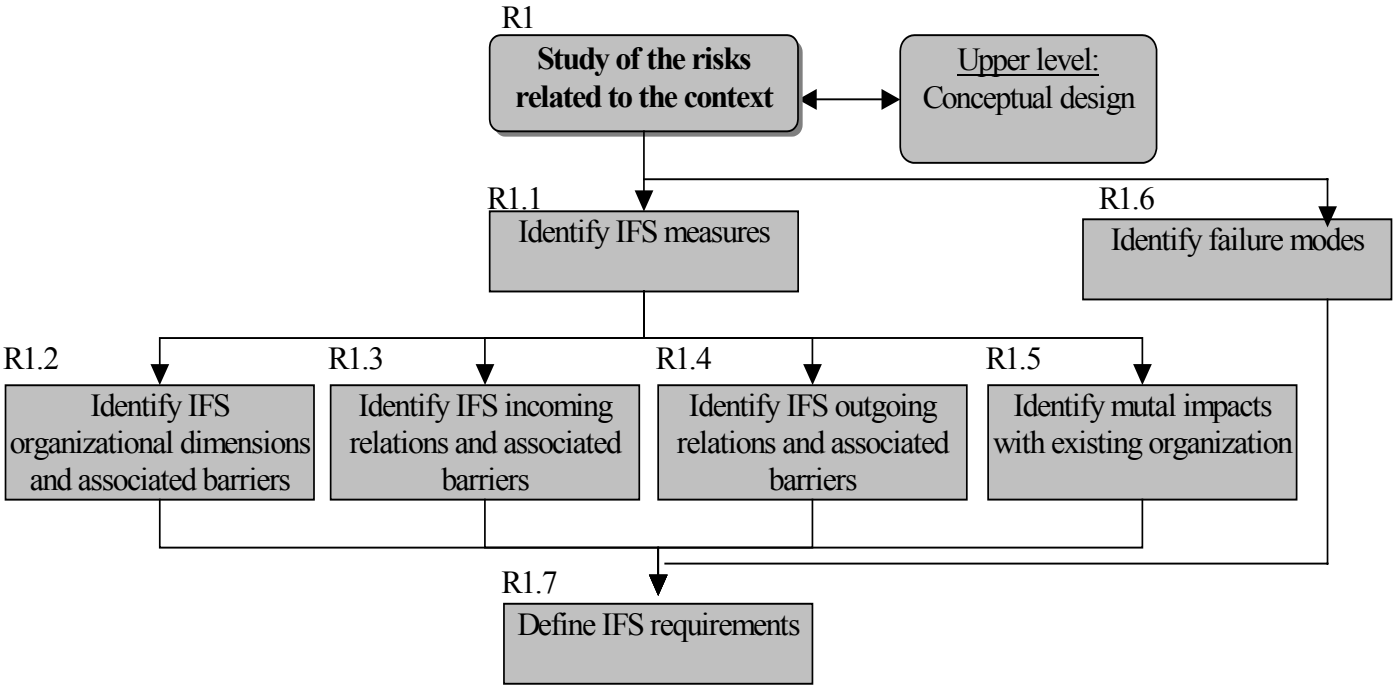
1.1.13 Study current system

If the project is to modify an existing system (replace one and/or modify the organization in which a new system integrates), it is necessary to identify this system well. On one side, this will improve our understanding of the context as well as the next analyses. On the other side, in the case of an organizational change, the existing system will have a direct impact on the project.
The main activities are:

- Exploit the return-on-experience, especially the positive and negative aspects of the existing system
- Identify the impact of previous projects on the system and their acceptance
- Analyze the informal organization: goals, constraints, powers and strategies
- Gather needs, ideas, and remarks from the concerned users. This can be achieved through the use of questionnaires and interviews. Identify weak and strong points.

R1 Study of the risks related to the context

We will identify the elements that can be positive or negative for the system, especially for its safety. These elements are linked to the definition of the system, through its measures, to the organizational dimensions and to the relationships.



This activity does not require specific skills. An introduction to cindynics might be helpful in order to get a global view of the risks. Concerning IFS organizational dimensions and barriers, an introduction to organization reliability is recommended.

R1.1 Identify IFS measures

Among the measures of effectiveness, identify the ones with a great impact on the reliability of the system.

Also identify other aspects important to the reliability, linked to the different kind of risks, by analyzing the failure modes of the main functions.

	Associated risks (financial, deterioration, loss of prestige etc…)			
Measures & main functions				

R1.2 Identify IFS organizational dimensions

Among the organization dimensions of the system, identify the ones with a great impact on reliability and safety.

Identify possible barriers to limit the risks associated with these dimensions (for example by ensuring that they will be respected in the real organization that will develop from the prescribed one).

	Prescribed organizational dimensions		Possible organizational dimensions	
IFS measures & main functions	Impact / Barrier			Impact / Barrier
			Impact / Barrier	
		Impact / Barrier		Impact / Barrier

	What can impact those dimensions			
Organizational dimensions		Impact / Barrier		
			Impact / Barrier	Impact / Barrier
	Impact / Barrier			Impact / Barrier

R1.3 Identify incoming IFS relations

Among the relations between the environment and the system, identify the ones towards the system that impact the safety. By impact, we mean those that are sources of hazards for the system, but also those required to guarantee a given level of safety.
Establish the level of criticity of the relation and obtain its level of IFS importance by multiplying it with the intensity of the relation (keep in mind the polarity of the relation).
Identify possible barrier to limit the risks linked to these relations.

	Incoming IFS relations			
IFS measures & main functions	+ Impact			+ Impact
			- Impact	
		- Impact		- Impact

	Incoming IFS relations			
IFS measures & main functions	Barrier			Barrier
			Barrier	
		Barrier		Barrier

R1.4 Identify outgoing IFS relations

Among the relations from the system towards its environment, identify the ones that can present a risk for the elements belonging to the environment. Distinguish between risks linked to the system in its normal state and those linked with the system in a degraded state.
Identify possible barriers to limit those risks.

	IFS measures & main functions			
Outgoing IFS relations	+ Impact			+ Impact
			- Impact	
		- Impact		- Impact

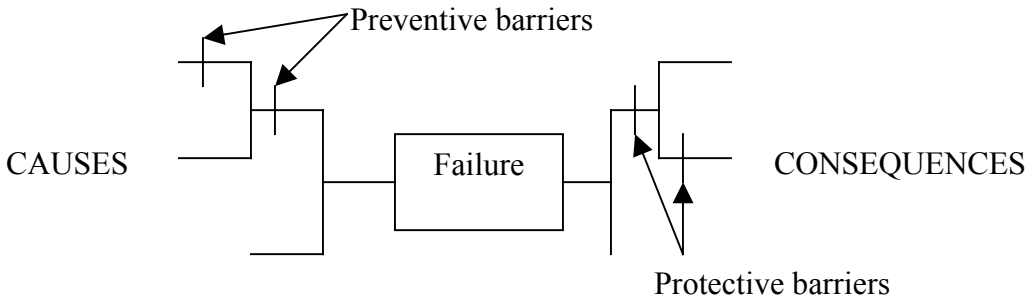
	IFS measures & main functions			
Outgoing IFS relations	Barrier			Barrier
			Barrier	
		Barrier		Barrier

R1.5 Identify mutual impacts with the existing organization

Evaluate how the existing organization in which the system integrates can impact the system and vice-versa in terms of safety. This consists in fact in refining the analysis to this specific environment that can more easily be observed and modified, and has also usually a bigger impact.

R1.6 Identify failure modes

From the previous elements as well as brainstorming on other possible problems, build a diagram of the possible failures, their causes and consequences, as well as the possible or existing barriers.



This identification will be more and more detailed when the project goes on, so that the aspects identified here will be further refined in requirements, functions and elements of the system.

R1.7 Define IFS requirements

From the measures, organizational dimensions and IFS relations identified previously, as well as the associated barriers, define requirements that will help ensure the safety and reliability of the system. Also refine IFS measures.
Identify aspects that require specific attention when the current barriers do not seem sufficient.

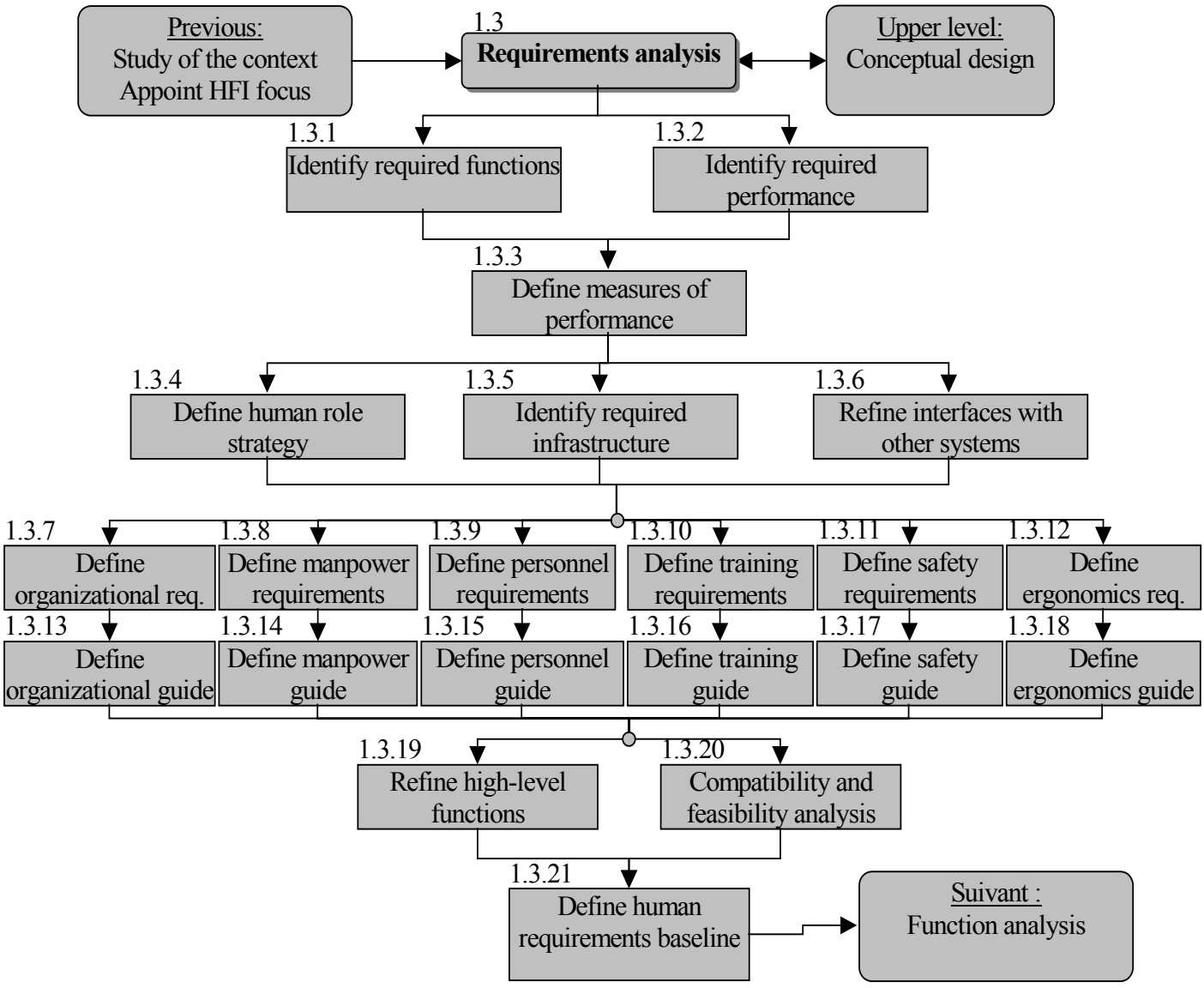
1.2 Appoint HFI focus

In order to ensure that required activities are well performed, and that consequently human factors have been taken into account, an HFI focus is to be appointed by the project manager. This person knows the method and has taken introductory training in the various skills used (sociology of organizations, theory of organizations, cindynics, organizational reliability, human reliability), however it is not necessarily a human factors specialist.
On some smaller projects, the project manager can be the HFI focus.

1.3 Requirements analysis

The purpose of the activity is to identify characteristics required from the system so that it can perform its mission while optimizing the measures.

The activities described here concern the HF ones, however the analysis of technical requirements is to be done in parallel of activities 1.3.7 to 1.3.18.



The definition of requirements and guides for the six HFI domains requires specific skills in each of those domains.

1.3.1 Identify required functions

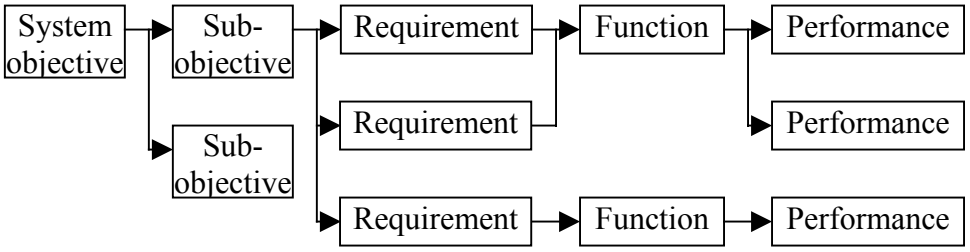
Identify activities, tasks and actions required for the system to correctly perform its mission.

Required functions are not only the ones that ensure the transformation process, but also the ones that are required for the barriers and for recovery purposes.

1.3.2 Identify required performance

Identify the performance required from the system to reach its objectives.

We will then build progressively the requirements, for example by using requirements trees such as this one:

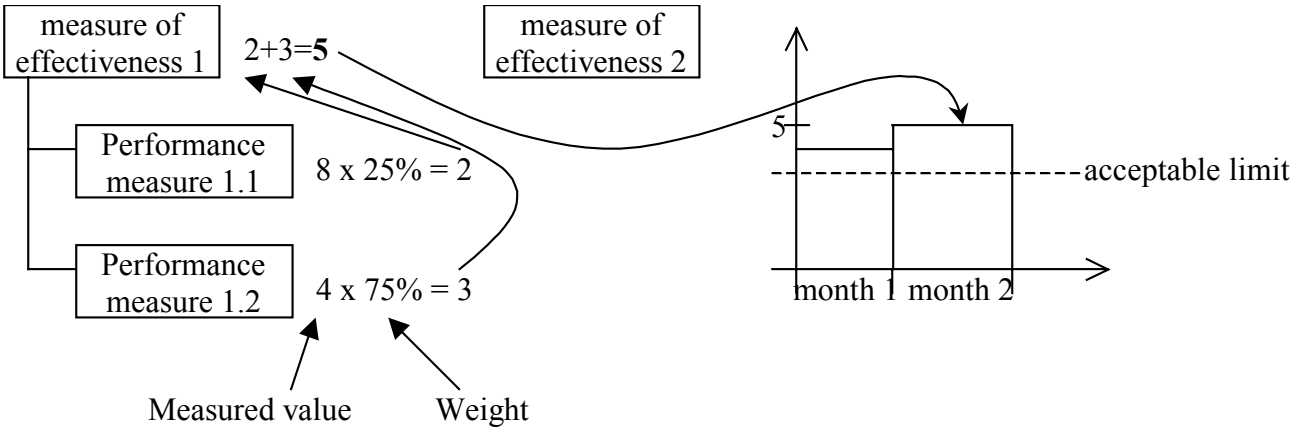


It is useful to classify and codify the requirements to enable a good traceability until the end of the project:

Code	Description
E1	
E1.1	This req. serves req. E1
E1.1.1	This req. serves req. E.1.1
E2	

1.3.3 Define performance measures

The measures of effectiveness identified previously are refined here. The IFS measures are of course added.
The performance measures will help evaluate the design and then the system, and verify its "health" in operations. More precise than measures of effectiveness, performance measures can be directly measured, and the aggregation of their results help obtain measures of effectiveness.



1.3.4 Define human role strategy

Start thinking about what entity of the organization will be in charge of which functions, activities and decisions, and about the global level of automation.

This level can be defined by identifying the characteristics of the functions and activities, and applying a given number of principles related to automation. At the organizational level, automation covers expert systems (decision aid), information systems etc.

Estimate globally acceptable number of people, skills and associated costs.
Identify methods and tools that will be used during the specific requirements analysis, as well as required skills.

1.3.5 Identify the required infrastructure

Identify the infrastructure that needs to be created or maintained in order for the system to operate. Define the elements considered as exterior to the system that need to be modified or controlled. This includes among others the organization in which the system integrates, maintenance and logistic support.

