Modeling analyses and data in human reliability

Rémi Nicolas Arnaud

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

Bruno Castanier, Co-Chair
C. Patrick Koelling, Co-Chair
Joel A. Nachlas

Defended August 26, 2010

In Blacksburg, VA

Keywords: Nuclear Power Plant, EDF, Human Reliability, Human Factors

Modeling analyses and data in human reliability

Rémi Nicolas Arnaud

(Abstract)

The safety of nuclear power plants must be proved, certified and improved. Probabilistic safety assessments are used to estimate the core meltdown risk, by means of sequential analyses of accidents. In order to assess probabilities of the appearance of these sequences, it is necessary to specifically assess probabilities of operation failures accomplished by human operators in a degraded mode. For this purpose, EDF, the French producer of electricity, developed a method that models failures of human actions, by means of a systematic determination of scenarios corresponding to different failure modes.

This method, called MERMOS, has been used for several probabilistic safety assessments. In order to increase its reproducibility and to make it more robust, example missions and scenarios will be built. This set of example analyses will be used by experts assessing human reliability: they will develop studies and deduce results more easily.

The purpose of this study involves the creation of a methodology to model existing analyses and human reliability data used in MERMOS. This study consists of optimizing a second generation human reliability assessment method in order to overpass its current weaknesses in an operational context by means of the identification of a set of example analyses.

Grant information

This work received support from EDF.

Acknowledgements

This study took place in the context of a dual degree between the Ecole des Mines de Nantes and Virginia Tech. Virginia Tech recognizes my studies at the Ecole des Mines, a French engineering school, and allows me to obtain a Masters degree after one year of studying in Blacksburg, VA. The concept of this dual degree is to integrate an American perspective in industrial and systems engineering, thereby producing more well-rounded engineering students.

As part of the dual degree, I have completed this thesis to fulfill requirements at both universities. This document, in English, corresponds to the evaluation for Virginia Tech. Two evaluations have been carried out for this internship.

I would like to thank all the members of my thesis advisory committee for their support and assistance throughout this project: Dr. Bruno Castanier, Dr. Joel A. Nachlas and Dr. C. Patrick Koelling. Dr. Sarah Ghaffari provided significant help regarding the evaluation of the degree of engineering from the Ecole des Mines de Nantes.

Dr. Bruno Castanier deserves special thanks for the time he has devoted to this. I would also like to express my sincere gratitude to my company tutors, Mrs Hélène Pesme and Mr. Pierre Le Bot for their sympathy, guidance and support and for having showed me this field of research known as Human Reliability.

In addition, I would like to thank other trainees, PhD students and colleagues for their contribution to the positive atmosphere during this internship.

This thesis is also the opportunity to respectfully thank Virginia Tech in general for having received me for one year and the ISE department in particular, specifically Ms. Hannah Swigger and Dr. Joel Nachlas for their support before and during my application. Sincerely, this year in the United States has been an important one in my life, personally and certainly professionally. This experience in the USA would not have been possible without the support of the Ecole des Mines de Nantes. I would like to thank the Graduate School and the administration for their help. In particular, I would like to respectfully thank Ms. Valerie Kirion and Dr. Annya Réquilé for having followed my application. In this context, I thank again Dr. Joel Nachlas and Dr. Bruno Castanier for maintaining a strong relation between the ISE Department and the Ecole des Mines de Nantes and making the dual degree possible.

Last but not least, I would like to thank Ms. Jeanne Mouton for her advice, support and patience during this thesis.

Table of Contents

Table of figures

1. Introduction

1.1. Research and Development at EDF

1.1.1. The company

Electricité de France (EDF) is the leader in the French and British electricity markets and has a solid position in both Germany and Italy. It is the world's largest utility company with €64.28 billion in revenues in 2008, operating a diverse portfolio of 120,000+ megawatts of generation capacity in Europe, Latin America, Asia, the Middle-East and Africa. The group has a assortment of 38.1 million customers in Europe and the world's premier nuclear generation fleet. The activities of the group are worldwide with the purchases of different local electricity producers. The company is composed of 160,913 employees worldwide. The next table gives some insights about the international size of the group Electricité de France[1].