1.3.6 Refine interfaces with other systems

Update the relations with the environment performed during the study of the context and the associated risk analysis. Analyze requirements related to those interfaces.
From the organizational specification and human role strategy, identify more precisely the entities of the system that will be directly involved in the interfaces.

1.3.7 Define organizational requirements

Define the requirements on the organization that will operate and maintain the system, the specific needs and constraints.
Use the initial organization specification as well as the evaluation of IFS organizational dimensions.

1.3.8 Define manpower requirements

Estimate requirements on the number of people.

1.3.9 Define personnel requirements

Define requirements on the skills/aptitudes of the personnel.

1.3.10 Define training requirements

Define the requirements in terms of documents to develop, training sessions to organize etc. to prepare the personnel.

1.3.11 Define safety requirements

Refine the previous analysis, by identifying the characteristics of the design, the performance specifications, training and measurement system required to ensure the optimal safety of the system.

1.3.12 Define ergonomics requirements

Identify the properties of the system required to be adapted to the human sub-system. This includes among other interfaces, workplace, and work cycles.
These requirements must respect the physiologic and cognitive human capacities.

1.3.13 Develop organizational guidelines

The guidelines take into account requirements and constraints in order to define the required properties, limits and actions required, skills to mobilize during the project, documents and previous studies to use. They transform the requirements on the system into requirements for the project.
The organizational guideline describes the more appropriate or risky structures, levels of formalization and integration etc…

1.3.14 Develop manpower guidelines

Estimate constraints and needs in terms of number of people.

1.3.15 Develop personnel guidelines

Estimate possibilities and limits in terms of knowledge, skills and aptitudes.

1.3.16 Develop training guidelines

Estimate constraints in terms of training. Consider aspects like cost, time and availability of the personnel. Take into account available skills and skills required to operate the system in order to evaluate the required training.

1.3.17 Develop safety guidelines

Provide guidance for the project to ensure that safety factors are taken into account. Include norms to respect, authorizations to obtain etc.

1.3.18 Develop ergonomics guidelines

Guide the design so that human capacities and limits are taken into account. This includes the description of human performances, models, methods and techniques.

1.3.19 Refine high-level functions

Define to greater detail the functions. Take into account changes induced by the requirements analysis.

1.3.20 Compatibility and feasibility analysis

Study the requirements to identify conflicts among them, variances with system characteristics like infrastructure and interfaces with other systems. Estimate the feasibility of the project.

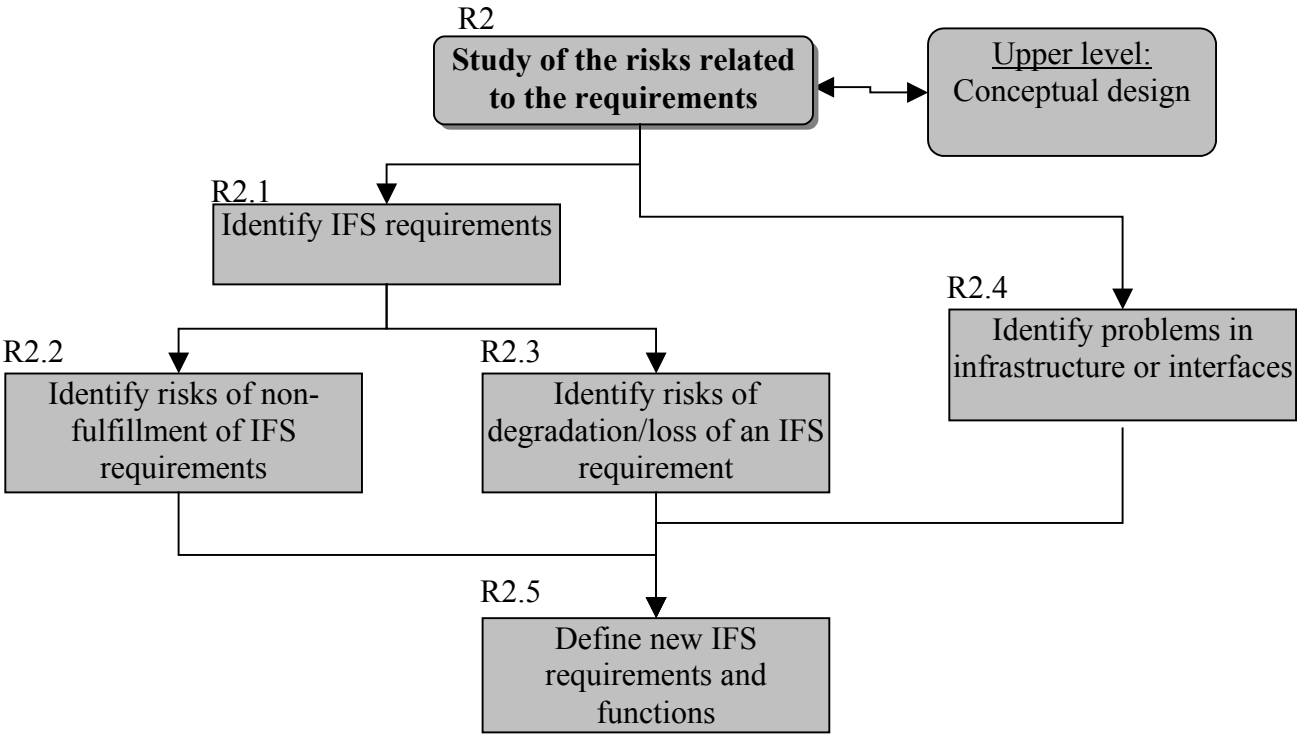
1.3.21 Define human requirements baseline

Establish the synthesis of information required to ensure that HF are well integrated.

R2 Study of the risks related to the requirements

Risks related to the requirements are identified here. Activity R1 is reused and refined here. We consider that risks can be of three types:

- risk that the requirement cannot be fulfilled by the project, which represents a project risk but also a risk for the system given the possible consequences
- risk of a requirement degradation, failure or loss during the system lifecycle
- problem in an infrastructure or interface with consequences on the requirements, or risk that a requirement represents for the system and/or its environment.



R2.1 Identify IFS requirements

Among the various requirements, identify the one which have an important role for safety. Those can be partly deducted from activity R1, especially from the IFS measures.

Requirement	IFS measure 1	IFS measure 2	IFS measure 3	IFS	Importance
E1				Yes	
E1.1				Yes	
E2				No	
E3				Yes	

R2.2 Identify risks of non-fulfillment of IFS requirements

The feasibility of the requirements will be evaluated here. This task will identify how a requirement could not be done and the consequences on the general safety of the system. This activity is concerned mostly with project risks.

Requirement	Probability	Criticity	Risk	Observations
E1				
E1.1				
E3				

R2.3 Identify risks of degradation/loss of an IFS requirement

The problems that could affect the requirements during the operations of the system are identified here, as well as the possible causes and eventual consequences of those degradations or losses.

R2.4 Identify problems in infrastructure or interfaces

The work performed in R1 is continued here. Impacts and barriers are further detailed, as well as problems that can happen with the required infrastructure and their consequences on the system.

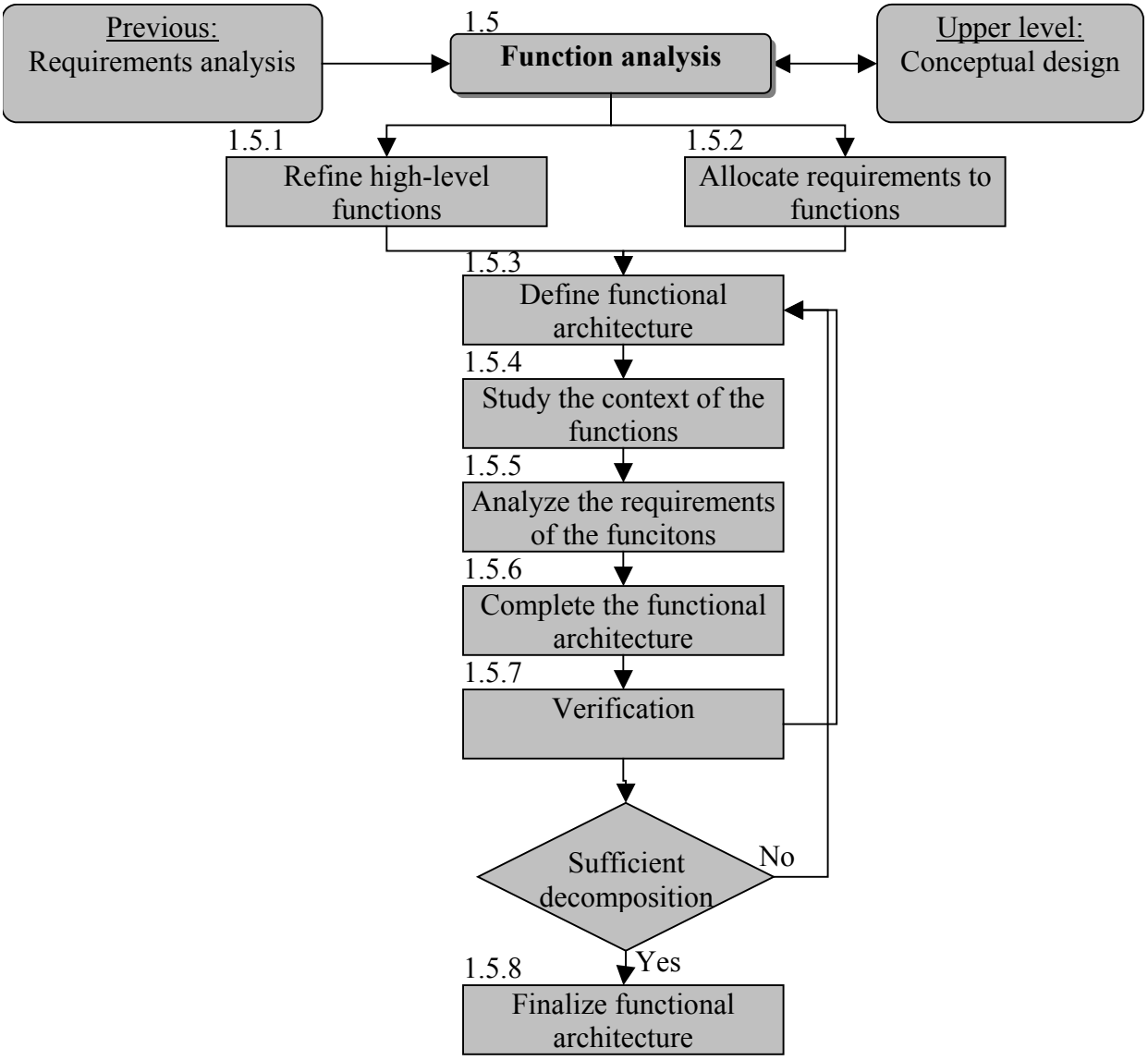
R2.5 Define new IFS requirements and functions

From the risks identified and the barriers, it is possible to identify new IFS requirements. It is also time to start turning these requirements into functions, which will be integrated in the function analysis.

1.4 Constitute an HFI working group

A HFI working group must be constituted in parallel of the requirements analysis activity.
The composition of this group will depend on this activity and the study of the context, which enable to identify important organizational and human factors in the project, as well as the relative importance of the various domains.
For each domain, the FHI focus and the project manager appoint a domain focus. The focus is proficient with the domain (or domains) he is in charge of and is responsible of communicating correctly with the right experts.

1.5 Function analysis



This activity requires a good knowledge of function analysis methods.

1.5.1 Refine high-level functions

From the previous analyses, describe more precisely the high-level functions, in order to set the bases for the functional architecture.

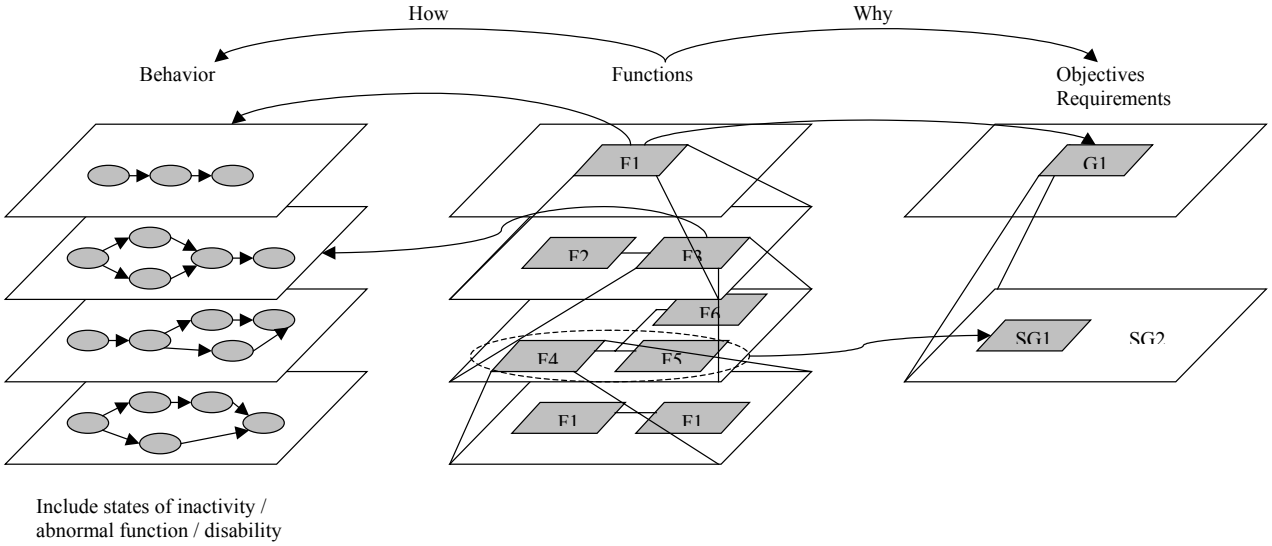
1.5.2 Allocate requirements to functions

Identify the functions required for the system to be operational based on the requirements.

1.5.3 Define a functional architecture

Using the previously identified functions, define a functional architecture.

The aim is to obtain a "picture" of the system in terms of functions, which are used to reach goals, and are performed following a given behavior.

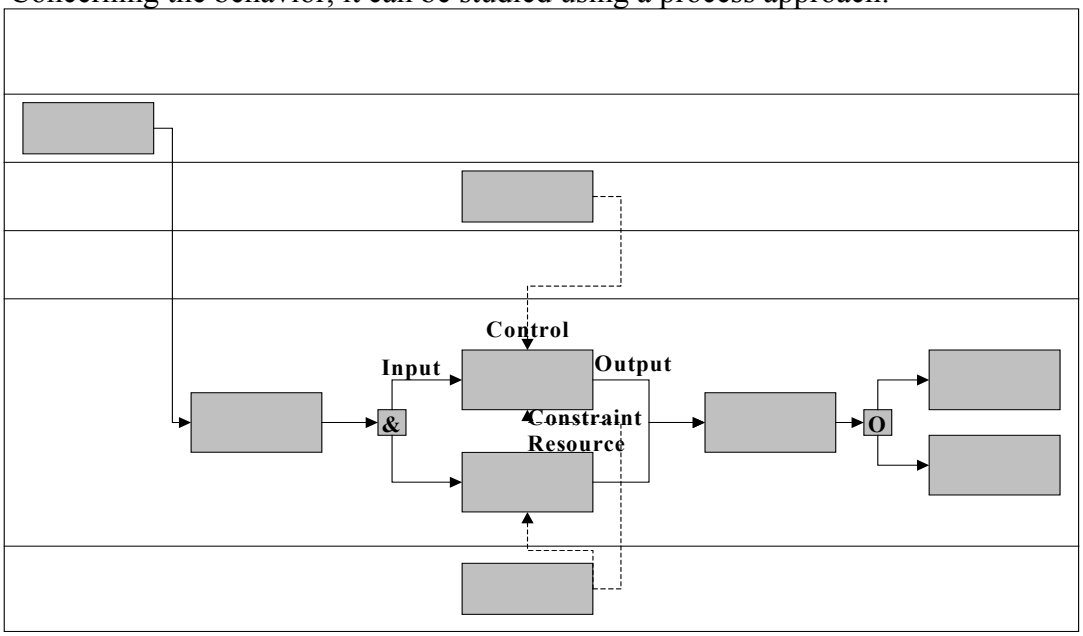


It is important to identify well the goals and resources. Indeed, the future evaluation of human and organizational reliability will use not only the structure of the system, but also the goals, as they will play a major role in the development of strategies and the dynamic allocation. Similarly, the behavior is important as it is how the system will work and how human will perceive it.

Functions fulfill the requirements. They include not only the functions used by the system to perform its mission, but also the one necessary for its safety, and those which provide the appropriate support.

The behavior indicates of course the behavior in normal state, but also that in possible degraded state as well as recovery behavior.

Concerning the behavior, it can be studied using a process approach:



For the important goals, identify other ways of reaching those goals in order to understand how the system might evolve in real operations.

1.5.4 Study the context of the functions

Repeat the context study for the functions. This implies particularly to analyze well the various scenarios they will face, their inputs, outputs and relations with the system and its environment. also identify the frequency, precision, duration, priority and various modes.

1.5.5 Analyze function requirements

From the context and requirements, identify requirements for each function.

1.5.6 Complete the functional architecture

Using the previous tasks, complete the functional architecture.

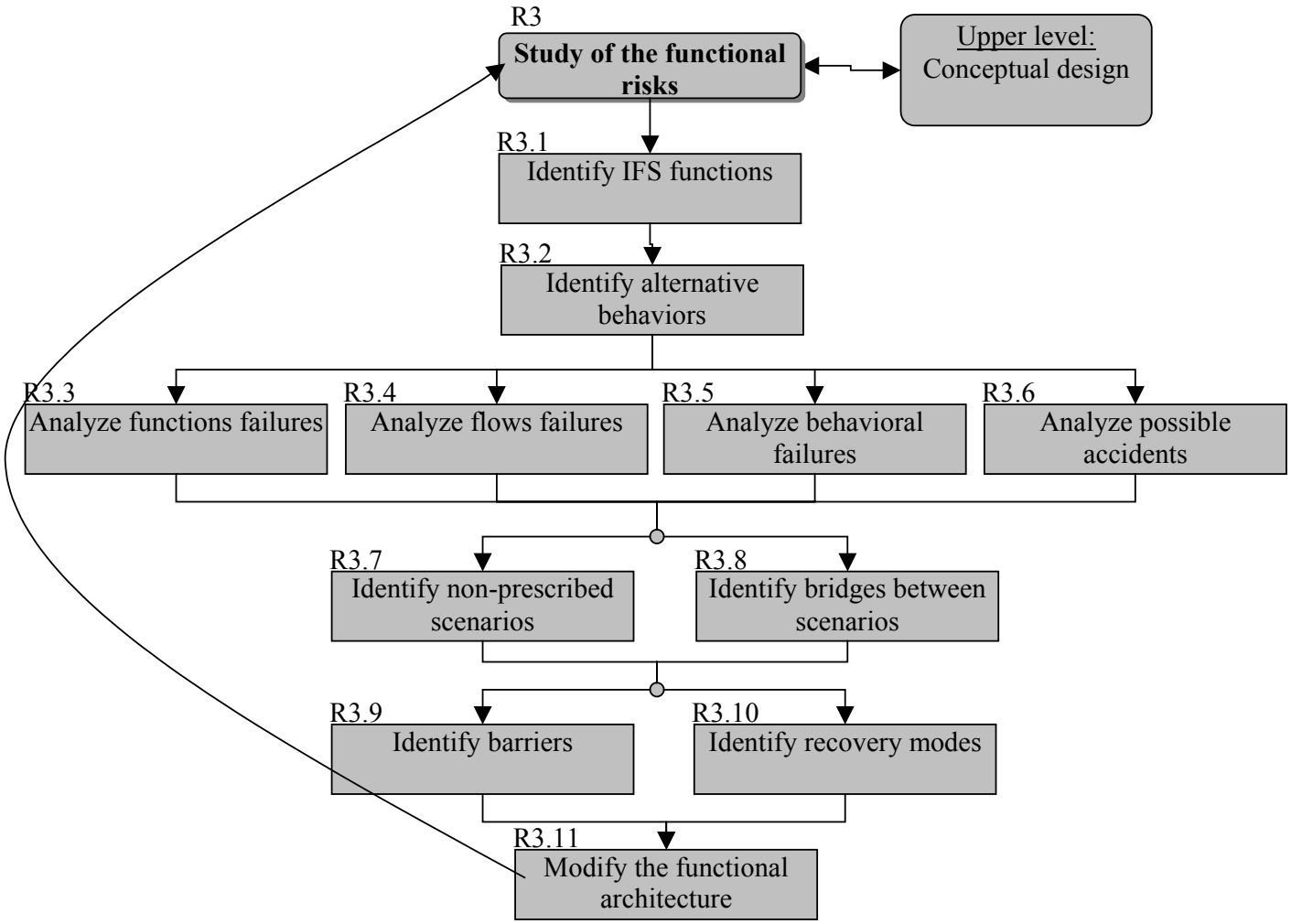
1.5.7 Verification

Verify that the architecture fulfills the requirements, and is compatible with the measures and context of the system. Check if it is necessary to further develop the functional architecture.

1.5.8 Finalize the functional architecture

Combine the architecture, the results of the risk analysis and of the context and requirements studies to obtain the whole functional architecture of the system.

R3 Study of the functional risks



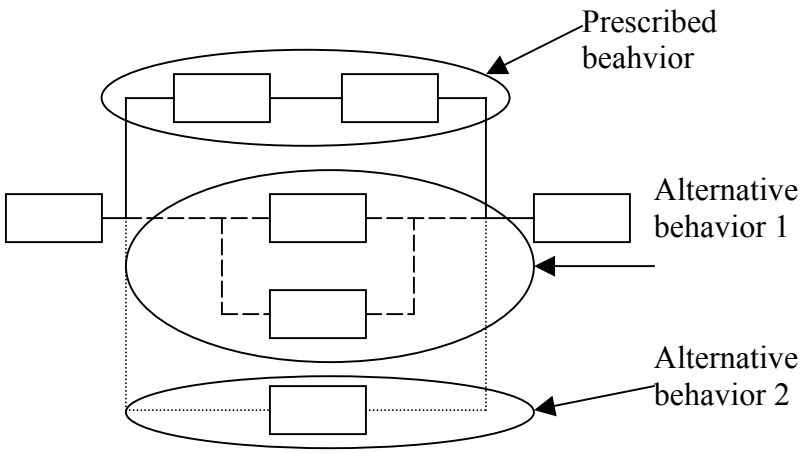
For this activity, a good knowledge of function analysis and FMEA is recommended.

R3.1 Identify IFS functions

Among the functions, identify which ones play an important role for the safety. Those are in particular the one to which IFS requirements have been allocated.

R3.2 Identify alternative behaviors

Identify other behaviors that enable to perform the functions and/or reach their objectives.



R3.3 Analyze function failures

Analyze how IFS functions can fail and the consequences of such failures.

Function	Failure	Cause	Consequence
F1	…	…	…
	…	…	…

R3.4 Analyze flow failures

Analyze how flows from and to the IFS functions can fail.

Flow	Failure	Cause	Consequence
f1	…	…	…
	…	…	…

R3.5 Analyze behavioral failures

Identify how the behavior can fail, for example how a function can be activated at the wrong time.

R3.6 Analyze possible accidents

Identify the possible accidents identified in the previous analyses, and understand their functional origins.

R3.7 Identify non-prescribed scenarios

Identify possible scenarios that do not correspond to the prescribed operations of the system. This includes safe scenarios that can then be considered as redundancy scenarios, and hazardous scenarios.

R3.8 Identifier bridges between scenarios

Understand how the system can move from one scenario to another. This includes of course going from a prescribed scenario to a hazardous one, but also the recovery, going from a hazardous scenario to another one, and going through redundancy scenarios.

R3.9 Identify barriers

Identify barriers that avoid entering a hazardous scenario or maintaining the system in such a scenario.
Verify the independence of those barriers (to avoid common mode failures).

R3.10 Identify recovery modes

Identify how to recover the system when it has entered a hazardous scenario.

R3.11 Modify the functional architecture

The identified barriers and recovery modes will help define new functions that allow a better safety of the system. It can also be interesting to modify the functional architecture to strengthen the safety.

1.6 Preliminary allocation

In order to evaluate the feasibility, it may be required to start thinking of possible allocations. In this case, refer to activities 2.1, 2.3 and 2.4.

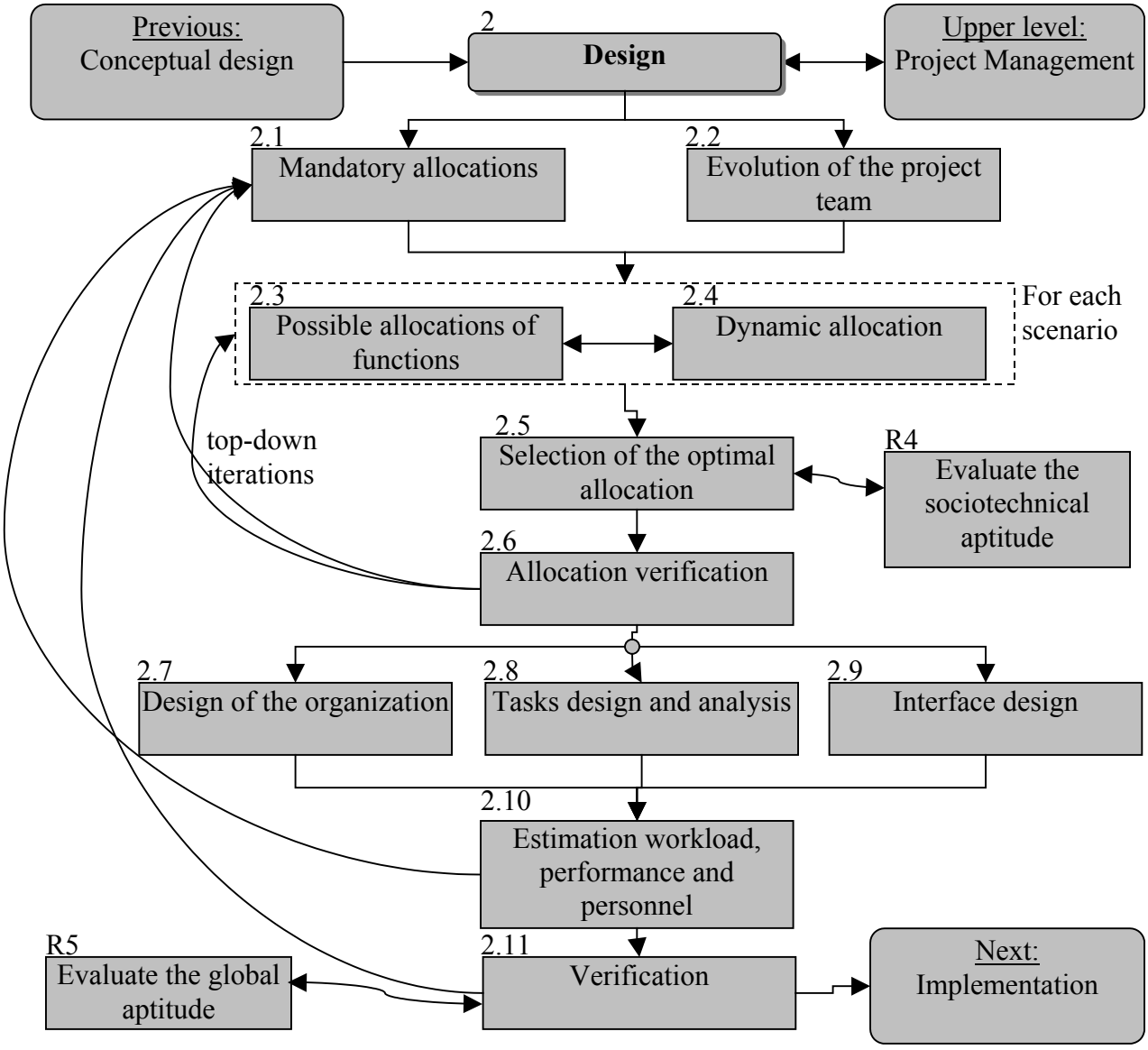
1.7 Verification

We will now check that:

- the sociotechnical context of the project has been well taken into account
- the various sociotechnical aspects have been identified and turned into requirements and functions
- the sociotechnical intervention within the project has been planned:
    - a HFI focus has been identified
    - responsibilities for the six HFI domains are identified or planned
    - the HFI needs during the project are identified
    - guidelines for each HFI domain exist and have been included in the project documents

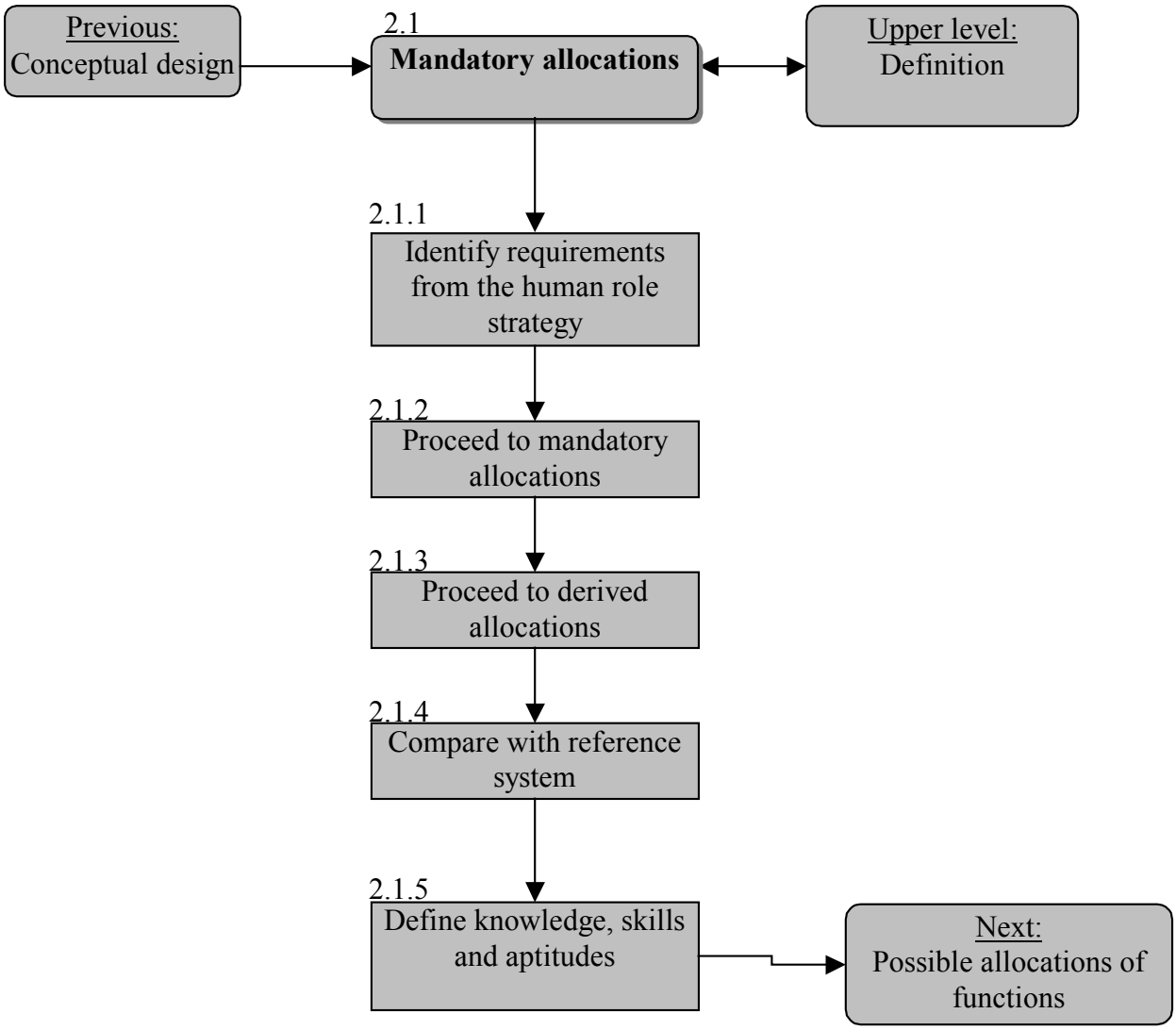
2 Design

The aim of the design phase is to define more precisely the system. In a first time this consists in allocations functions to the right entities of the system, first at a high level the main functions to the main departments, and then by proceeding in a top-down manner until deciding the exact tasks allocated to a given machine and the human in charge of using or maintaining it.
Then, the organization, tasks and interfaces must be designed before estimating the system.