Group Sales	€64.3 billion (+10.6%)
38.1 million customer accounts worldwide	
Electricity generation worldwide	609.9 TWh
EBITDA	€14.2 billion
Net income (Group Share)	€3.400 billion

Table 1 Insights about EDF (from the group website, http://www.edf.com, accessed February 2010)

In 2008, EDF produced 22% of the European Union's electricity, primarily from nuclear power:

- nuclear: 65%
- hydro-electric and other renewable sources: 21%
- thermal: 14%

Its 58 active nuclear reactors are spread out over 19 sites. They comprise 34 reactors of 900 MWe, 20 reactors of 1.3 GWe, and 4 reactors of 1450 MWe, all Pressurized Water Generators.

[1] These pieces of information come from the financial report of the EDF group for the year 2008, accessible on the website http://www.edf.com .Tables and key figures about the worldwide activities of the group are in appendix.

1.1.2. Research and development at EDF

Research and development activities are a strategic orientation of the company. Roughly 2,000 people are involved with research and development and are working in 15 departments, representing a total funding of more than 400 million euros per year. The department where this study has been carried out is the Industrial Risks Management department.

1.1.2.1. Industrial Risks Management (MRI, for Management des Risques Industriels) Department

The MRI department is in charge of leading research and development in the domain of reliability and performance of unsecured socio-technical systems. The subjects of study of the department include: components, technical systems, human factors, organizational factors, the environment (natural, technologic, organizational, regulations), considering the long-term maintenance of these systems. These subjects of study are of interest to EDF. The safety of production systems is a mandatory condition to the exploitation of nuclear power plants. The Industrial Risks Management Department is composed of different services. The Human Factors team is one of these services.

1.1.2.2. Human Factors Team

Human factors (HF) are the subjects of study: HF regroup people from different fields of research such as ergonomics, sociology, psychology or reliability engineers. The team focused on HF considers human beings while they are working, inside complex socio-technical systems that present a certain level of risk. A Human Factor Reliability Assessment (HRA) is done by means of a realistic point of view: a human operator is a source of performance and of reliability; but at the same time, a human operator can fail. These studies are done considering the entire system because the actors are not independent components. Thus, the objective of the HF studies is to integrate entire parts of the socio-technical system and to understand and explain interactions. The aim is to design or modify working situations, to assess the global performance of these systems, and to supervise changes among these work situations. More specifically, the missions of the HF team consist of:

- Producing knowledge about the activities and the organizational situations that answer some specific concerns of the operators;
- Adapting this knowledge into training by means of experience feedbacks in order to increase the global level of reliability. In this case, the HF team contributes to the decision making by means of the pieces of information that are made accessible;
- Designing and rationalizing methods, tools and changes thanks to the situations experimented by the operators;
- Distributing and communicating about these methods in order to develop a HF culture inside and outside the company.

1.2. Objective and Motivation

1.2.1. Human reliability assessment at EDF

Safety in nuclear power plants is emphasized as a top priority. Regulation authorities ask electricity producers to be able to prove that their nuclear power plants are safe. Nuclear safety concerns infrastructures, technical subsystems, and human factors. EDF makes continuous attempts to increase its performance in terms of reliability. By maintaining reliability as a priority, the management of this company is clearly giving a significant example of how important this aspect of using a nuclear power plant is.

Human reliability assessments are the new direction of improvement of reliability analyses. Technologic and technique sides of the system have already been identified in probabilistic safety assessments, even if it is always possible to increase the accuracy of the models. This new direction is emphasized by recent requests of nuclear authorities. Considering human operators in reliability assessment is now a requirement.

In order to assess failures of human missions, EDF uses a second Human Reliability Assessment (HRA) method called MERMOS[2]. This method is the reference method at EDF. In a nutshell, MERMOS allows EDF to model failures of human actions in a degraded mode, by means of different scenarios which are imagined by analysts. Thanks to this method, this company is clearly occupying a spot of leader in Human Reliability Assessment with this innovative method which consists in analyzing accidents by means of scenarios leading to the failure of missions. The great majority of other methods used to assess human reliability is more task-modeling oriented and considers failures of these tasks.

1.2.2. Motivations

The MERMOS method has been used for more than 12 years in hundreds of studies. Feedbacks about the use of the method in an operational context have shown that it requires a high level of expertise and that its use consumes a significant amount of time. Engineers doing reliability assessments are doing more and more studies as regulatory authorities are asking for more reliable systems. The resources to use this method are seen as constraints which limit the integration into general probabilistic reliability assessments: indeed, MERMOS is used to provide a probability of failure of a mission used in the probabilistic reliability assessment of the entire system.

The purpose of this internship is to look for solutions in order to improve the use of MERMOS, what might pass through the creation of a new methodology to use existing analyses, considered as example analyses. Clearly, the objective is not to change MERMOS but to improve its use in an industrial context. Basically, missions can be divided into two main categories. On one hand, missions can be totally innovative and different from what has already been done. On the other hand, missions can be similar to other missions already studied. The objective is to make easier the reuse of already performed analyses.

[2] Assessment Method for the Performance of Safety Operation (*"Méthode d'Evaluation de la Réalisation des Missions Opérateurs pour la Sûreté"*)

In brief, EDF wants to know if optimizations in the reuse of existing studies are possible, by means of example analyses. From these example studies, analysts might be able to easily deduce their own analyses. Analysts would have to provide some key parameters about the HF mission they are assessing. These key parameters would explain the specificities of the current mission compared to any example mission and they would get a probability corresponding to the failure of the considered mission. In addition, example analyses would help junior analysts to perform their assessments.

From this study, EDF expects answers about potential evolutions of the use of example scenarios. The aim of this study is to propose elements of methodology for modeling existing analyses and data of human reliability. More specifically, the study will be focused on a specific set of missions, corresponding to a process that consists of removing residual heat from the core, thanks to water with bore. This set of missions is called “Missions GAVE-OUVERT” (missions “Feed and Bleed” in English).

1.3. Project overview

This subject corresponds to a cross between different fields of human sciences and engineering sciences. The project can be divided into four different phases which correspond to the points described in the previous section.

1.3.1. Phase 1: Identifying example scenarios

Example scenarios are identified by means of the EDF database which contains previous analyses. However, any definition of these scenarios implies a background in Human Factor Reliability, more specifically in Nuclear Safety. Secondly, it is necessary to get used to the database used with MERMOS. Once this study was started, it was possible to get access to the data and to the different parameters specified by the analysts. The main parameters are thus identified by studying the database containing analyses.

This database contains 8003 scenarios, divided into 958 missions. Thus, because of its size, it appeared from the beginning that the acquisition of data had to be done automatically. Another important point deals with the variability of the analyses: differences of vocabulary, different abbreviations, spelling errors and sometimes conceptual mistakes about the method dramatically increase the number of groups. An important characteristic about these data is the fact that they have not been created to be used automatically. The reuse of the previous analyses consists of copying-pasting the entire analyses or just part of them when it is appropriate, and changing some parameters in order to make them fit the considered situation. The first phase deals with an important work of data mining which consists of selecting the relevant pieces of information and in developing a method to obtain them, to correct them and to categorize them, in function of rules of association.

Insights about MERMOS are given in this phase, in order to understand the particularities of this method, regarding other accident modeling theories as described in the literature review. Then, a more accurate literature review dedicated to MERMOS will be given. This analysis will lead to identify potential directions of improvement and the different elements to consider in order to build the future example scenarios.