2.1 Mandatory allocations

The allocation of some given functions is mandatory given the constraints identified during the context study and requirements analysis as well as the characteristics of those functions.



This activity requires technical and human skills in the domains related to the concerned functions.

2.1.1 Identify requirements from the human role strategy

Analyze the strategy to determine the impact on function and decision allocation.

2.1.2 Proceed to mandatory allocations

From the requirements, allocate the functions and decisions to the entities of the organization and then the men, machine, software or combination of those.

2.1.3 Proceed to derived allocations

Given the previous allocations, determine the functions that require to be allocated now.

2.1.4 Compare with reference system

Compare with systems identified previously as equivalent. Use this comparison to determine the performance, safety and other characteristics of the present allocation.

2.1.5 Define the required knowledge, skills and aptitudes

Identify the KSAs required from the personnel to which the functions have been allocated.

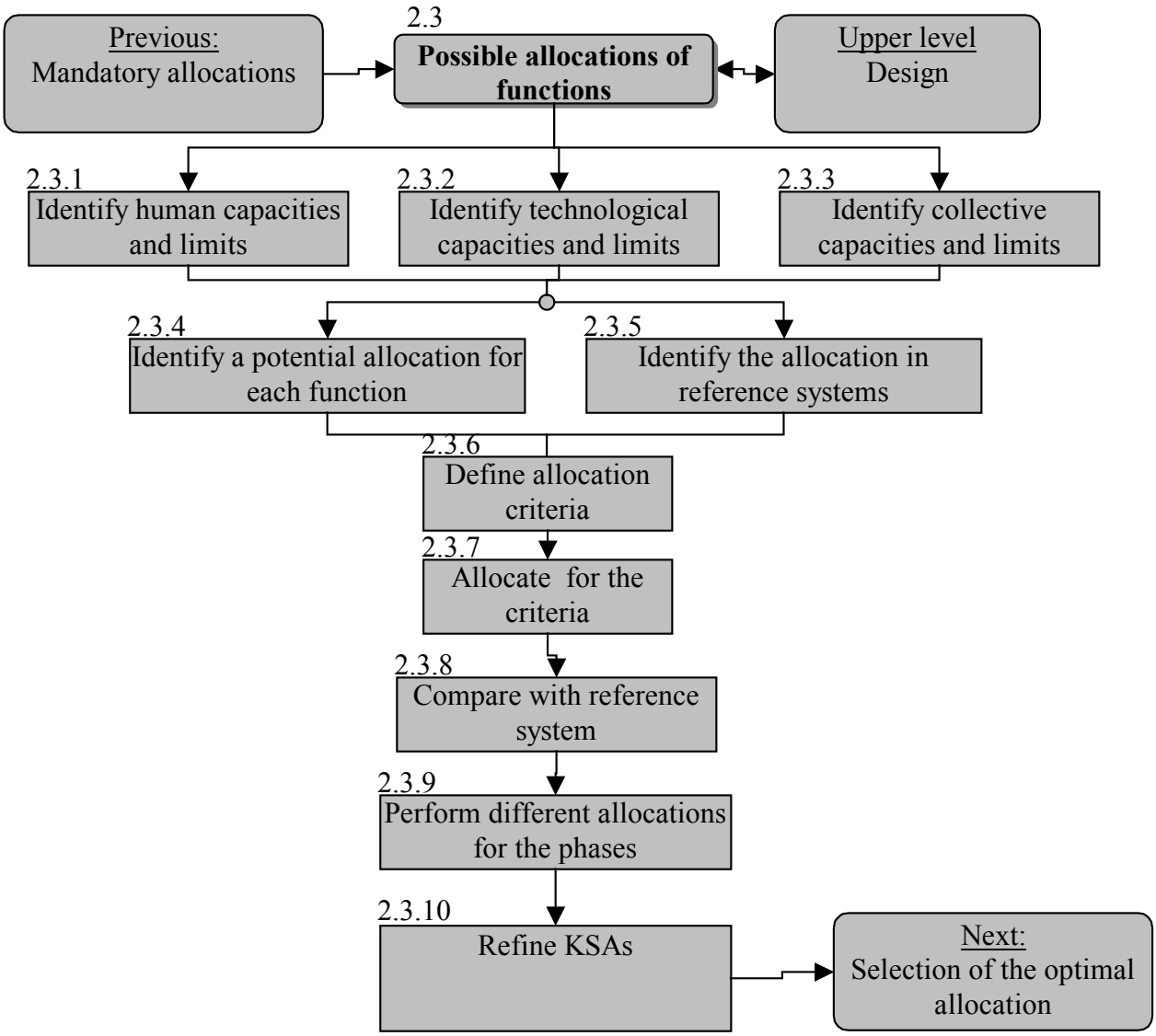
2.2 Evolution of the project team

Given the allocation and KSAs, it can be meaningful to strengthen some skills among the HFI working group.

Furthermore, the allocation enables to evaluate more accurately the tasks and interfaces, and hence to plan more precisely the HFI activities.

2.3 Possible allocations of functions

In this activities different possible allocations will be identified, given human, technical and collective capabilities, and a set of criteria we want to optimize.



The identification of human and collective capacities and limits requires a good background in HF, especially physiology, psychology, sociology or ergonomics depending on the functions. Similarly, the identification of technological capacities and limits requires technical skills.
The definition of allocation consists rather in brainstorming and does not require specific skills. However, people with good technical and/or HF background must supervise this activity.
Task 2.3.10 requires skills in KSA and training management.

For this activity, it is advised to use return on experience and involve future users or users of equivalent systems, which allows a more accurate estimation of human and collective capacities.

2.3.1 Identify human capacities and limits

Identify human models applicable to the concerned context and functions. These models cover among others physical, physiological and cognitive aspects.

2.3.2 Identify technological capacities and limits

Identify technical models applicable to the concerned context and functions.

2.3.3 Identify collective capacities and limits

Identify models of teamwork and human-machine coupling applicable to the context and functions.

2.3.4 Identify a potential allocation for each function

Given the capacities and limits observed previously, evaluate to whom or what each function may be allocated. This consists in eliminating impossible allocations (a machine cannot handle a discussion alone) and to indicate preferences on some allocations (for example to put the human "in command").

2.3.5 Identify the allocation in reference systems

Identify how the allocation has been previously realized in equivalent systems, and eventually the consequences of those allocations if a return on experience exists. Identify how technological, cultural, social etc. evolutions may affect the possibilities for our system.

2.3.6 Define allocation criteria

Determine some priority criteria for which we will propose optimal allocations. These criteria can concern: aptitudes, cost, cognitive support, workload, frequency, training, personnel, safety etc.

2.3.7 Allocate for the criteria

Propose allocations that optimize the criteria.

2.3.8 Compare with reference system

Identify common points and differences with reference systems. This enables us to obtain a first idea of the expectable performance.

2.3.9 Perform different allocations for the phases

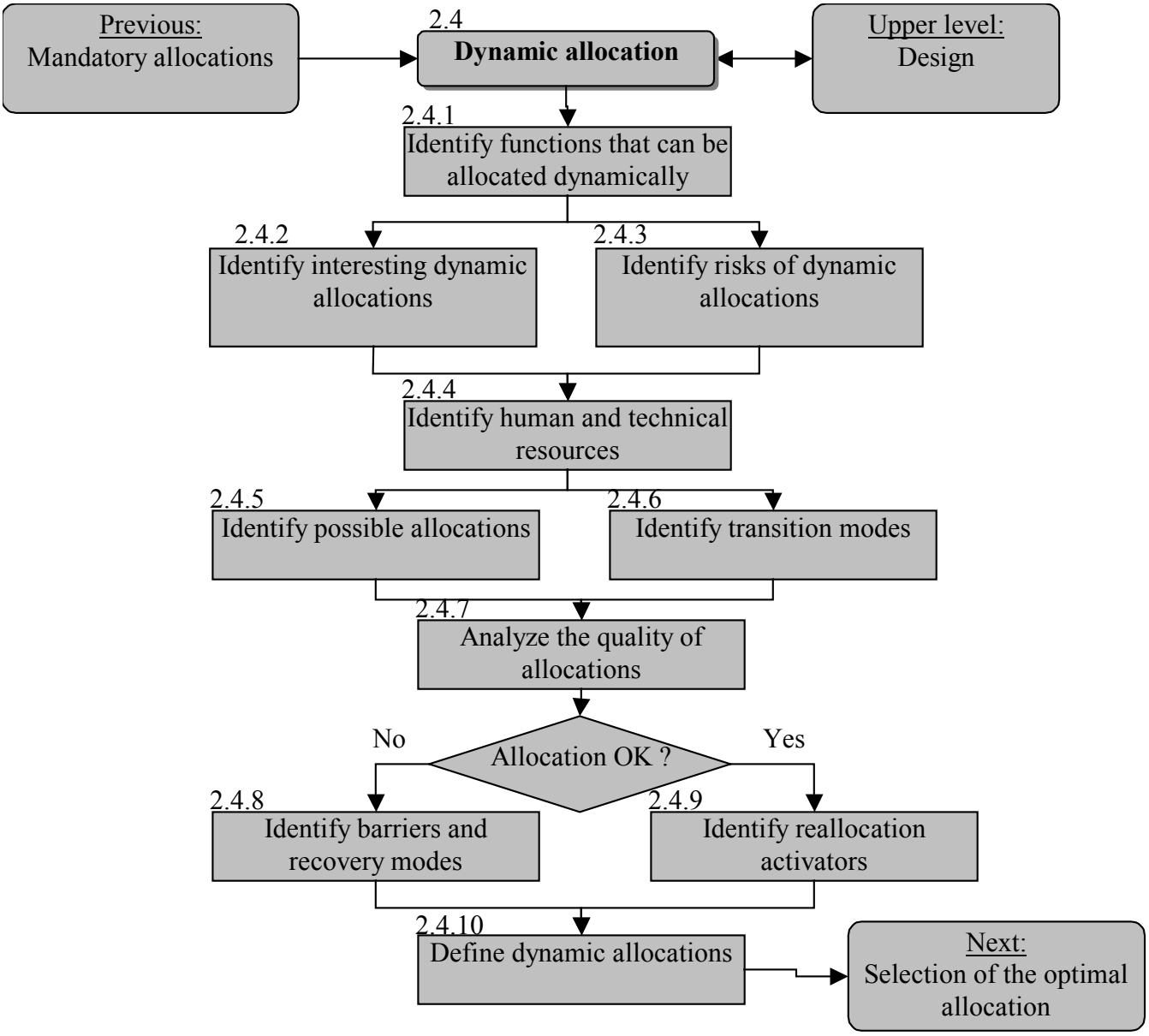
The optimal allocation can depend upon phases or scenarios. In this case, solve the problem either by fixing the most appropriate static allocation, either by using dynamic allocations. Those will be studied in 2.4.

2.3.10 Refine KSAs

Given the proposed allocations, refine KSAs.

2.4 Dynamic allocation

Dynamic allocation is an allocation that evolves between the scenarios and will be decided during operations.



This quite complex activity requires good skills in human factors and human reliability, as well as a fair capacity of innovation as few tools exist.

2.4.1 Identify functions that can be allocated dynamically

Identify which functions do not require having a static allocation, e.g. the ones allocated to several departments, human and/or machines.

2.4.2 Identify interesting dynamic allocations

Among the previously identified functions, identify the ones for which a dynamic allocation presents an interest. This depends on the wanted flexibility, safety, collaboration and polyvalence.

2.4.3 Identify risks of dynamic allocations

Identify for which functions it is possible that the allocation evolves during operations while the design recommended a static allocation. This identification can be based on return on experience as well as on traditional schemes. Reasons may be the research of productivity, a bad definition of responsibilities, etc.

2.4.4 Identify human and material resources

Identify precisely what resources can be allocated to the functions.

2.4.5 Identify possible allocations

Identify the different possible allocations given the resources and functions to perform. This includes allocations in degraded state (person is not there or unable to perform the tasks, very high workload, technical failure…).

2.4.6 Identify transition modes

Identify how it is possible to move from one allocation to another.

2.4.7 Analyze the quality of allocations

Distinguish among the allocations the ones that enable to perform the functions while respecting the requirements and those that cause problems and must be avoided.

2.4.8 Identify barriers and recovery modes

Identify what may prevent to enter an unwanted allocation, or allow coming back to the appropriate allocation quickly and safely.

2.4.9 Identify reallocation activators

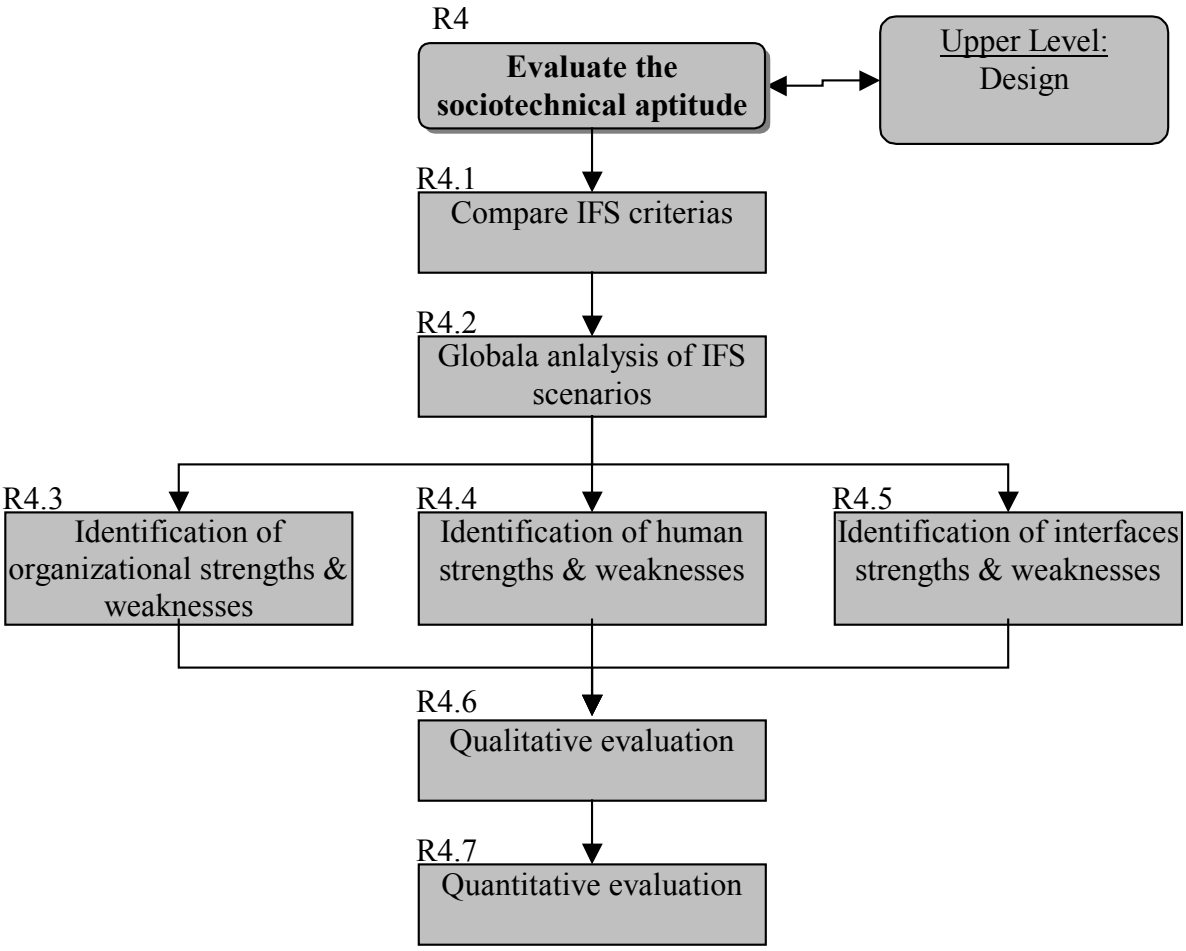
Analyze elements that will drive the allocations, and especially how to be sure that the right allocation will be made at the right time.

2.4.10 Define dynamic allocations

Define the impacts of the dynamic allocations and related studies for the design of the organization, tasks and interfaces.

R4 Evaluate the sociotechnical aptitude

During this activity, the reliability factors and risks related to human factors in the allocations will be studied.



This activity requires knowledge in human and organizational reliability.

R4.1 Compare IFS criteria

Evaluate how the allocation satisfies globally the IFS measures, dimensions, requirements and functions previously identified.