1.3.2. Phase 2: Construction of the methodology

This phase consists of building the methodology to use for the rest of the study. In order to reinforce the literature review, it is necessary to get experience feedbacks from people in charge of the method in order to understand how analysts use MERMOS and look for previous analyses. In other words, the literature review is completed by a study of the use of MERMOS in an operational context. This step was necessary to identify what parameters are important and must be taken into account in the model of an example MERMOS analysis.

Then, it is necessary to define building rules and the support for the modeling. These two points are independent. It was then possible to build an influence diagram of an example MERMOS analysis. A Bayesian Network using this influence diagram was a satisfying support for the model of example MERMOS analyses; this tool is often used in a reliability context. About the quantitative side of this study, it is important to check the validity of the data, in order to assess the roles of the parameters and to check the relevancy of the results given by the model, from a quantitative point of view.

1.3.3. Phase 3: Methodology testing

The model and the results developed in phase two have been done regarding the optimization of the process which consists of assessing failures of human factor missions. In order to build the model, experience feedbacks from researchers from the FH team of EDF have been used. Also, bibliographical references have been used in order to better understand accident modeling. Last but not least, data were used to check the validity of the model from a quantitative point of view. Clearly, the existing analyses have been used as practitioners' feedbacks. The confrontation between reality and the model will serve two purposes. First of all, the objective will be to determine if example missions and example scenarios help analysts to deduce new analyses. Consequently, this phase will test the robustness of the model and its usefulness regarding the optimization of the way the analyses are carried out. In this phase, example scenarios are identified, and their quantitative parts are defined.

1.3.4. Phase 4: Outcomes: evolutions in terms of time and cost saved

This phase will answer the question initiated by EDF about the feasibility of developing example missions for human reliability assessments. It will consist in summarizing the entire methodology developed during this study. The improvements concern the reuse of existing studies and the time to know if there is an existing analysis which can be used to deduce the study to carry out. The second improvement deals with the time to perform the analysis once the relevant study is identified.

1.4. Outlines of thesis

This thesis is organized as follow. The second chapter introduces different HRA methods in order to understand the theoretical background of MERMOS. This chapter will give the necessary insights about the use of this method and its limits. Chapter three is focused on the systematization of analyses in MERMOS. The modeling of the different parameters to consider in MERMOS scenarios is presented. This representation is then used to identify example scenarios and to perform quicker researches and assessments. Then, the outcomes of this study are presented and evaluated in the context of a complete application for the HRA performed at EDF.

2. Human Reliability Assessment (HRA) methods

This literature review places EDF’s method in its context regarding the evolution of accident modeling. The proposed methodology consists of analyzing scenarios that may lead to an accident. This methodology will use the MERMOS method developed by EDF in this context.

This chapter is organized as follow: in a first part, an analysis of accident modeling is proposed. This analysis will be used to give the necessary key elements to understand this thesis and to identify the bibliographical elements which are used for the new approach. In a second part, the MERMOS method is presented in order to identify the potential ways of improvement in terms in reproducibility and of robustness.

2.1. Introduction

Modeling MERMOS analyses in order to identify examples scenarios deals with different fields of knowledge and belongs as much to engineering as to human sciences. In that sense, human factors are unique. “High-Risk Systems”, such as a nuclear power plant, are required to deal with risk; thus, different tools have been created in order to assess this risk (Perrow 1984). Basically, one can divide these tools into two categories: the first generation HRA and the second generation HRA. The first category consists of dividing any activities in elementary operations. A succession of operations constitutes a task; a product of probabilities corresponding to the failure of any of these elementary operations gives then a general risk of failure of the task. The second generation of HRAs is trying to consider human operators in their socio-technical environment, keeping in mind that human beings are certainly a source of failure, but on the other hand an incredible source of performance.

This literature review on the evolutions of perspectives about implications of human beings in risk is necessary to understand the current method used at EDF. Other researches give interesting grids that will be used to create categories used later in this study.