R4.2 Global analysis of IFS scenarios

Study how scenarios and functions are handled through the allocation. Identify the impact of the allocation, and its actual respect, on the aptitude of the system (RAMS).

R4.3 Identification of organizational strengths & weaknesses

Identify the functions allocated to some kind of organizational entity, and their relations with other functions. Evaluate how the allocation contributes to the safety of the system, and identify its weaknesses in terms of safety.

R4.4 Identification of human strengths & weaknesses

For the functions allocated to human, and those in relation, analyze the strengths and weaknesses of the allocation through human reliability aspects (possible errors, capacity to anticipate/recover).

R4.5 Identification of interfaces strengths & weaknesses

For the functions allocated to human/machine couples or to human/human cooperation, identify strengths and weaknesses.

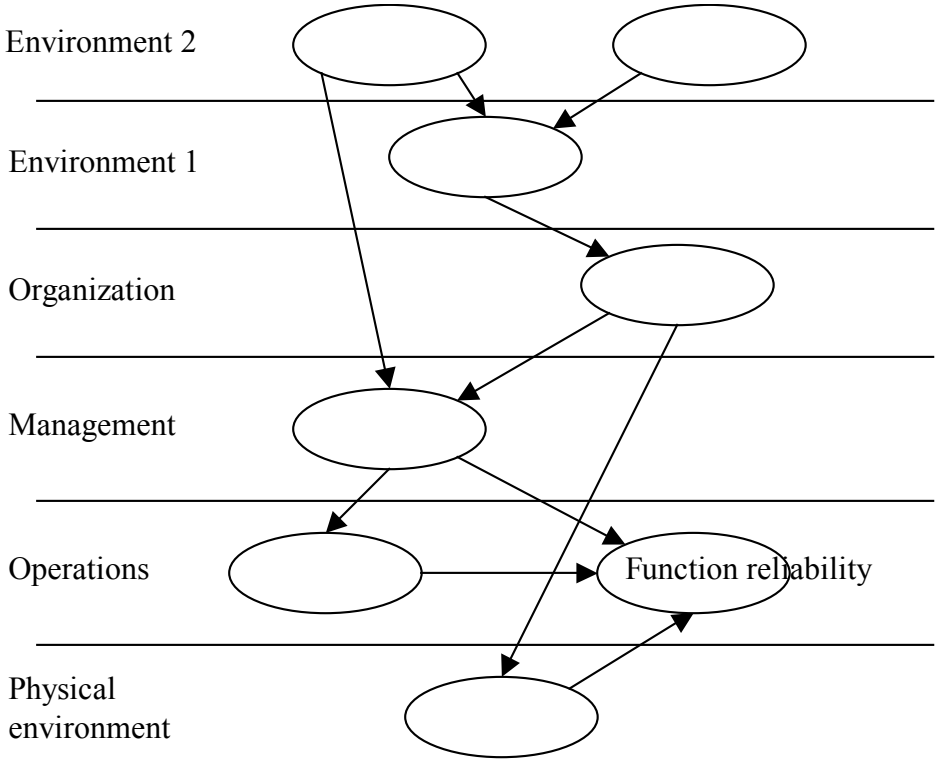
The THEA method (THEA – a reference guide, by S. Pocock, M. Harrison and P. Wright, University of York) can be helpful for activities R4.4 and R4.5, as it helps evaluate the system given the current knowledge about human error while remaining simple enough to evaluate different allocations.

R4.6 qualitative evaluation

From the previously identified points, it is possible to evaluate qualitatively the allocation.

R4.7 Quantitative evaluation

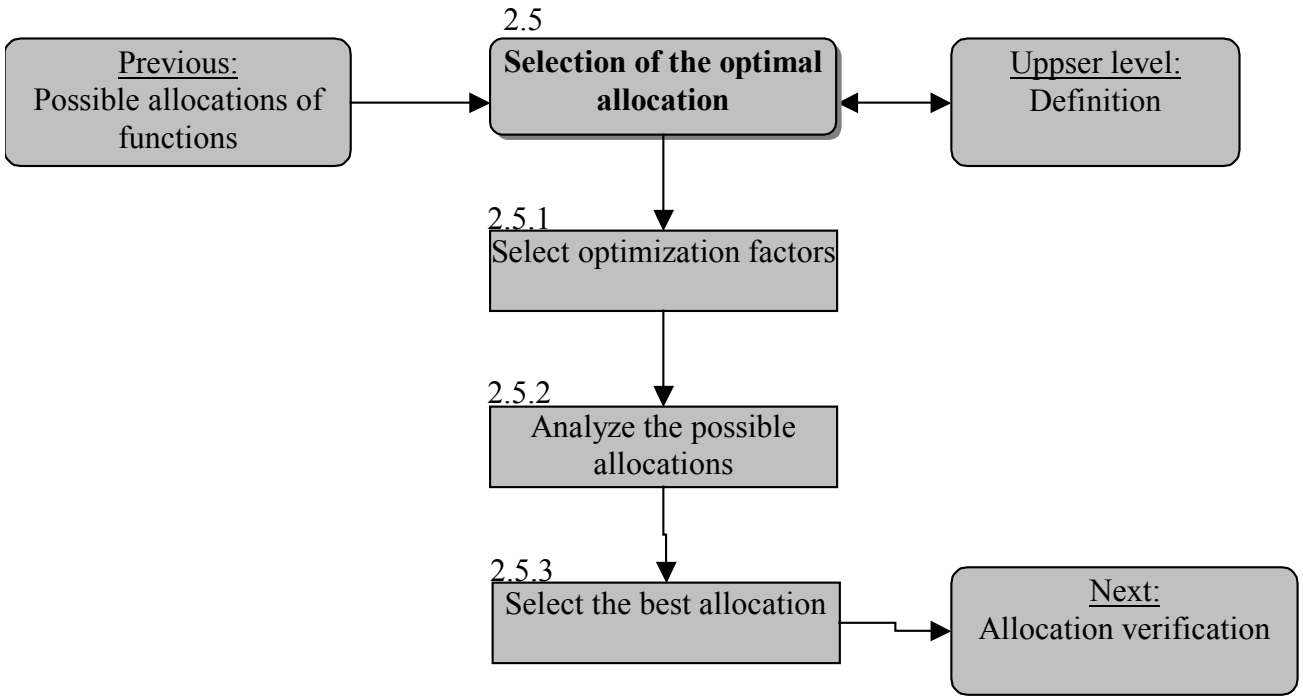
Concerning the most critical functions, a quantitative evaluation can be required. Previous activities of the project have helped obtain a quite complete view of the context of the function, which should allow a quite precise quantification.
Traditional methods can be used for relatively isolated functions. However, in order to take into account the complexity of the system as it has been studied and conceived until yet, influence diagrams and Bayesian networks can be a great help.



Previous analyses concerning the context, organizational dimensions, possible and prescribed scenarios, barriers and dynamic allocations should of course be reused.

If one wishes to quantify one part of the system or the whole system, proceed through the various levels of detail.
The quantification will make good use of return on experience, expert judgment and researches.

2.5 Selection of the optimal allocation



2.5.1 Select optimization factors

Assign a weight to the factors depending on their importance for the system.

2.5.2 Analyze the possible allocations

Evaluate the previously defined allocations through the set of criteria to obtain a global evaluation of each allocation.

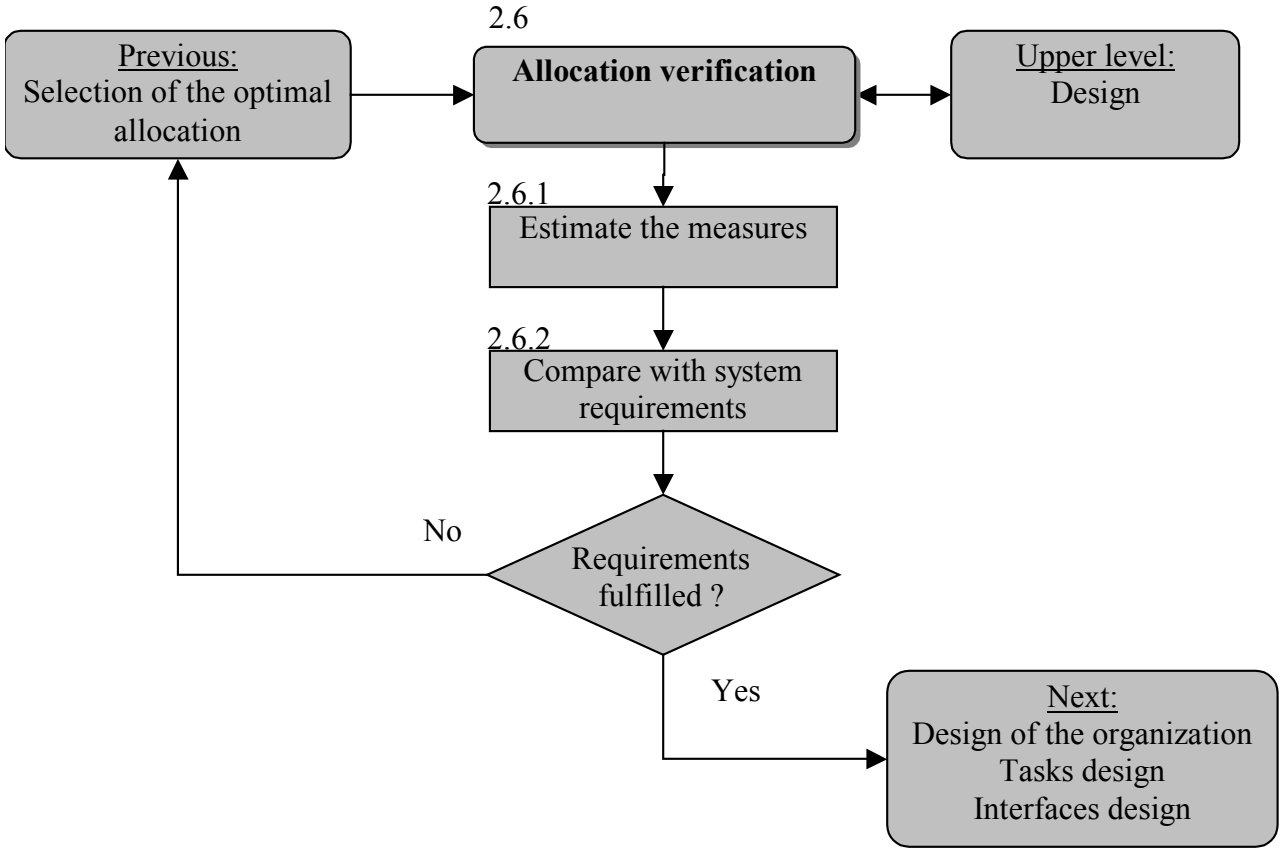
	Criteria 1, weight x	Criteria 2, weight y	Criteria n, weight z	Total
Allocation 1	Value*x=a1c1	Value ***y=a1c2**	Value *z=a1cn	a1c1+…+a1cn
Allocation 2	Value ***x=a2c1**	Value *y=a2c2	Value *z=a2cn	**a2c1+…+a2cn**
Allocation n	Value *x=anc1	Value *y=anc2	Value ***z=ancn**	anc1+…+ancn

The most difficult is to estimate the quality of allocations for a given criteria. For this purpose, expert judgment, return on experience, existing tables and simple methods can be used.

2.5.3 Select the best allocation

Determine which allocation fulfills at best the various criteria.

2.6 Allocation verification



2.6.1 Estimate the measures

Estimate the allocation with the effectiveness and performance measures, IFS criteria and requirements.

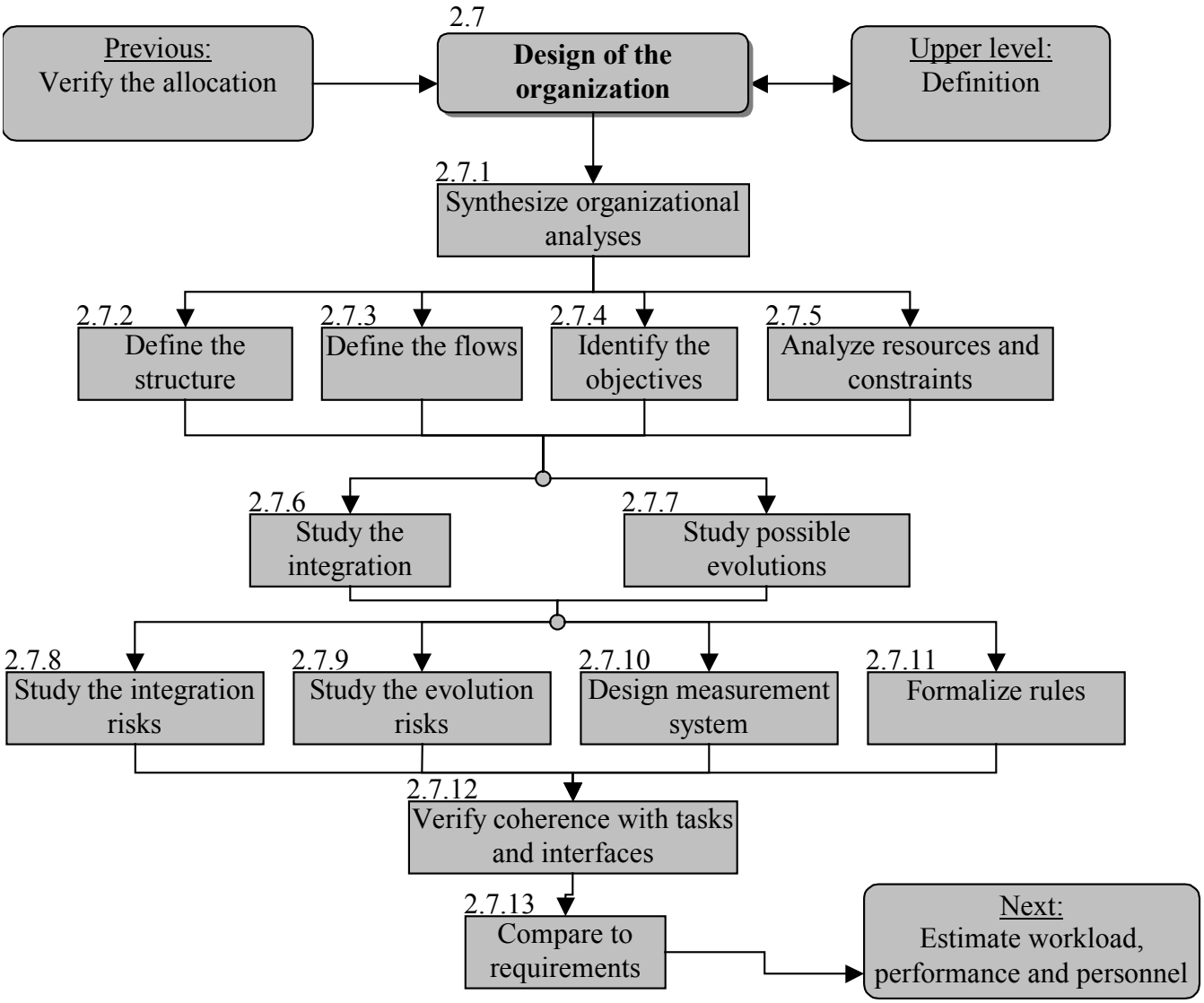
2.6.2 Compare with system requirements

Evaluate the coherence with the system requirements. In case of variance, decide to adapt the allocation and/or the requirements.

2.7 Design of the organization

The goal of this activity is to design the organization. It is performed coherently with the task and interfaces design as those three activities are strongly correlated.

The objective is not only to design the organization as we want it, but also to take into account the fact that an informal organization will develop from the prescribed one, and that the organization will evolve along the system's lifecycle. Hence, the measurement system that will help ensure the system does not become a source of unreliability must also be designed.



This activity requires skills in management and theory of organizations. The resources, evolutions and integration analysis require skills in sociology of organizations. Finally, the second half of the activity requires notions in organizational reliability.

2.7.1 Synthesize organizational analyses

Regroup the previous analyses concerning the organization (context, organizational specification, requirements and allocation).

2.7.2 Define the structure

Define the organizational structure.

2.7.3 Define the flows

Define the dynamics of the organization through information and resources flows.

2.7.4 Identify the objectives

Define the organizational aspects related to the objectives to reach and required tasks.

2.7.5 Analyze the resources and constraints

Evaluate the potential for each entity of the organization. This will help think later on possibilities of informal organization.

2.7.6 Study the integration

Study how the organization will interface with the existing organization. Identify how to adjust the two at their best to ensure the required coherence and a good organizational reliability.