2.2. Models for integrating human errors in accident analysis

2.2.1. Basic knowledge in accident modeling

According to the field of studies, words such as “risk” or “hazard” do not necessarily have the same meaning (Hood and Jones 2001). From a mathematical point of view, an accident is nothing but an event. From an engineering point of view, an accident is an event with variable qualities that differ from one book to another. For (Hollnagel 2004), an accident is a “short, sudden and unexpected event or occurrence that results in unwanted and undesirable outcome”. However, an accident is not an hazard: for (Hollnagel 2004), this event must be related to human activities. (Perrow 1984) associates the accident with the failure of a component or the failures of different components. These components may be linked together in an anticipated sequence. If the accident involves the unanticipated interaction of failures, thus (Perrow 1984) considers it as a system accident. The notion of anticipation is a key concept in the understanding of accidents: it is impossible for human beings to anticipate some sequences that cause accidents. For the rest of this thesis, an accident will be considered as an event with unwanted consequence, involving human operators.

In the context of nuclear power plants, complexity is an important parameter to consider. Nuclear power plants contain many interactions: failures can interact with other failures and create an “interactive complexity” (Perrow 1984). The system is tightly coupled: the processes happen very fast and cannot be stopped. In other words, in a nuclear power plant, a lot of failures can interact in an unexpected way. Even if the system is designed as redundant (which provides an alternate way to control mechanism), it is not possible to avoid all accidents because of the interactive complexity. A nuclear power plant is an example of what a high risk system is in the sense that it is set of complex and tightly coupled components with a high potential for destruction.

2.2.2. How to model Human Errors in HRA

2.2.2.1. From the 60's to now: different perspectives

Historically, in the context of an accident, human operators have been seen as sources of error or root causes of the malfunctioning of any device. In other words, when something turned out badly, the reason was the human being using the system. The objective of such a point of view was to determine who was to blame for the unwanted outcome of the accident. The tools were generally simple, not subtle. As a general rule, we can say that until the 1960's, models were not sophisticated. A human being can be represented in the models by a piece of data: skills, personality factors, motivational factors and fatigue (Stellman 1998). For engineering departments, the designers, specialists of safety, the human factors are the non-technical parts of the system; they consider that they do not have any influence on these parts (Largier 2008).

In summary, there are two manners of considering human beings at work. On one hand, it is a source of failure that must be controlled (Hollnagel 2004; Le Bot 2005). The main objective is consequently safety. In order to improve safety, the strategy is to characterize the work situation: every step of the work of the human operator is given. The discipline (which consists in following the procedures) guarantees the elimination of accidents. If the operator does as the designers wanted him or her to do, then an accident is impossible. On the other hand, the operator is seen as a resource: the objective is then to use this resource. The main objective is the quality (of the production for instance). A partial description of the work follows. The procedures are sometimes missing, because the system is expecting the operator to be able to make some decisions regarding the situation and the context. In the case of an accident, these two conceptions of the human operator lead to different manner to consider errors and failures.

Human operator = source of errors	Human operator = resource
The situation is known and described. The operator is supposed to follow procedures. If there is an error, it is due to: - Some bad behavior of the operator, such as negligence; - The prescription, such as the description of the procedure, was not effective.	The situation must be studied. Consequently, if there is an error, it is due to: - Lack of attention; - The operator was performing according to a strategy; - Issues due to the context (noise, light, etc.), creating a stressful situation; - A problem in the organization, or the management,…

Table 2 Two points of view about Human operators

According to these distinctions, it is possible to determine the errors that can happen. Three different errors can be identified:

- Human error: corresponds to the gap between the behavior of the human operator and what it should have been. Basically, it corresponds to the last individual in the causal chain and consequently to the guilty person.
- Active error: wanted action, or unwanted action, that has immediate consequences on the system. These consequences are negative.
- Latent error: corresponds to an action or a decision for which the consequences are obvious only after a certain period of time, when other conditions are fulfilled and can trigger this error, resulting in negative conditions on the system.