2.7.7 Study the possible evolutions

Identify how the real organization can deviate from the designed organization.
This implies on one hand to identify power games and other actor strategies that are likely to develop given the resources and constraints as well as the return on experience, in order to evaluate probable informal organizations.
On the other hand, evaluate how the organization may deviate from its principles and initial vision (especially through escalation, simplification and deviance).

2.7.8 Study the integration risks

Analyze how the integration may not turn out well, and what risks this represents on the long term (how an evolution in the existing organization or designed system may have negative consequences on the other).

2.7.9 Study the evolution risks

Evaluate how the possible evolutions can reduce the organizational reliability.

2.7.10 Design measurement system

Given the previously identified measures and risks linked to the evolutions, design a set of metrics and the way to manage the measurement. this consists in a scorecard what will allow to observe the "health" of the system in operations and detect deviances (before they "normalize").
This includes the identification of whom or what will be in charge of measuring, displaying and analyzing the measures.

2.7.11 Formalize rules

Identify the minimum requirements to ensure organizational reliability, and formalize. those rules will help ensure that no mistakes are made in future evolutions of the system.

2.7.12 Verify coherence with tasks and interfaces

Ensure that the analysis of tasks related to the organization as well as required collective interfaces are performed, and that everything is coherent.

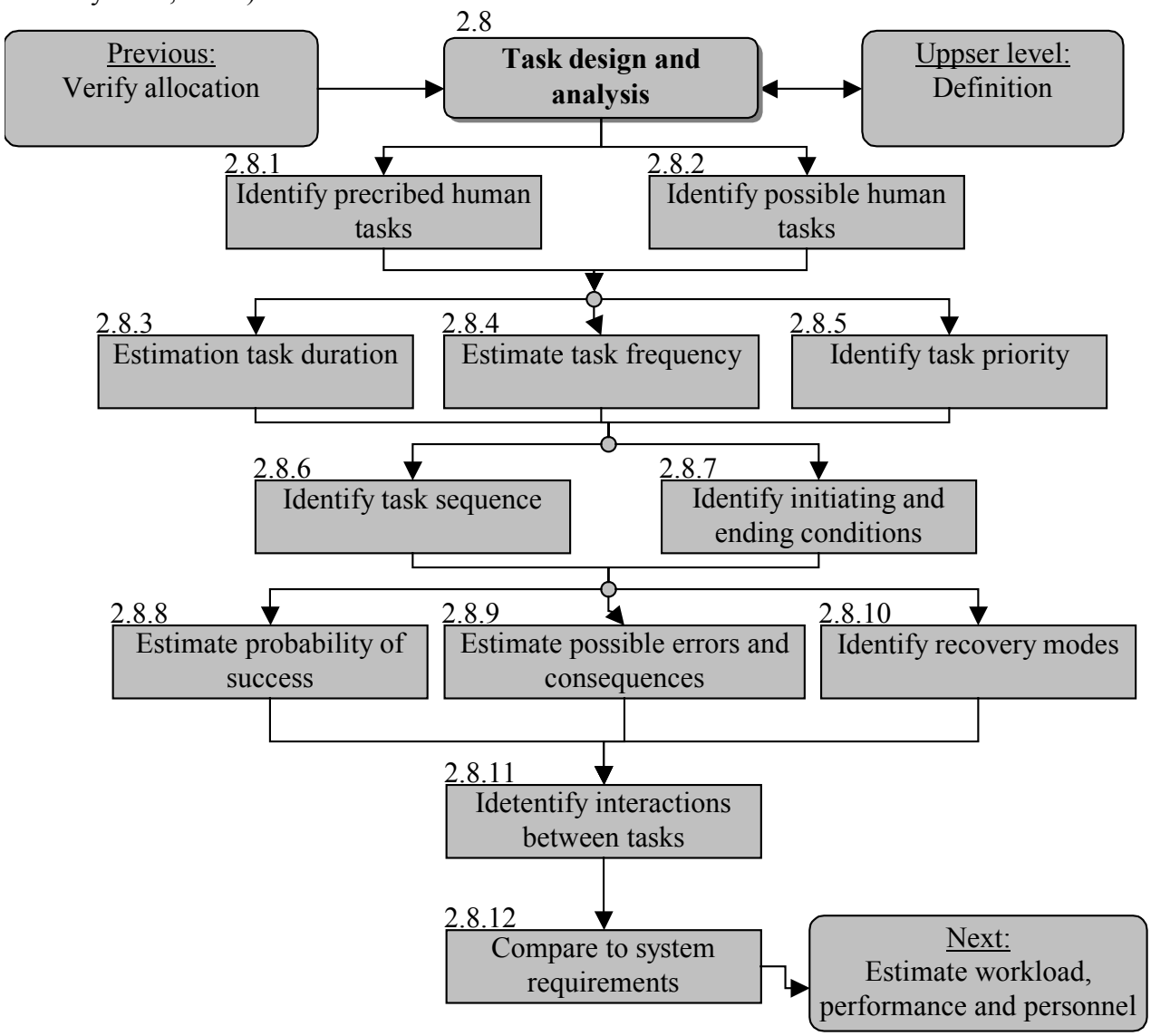
2.7.13 Compare to requirements

Verify that the organization respects the requirements.

2.8 Task design and analysis

During this activity we will design and analyze the tasks. That concerns of course the tasks required for the good operations of the system, but also those that ensure safety barriers or recovery.

In the case of relations with the environment, it may be necessary to study also some tasks required from it (for example the customers) so that they can get the service. Those must be analyzed, while keeping in mind that the model applicable to customers is not the same as the one for employees (no training, lower acceptation of physical and cognitive workload, lower respect of safety rules, etc…).



2.8.1 Identify prescribed human tasks

Identify tasks that will be performed by humans (my they be operators, managers, maintainers or users). This includes mission tasks and support ones, either physical or cognitive (including the one used for reallocation).

2.8.2 Identify possible human tasks

Identify tasks that could be developed in operations to replace prescribed tasks. To this purpose, the work done on functional risks and dynamic allocations must be reused.

2.8.3 Estimate task duration

Estimate the average duration and duration variances required to perform the tasks.

2.8.4 Estimate task frequency

Estimate the frequency and rate of occurrence.

2.8.5 Identify task priority

Estimate the priority of tasks given the systems mission and the global performance. Estimate also the priority that is likely to be given by the task performers, the possible impact of the gap between those two variances and the ways of reducing them or their effects.

2.8.6 Identify task sequence

Identify the sequence of tasks and coordinate with the functions allocated to machine or software.

2.8.7 Identify initiating and ending conditions

Identify the information, actions and events required for a task to start, continue or stop.

2.8.8 Estimate the probability of success

Identify the probability of success and precision of a task.

2.8.9 Estimate the possible errors and their consequences

Identify the possible error types that can occur and their effects on the system.

2.8.10 Identify recovery modes

Identify and analyze tasks and functions that enable a recovery.

2.8.11 Identify interactions between tasks

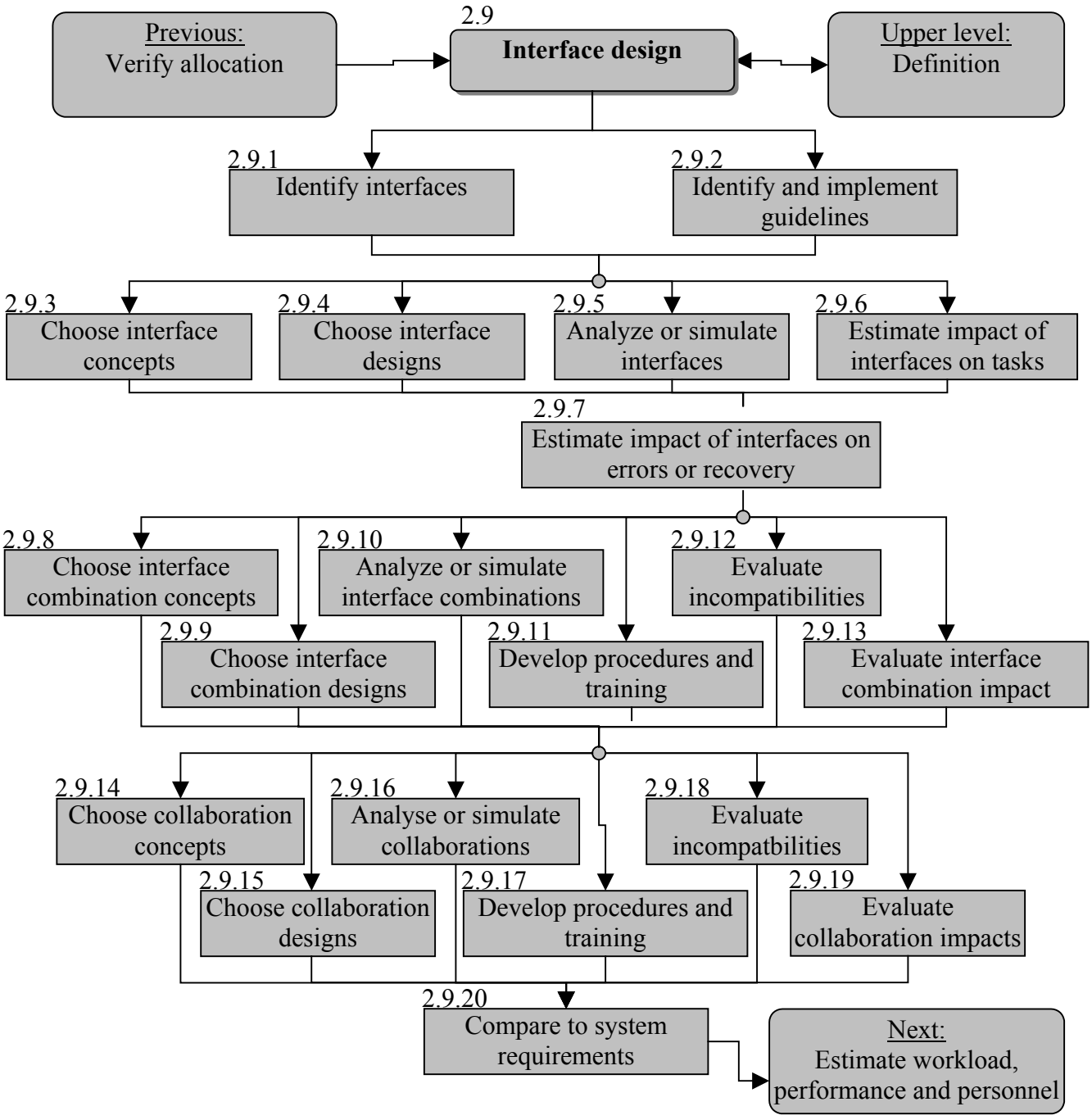
Identify interactions between tasks and external factors. Identify how the presence or absence of inputs or outputs can alter the flow of operations. This includes the identification of task overlaps and waiting times as well as interactions with functions allocated to the hardware or software.

2.8.12 Compare to system requirements

Verify that the tasks respect the requirements.

2.9 Interface design

This activity consists in designing interfaces. Those interfaces can be either human-machine or human-human or even team-team. Not only internal interfaces but also the ones with the environment (including with the customers) must be analyzed.



This activity requires skills in ergonomics, management and eventually sociology for the collaborations.

It is highly recommended to involve future users and perform simulations, including "group simulations". In some cases it is also advised to involve future customers and other people of the environment (service suppliers etc…) to evaluate the interfaces with the environment.

2.9.1 Identify interfaces

Identify the points in the functional architecture where information / objects are exchanged between humans or with the equipment.

2.9.2 Identify and implement guidelines

Identify existing guidelines applicable to interfaces. Those guidelines may concern among others memory limitations, display and control modalities, and physical limitations.

2.9.3 Choose interface concepts

Identify the most appropriate interface concepts.

2.9.4 Choose interface designs

Identify the various designs satisfying the chosen concept, and select the most appropriate one.

2.9.5 Analyze or simulate interfaces

Test interfaces. This can be done by using prototypes, human models, software simulations etc.

2.9.6 Estimate impact of interfaces on tasks

Determine how the selected interfaces will affect human performance.

2.9.7 Estimate impact of interfaces on errors and recovery

Evaluate the capacity of interfaces to limit errors and help recovery.

2.9.8 Choose interface combination concept

Compare and select a concept of interface combination. By combination we mean a workstation or work environment.

2.9.9 Choose interface combination designs

Identify the most appropriate design. Think especially in terms of compatibility to avoid confusions.

2.9.10 Analyze or simulate interface combinations

Test interface combinations

2.9.11 Develop procedures and training

Start developing the procedures and instructions. If possible, include those in the interfaces or work environment.

2.9.12 Evaluate incompatibilities

Identify incompatibilities between interfaces and solve them.

2.9.13 Evaluate impact of interface combinations

Determine how interface combinations may impact task performance and safety.

2.9.14 Choose collaboration concept

Choose from the different concepts for the design of team interactions.

2.9.15 Choose collaboration designs

Choose the most appropriate design for collaborations.

2.9.16 Analyze or simulate collaborations

Test the design.

2.9.17 Develop procedures and training

Start developing procedures and training associated with the team interactions. If possible, facilitate the integration of those in the interactions.

2.9.18 Evaluate incompatibilities

Identify and resolve incompatibilities between interfaces, interface combinations and collaborations.

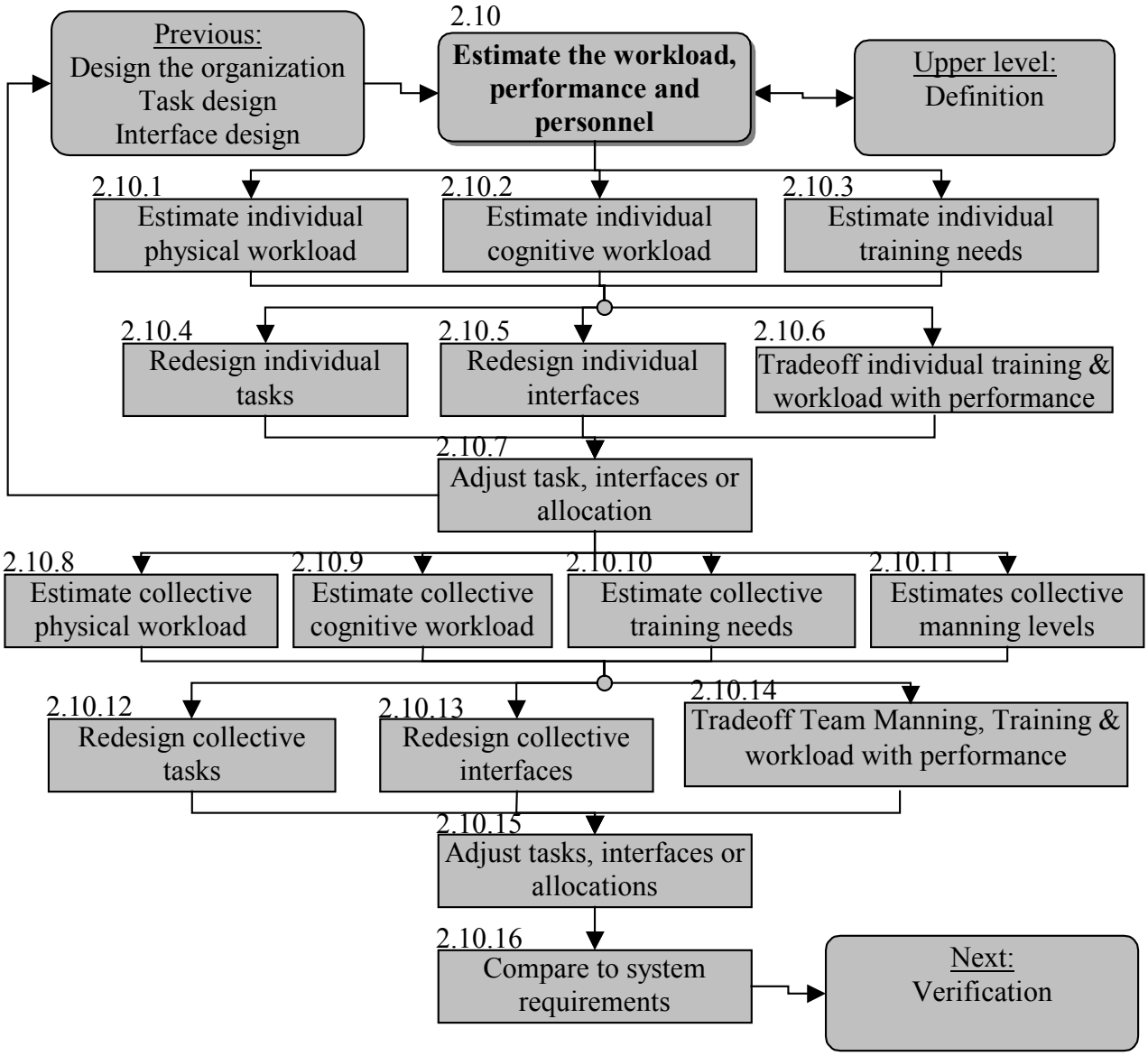
2.9.19 Evaluate the impact of collaborations.

Evaluate how collaborations may impact the performance.

2.9.20 Compare to system requirements

Compare the design with systems requirements.

2.10 Estimate workload, performance and personnel



Skills in ergonomics / task analysis are required for this activity.

The knowledge of the system acquired in the previous steps gives a good overview of the activity, both context, tasks, decisions and required interactions. This enables a more precise analysis, especially of strategies and cognitive resources implied (for example using Cognitive Work Analysis).

2.10.1 Estimate individual physical workload

From the tasks assigned to individuals, determine the physical load. Identify limit levels for the various mission scenarios (take into account the context).

2.10.2 Estimate individual cognitive workload

Similarly, determine the cognitive load.

2.10.3 Estimate individual training needs

Determine the training required to develop the necessary KSAs.

2.10.4 Redesign individual tasks

Identify and redesign tasks that require an unacceptable workload (too high or too low).

2.10.5 Redesign individual interfaces

Identify and redesign interfaces responsible for an unacceptable workload.

2.10.6 Tradeoff individual training & workload with performance

Estimate the relation between workload, performance and associated training costs. Find an optimal solution.

2.10.7 Adjust tasks, interfaces and allocation

Change tasks or functions requiring unacceptable workloads by consolidating, eliminating, simplifying or allocating to other human or machines.

2.10.8 Estimate collective physical workload

For the tasks allocated to teams, estimate the physical workload on each individual and on the team as a whole.

2.10.9 Estimate collective cognitive workload

Proceed similarly for the cognitive workload.

2.10.10 Estimate collective training needs

Estimate the training required for teams to have sufficient performance.

2.10.11 Estimate collective manning levels

Estimate the manpower resources required.

2.10.12 Redesign collective tasks

Identify and redesign collective tasks requiring too important load or needs.

2.10.13 Redesign collective interfaces

Identify and redesign collective interfaces requiring too important load or needs.

2.10.14 Tradeoff Team Manning, Training & Workload with performance

Estimate the impact between workload and performance, and the associated manpower and training costs. Find an optimal solution.

2.10.15 Adjust tasks, interfaces or allocation

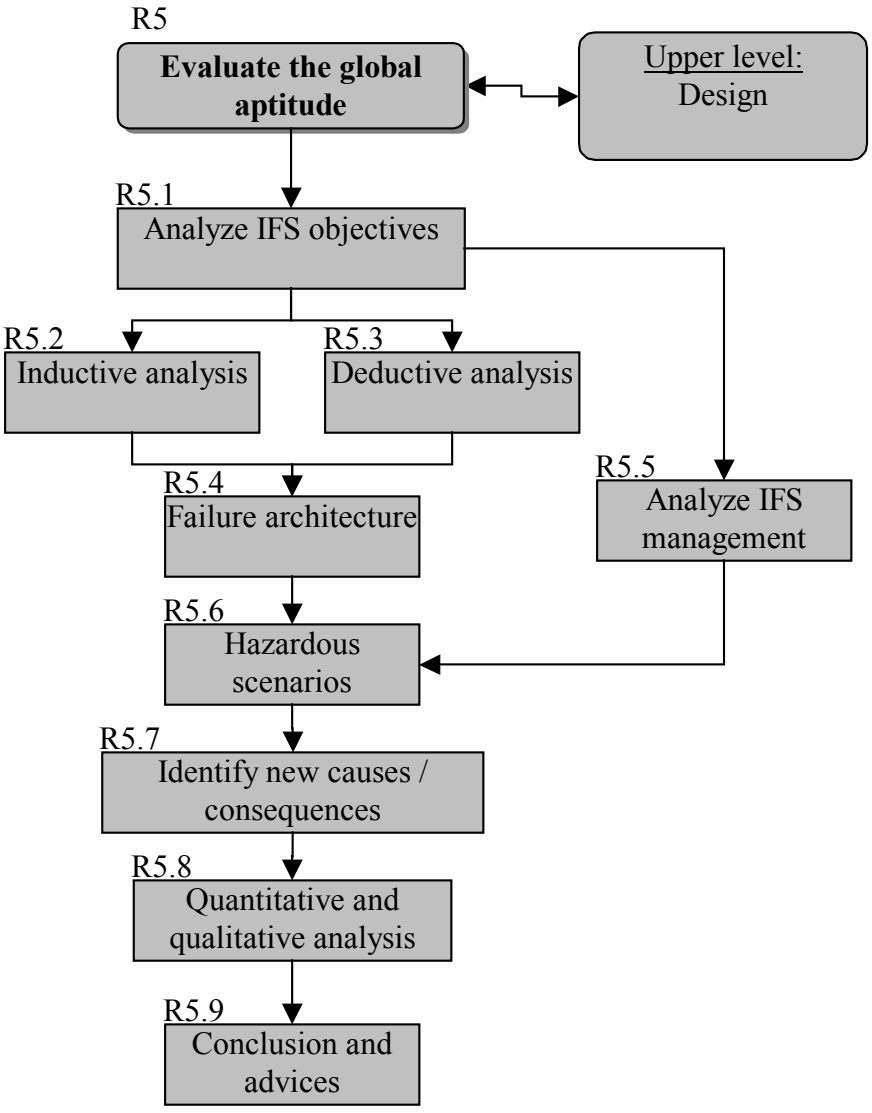
If the workload or needs are too high, redesign by consolidating, eliminating, simplifying or reallocating.

2.10.16 Compare to systems requirements

Verify that the design respects the requirements.

R5 Evaluate the global aptitude

Data from the previous analyses will be compiled here.
The evaluation can be either qualitative or quantitative.



Skills in RAMS are required for this activity.

In order to adopt a structured approach, we can consider that there are two kinds of problems: identified and unidentified, and similarly two kinds of causes.

	Identified problem	**Unidentified problem**
Identified cause	The safety of the system has been progressively built. Its reliability can be estimating by ensuring that the IFS objectives / functions are well identified.	As the cause is identified, we must check the IFS objectives/functions.

Unidentified cause	We will identify the capacity of the system to adapt / recover thanks to the barriers, redundant behaviors, recovery modes etc.	Here we will study what enables the safety to be maintained, i.e. the safety (or risk) management (IFS organizational dimensions, measurement system, safety culture…).

If the previous studies have been well done, normally the remaining work is to complete the studies at the micro-level (technical and human reliability) and to ensure than no important scenario has been missed.

R5.1 Analyze IFS objectives

The objectives identified as IFS and their importance are synthesized.

R5.2 Inductive analysis

Adopt an approach that starts from the cause to identify the consequences.
The causes can be found in:

- incoming relations
- objective activation problems
- objective understanding problem
- objective reaching problem
- resources problems
- allocation problems

Those different causes have been studied previously and detailed along the project.

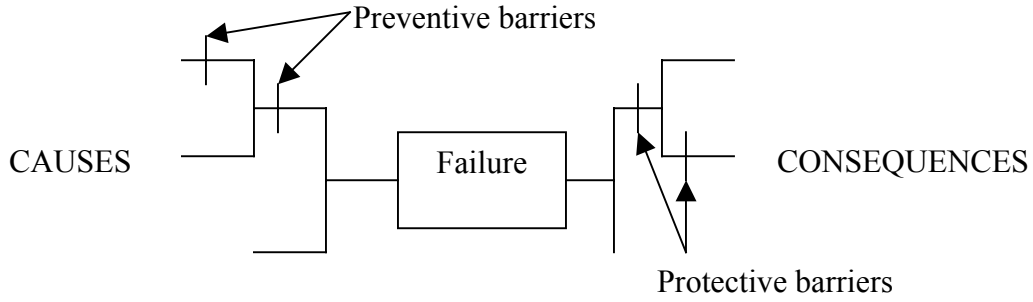
R5.3 Deductive analysis

Adopt the opposite approach: start from the failures to identify the causes.
Possible failures can be identified thanks to:

- outgoing relations
- measures
- objectives
- requirements
- hazard sources

R5.4 Failure architecture

Combine the results of the previous steps to obtain an overall view.



R5.5 Analyze IFS management

The IFS management will ensure that the IFS objectives are continuously reached, it represents the major barrier against unidentified problems.
We will especially evaluate what has been embedded in the design concerning:

- managing and maintaining the IFS requirements, especially organizational dimensions and barriers
- the measurement system that helps identify a reliability loss in the system
- return on experience

R5.6 Hazardous scenarios

From the architecture of failure, identify hazardous scenarios and recovery modes.

R5.7 Identify new causes / consequences

Identify new causes for going from a prescribed or possible scenario (non-prescribed but which could develop through dynamic allocation, informal organization or task modification) to a hazardous scenario, causes for non-recovery and for going from one hazardous scenario to another of different criticity.

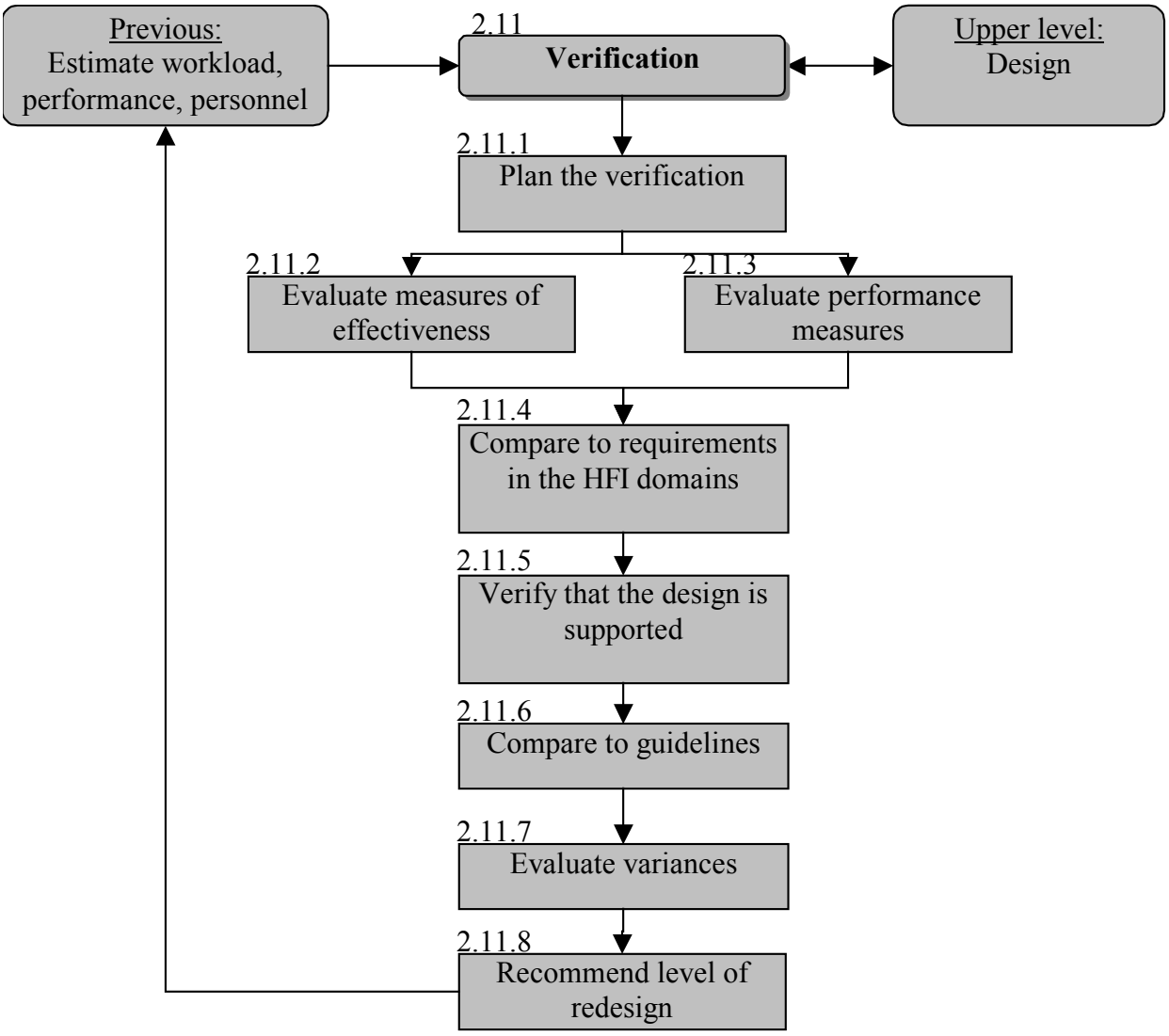
R5.8 Qualitative and quantitative analysis

From the architecture it is possible to perform a quite complete qualitative analysis of the system. Its main interests rely in the number of parameters that can be integrated, especially in terms of organization, in the integration of non-prescribed scenarios and allocation and the evolutions between scenarios, and in the integration of the dynamics of the system and its environment.

R5.9 Conclusion and advices

Conclude on the aptitude of the system and propose redesigns if necessary.

2.11 Verification



2.11.1 Plan the verification

Plan the tests, simulations and demonstrations that will help ensure the system meets the system requirements and HF guidelines. Plan also the verification activities to be performed once the system is deployed.

2.11.2 Evaluate measures of effectiveness

Verify that the system meets the measures of effectiveness.

2.11.3 Evaluate performance measures

Verify that the system meets the performance measures.

2.11.4 Compare to requirements

Verify that the system meets the requirements.

2.11.5 Verify that the design is supported

Verify that the system we designed or made evolve will function correctly with the designed tasks, interfaces, resources and organizations.

2.11.6 Compare to guidelines

Verify that the system does not conflict with the HFI guidelines.

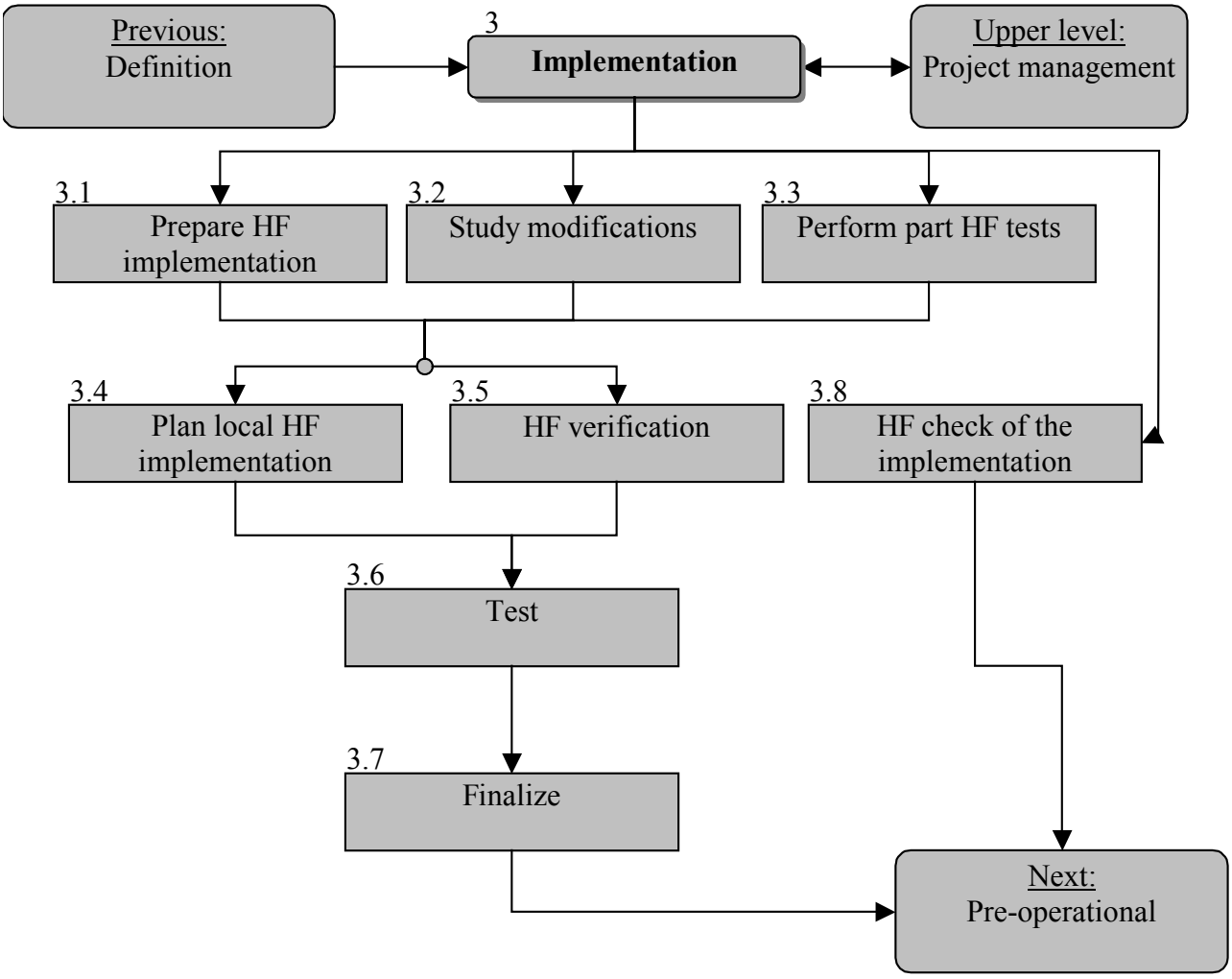
2.11.7 Evaluate variances

Evaluate where the design is in conflict or deviates from the above criteria.

2.11.8 Recommend degree of redesign

Compare costs and benefits of redesign strategies with the risks of not redesigning and recommend the appropriate level of redesign.

3 Implementation



3.1 Prepare HF implementation

Plan the implementation of human aspects of the systems. This implies to:

- plan how the organization will be put in place, and especially the work of preparation in the current system
- prepare trainings
- prepare recruitments or transfers
- prepare KSAs tests
- Write procedures (involve future users)

3.2 Study modifications

Study how the modifications brought to the design impact the performance. In case of a long-term project, evaluate the possible impact of context modifications.

3.3 Perform part HF tests

As the interfaces are created, let them test by future users to verify the previous assumptions.

3.4 Plan the local implementation

Plan specific actions in case a system is to be deployed in several places. It is also the right time to allocate the tasks to the persons with the right KSAs.

3.5 HF verification

Check that everything relevant to the HFI domains has been done, i.e. that the system can be functional.

3.6 Test

Test the training, procedures, interfaces and acceptance.

3.7 Finalize

Ensure coherence and completion of HF integration.

3.8 HF check of the implementation

Ensure that the implementation is done in respect of HF aspects, especially safety and physical workload.

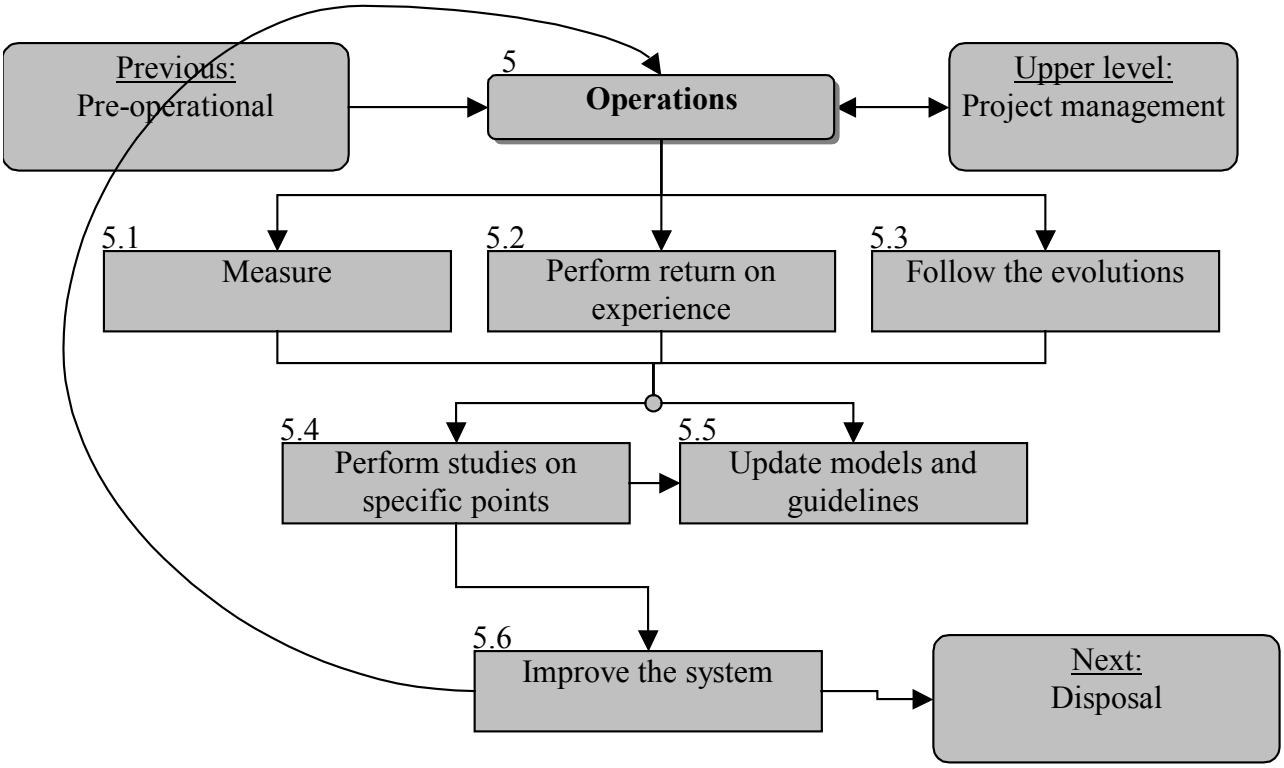
4 Pre-operational

This phase is the occasion to make a point on the project.
This has many interests:

- Evaluate strengths and weaknesses of the HFI method in order to improve it
- Identify positive HF actions and those with problems, in order to give ideas and recommendations for future projects. If new methods have been identified or developed, reference them.
- Estimate the advantage of the method, in order to advertise it among potential users.
- Evaluate the integration of HF, to enable an auto-evaluation of project team members and improve their experience and skills.
- Document the HF integration to serve as an example for future projects. The return on experience between the methods used during the project and the performance in operations may help identify the factors of reliability in projects.

To sum up, make a synthesis in order to improve the skills in the company and provide other projects with a base for improvement.

5 Operations



5.1 Measure

Measuring helps evaluate the "health" of the system. A good measurement system allows the earliest diagnostic of negative variances and deviances of the system to understand and solve them. The identification of positive variances is also an occasion to identify "good practices" and build better future systems.

Two phases can be planned:

- One of detailed measurement right after putting the systems in operations, and to evaluate later the impact of changes or study a specific point
- One of "normal" measurement, less consuming in terms of resources, to evaluate the health of the system during normal operations

It is important to respect a given number of principles:

- many variances are only noise, and cannot be managed nor analyzed. Hence, it is necessary to distinguish meaningful variances by using techniques like SPC.
- do not conclude to quick: a variance does not necessarily indicate what was planned or identified at first sight. It is necessary to understand the meaning of a measure (be careful with raw numbers and proportions)
- measures are not fixed once the measurement system is built. Some may not be adapted, for others the mode of measurement is maybe inappropriate. It is important in a first time

to analyze the pertinence of measures in order to make them evolve. The idea is to obtain the set of measures that helps evaluate most accurately the safety of the system.

5.2 Perform return on experience

Perform a return of experience on incidents (and also "near-misses"). Encourage the personnel to report the incidents.

5.3 Follow the evolutions

The idea is to observe the "natural" and "forced" evolutions of the systems.
By "natural" evolution we mean the way the system evolves from itself along its lifecycle. Keeping a good understanding of the system is essential, especially by understanding the informal organization and unplanned behaviors that develop.
By "forced" evolution we mean the projects that generate changes in the system. It is necessary to evaluate their potential impact of the system to avoid deterioration, as well as their real impact to manage it and gather information for future projects.

5.4 Perform studies on specific points

When the measurement, return on experience or observation of evolutions highlight surprising things, it may be necessary to understand their causes.

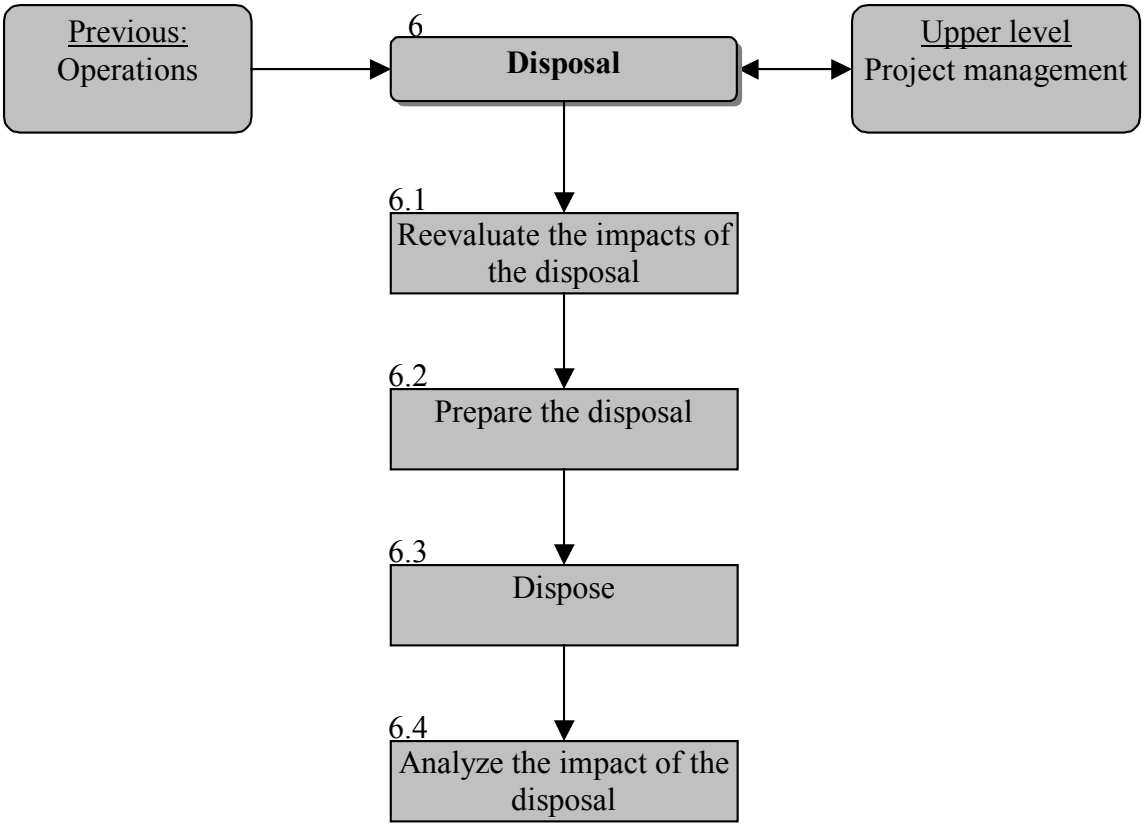
5.5 Update models and guidelines

The observation and study of the system helps improve the knowledge of systems. This knowledge may be used efficiently for the success of future systems.

5.6 Improve the system

Thanks to the measurement and studies, it is possible to propose improvements. Close the loop by studying the impact of those improvements to allow a continuous improvement.

6 Disposal



6.1 Reevaluate the impacts of the disposal

Evaluate the modifications brought by the disposal of the disposal on the related systems, personnel and customers.

6.2 Prepare disposal

Ensure that the necessary HF actions are performed to allow the disposal. Two aspects are to consider, on one hand the actions required for the disposal, and on the other the ones consequent to the disposal (procedures to modify, personnel to transfer, communication).

6.3 Dispose

Proceed to the disposal of the system.

6.4 Analyze the impact of the disposal

Gather knowledge for future systems.

Glossary

Allocation: The act of assigning functions or decisions to components of the system. Functions can be allocated to three kinds of components: hardware, software or human, or any combination of those components. The allocation can be dynamic if it evolves during the operations of the system.

Characteristics of the organization: Parameters that enable to characterize globally an organization. Some examples of characteristics are presented in activities 1.1.6 and 1.1.12.
One interesting reference is : NEA (1999) Identification and assessment of organisational factors related to the safety of NPPs : State of the art report

Degraded mode: State of the system in which it does not respect some requirements anymore, which makes it accident-prone.

Degraded situation: Period of time during which a system is in degraded mode.

Failure mode: It is the way that a component or group of components of the system fails, i.e. how it deviates from the requirements.

Functional architecture: The arrangement of functions, sub-functions, functions interfaces that define the behavior, control conditions, flows and required performances in order to meet the system requirements.

Human factors: Human factors represent every element related to humans as well as their interactions with one another and with the system in which they are integrated.

Human reliability: Capacity of a human to perform a given task in a given context while respecting the corresponding requirements, or to recover a system in a degraded state.

IFS: Important for the System. An IFS element is an element that impacts the system, through the risk it represents or the barrier it provides in regard of the realization of objectives. If one wants to focus on safety, IFS can then be understood as Important for Safety.

Measure of effectiveness: A measure that helps determine to which extent the system meets its objectives.

Mission scenario: Set of activities started in order to reach a given objective in a given context.

Performance measure: The measure of aspects required to meet a measure of effectiveness. There are usually several performance measures for one measure of effectiveness.

KSAs: Knowledge, skills and aptitudes. Characteristics required of an individual to perform a given task or mission.

Organizational reliability: Capacity of an organization to avoid generating unwanted dysfunctions.

RAMS: Reliability, availability, maintainability, safety. Aptitude of a system to meet the required function (reliability) at the right time (availability), without danger (safety) and in which the failures can be prevented or repaired (maintainability).

Requirement: A definition of the capacities of a product or process, or a physical characteristic, which must be non-ambiguous and quantitative if possible.

Systems engineering: "Systems engineering is an interdisciplinary approach and means to enable the realization of successful systems. It focuses on defining customer needs and required functionality early in the development cycle, documenting requirements, then proceeding with design synthesis and system validation while considering the complete problem. Systems Engineering integrates all the disciplines and specialty groups in a team effort forming a structured development process that proceeds from concept to production to operation. Systems engineering considers both the business and the technical needs of all customers with the goal of providing a quality product that meets the user needs" (International Council on Systems Engineering)

Workload: Measure of the demand placed on the internal resources of a human being.

Vita

Fabrice Delmotte

Professional Experience

OTIS, France
Safety & Quality Manager, New Equipment France Province *July 2003 – Present*
Coordination and animation of EHS & Quality aspects, for the New Equipment branch:

- EHS Plan: Analysis of accidents, hazards and Safety Audits results to define objectives and actions. Communication, animation and management to achieve the objectives.
- Customer Satisfaction Plan: Analysis of Customer Satisfaction Surveys and Reclamation Letters to define objectives and actions. Animation of these actions.
- Safety and Quality audits: Auditing of technicians, supervisors and supervisors over safety and quality management. Evaluation of compliance with ISO9000, CE directive, internal processes and procedures.
- Safety and Quality training : Coordination and animation of Safety and Quality training sessions for mechanics, supervisors, commercial engineers and superintendents.
- Safety Meetings: Preparation and animation of safety meetings, with personnel delegates, and at the technician, supervisor and superintendent level. Animation of EHS and quality aspects during weekly Staff meetings.
- Documentation: Redaction and updating of EHS and quality manuals.

Safety & Quality Manager, North-East Region of France *Oct 2002 – June 2003*
Coordination and animation of EHS & Quality aspects, for maintenance and modernization activities.

SNCF French Railways, France
Research Project *Jan 2002 – Sept 2002*
Development of a method to integrate Human Reliability into Project Management.

SICK, Germany
Summer Intern *May 2001 – August 2001*
Analysis of a Process Design / Simulation / Workflow middleware, in preparation of the ISO9000:2000 Certification. Evaluation of its functionalities and reliability, and development of workflow applications.

Education

Virginia Polytechnic Institute and State University, Blacksburg, Virginia
Master of Science in Industrial and Systems Engineering *Jan 2001 – Dec 2003*

Ecole des Mines de Nantes, Nantes, France
Engineering Degree in Quality & Risk Management *Sept 1998 – Dec 2003*