2.2.2.2. *First approaches: human beings as "black boxes"*

In this simple way to consider the error and the responsibility of human beings, the first models of human reliability were fairly simple. The classical approach of human error is a "black box" (Le Bot 2000; Hollnagel 2004) of the human behavior. The human operator is seen as a system, receiving inputs, performing a certain action with a certain rate of failure. Operator errors are classified according to their external characteristics. Since the activity is totally described by procedures, the error can happen if and only if a bad application has been performed (Swain

1976). Consequently, in order to improve reliability, the idea is to work on the inputs or on the outputs. For instance, the proposed ways to improve reliability were some actions on the reinforcement of the procedures, the improvement of the labeling or the improvement of the ergonomics. On the other hand, some actions can be performed on the outputs, such as a frequent control of the respect of the procedures with sanctions if operators do not respect them.

The main interest of this approach is certainly the probabilistic applications: it is possible to perform probabilistic assessment on the frequency of appearance of errors. In order to do so, an important hypothesis must be done: the actions of the operators have the same behavior as the functioning of the components of the system: there are no feelings, nor will. This model is called THERP, for Technique for Human Error Rate Prediction, described in (Swain 1976), and analyzed in (Le Bot 2000) and (Hollnagel, Woods et al. 2006).

2.2.2.3. Benefits of the "black box" perspective: THERP

The main objective of this method is predicting the probabilities of human errors and evaluating the degradations of the system. These degradations are potentially caused by human errors. The results are interesting: it is possible to get a probability that estimates the general reliability of the system, composed of humans and technical components, and to determine the weakest parts. The THERP method can be developed in 6 steps (Swain 1976; Swain 1990). First, every operation must be described by a procedure. Then, these procedures must be described in terms of elementary tasks. These tasks are described by elementary actions. These actions are associated with a probability of failure (or success), given by an expert. The failure of a task is thus the product of the probabilities of the actions. The failure of a procedure is the product of the probabilities of the tasks that compose the procedure. An example of a THERP like method is described in (Dhillon 2009).

This method is difficult to implement in the sense that a lot of tables must be considered to get a relevant result. However, THERP is well suited to the tasks where cognitive tasks are not important and where time is not an important parameter. THERP has been frequently used directly or indirectly; the previous method at EDF was derived from THERP, (Le Bot, Remond et al. 1996; Le Bot, Bieder et al. 2000; Le Bot, Pesme et al. 2002). Throughout its high popularity all over the world, some critiques have been formulated about this vision of human error. For instance, THERP does not allow one to take into account tasks where cognitive processes have a strong importance. It is not always possible to simplify and to cut a task into elementary operations. However, in order to take the cognitive tasks into account, THERP has evolved in order to account for the cognitive tasks of development of diagnostics (Swain 1990). Although these kinds of evolutions tend to make THERP more subtle, this reliability approach stays focused on behaviors and individual errors and does not include into its scope errors related to intellectual work: evaluation of situation, diagnostic, decision making etc. are outside the sphere of study of THERP. Besides, any error due to organizational causes is clearly outside THERP (Stellman 1998; Le Bot 2005; Largier 2008).

The answer to the limits is consequently to open the black box and to study the human operator in order to understand errors.

2.2.2.4. Opening the "black box": Rasmussen's legacy

As described in (Largier 2008), Rasmussen proposed a model that shows how pieces of information are given as inputs and used to get actions as outputs. The objective of this model is to propose a methodology that helps to identify errors that might happen in different operational situations. Secondly, some treatments are proposed as solutions for the errors which are identified. In the next table, the 3 different behaviors with the associated errors are described (Largier 2008).

Behaviors	Meaning	Error
Skill	Skill based behavior. It is the dominating behavior, based on habits: it is the regular way to do something	Errors are due to a lack of attention
Rules	Rule based behavior. The behavior is described by a procedure.	The risk is to trigger a procedure that is not adapted to a given situation.

Knowledge	Knowledge based behavior. There is no rule or procedure that is known by the operator that would allow one to solve a problem. The solution must be found from the situation and knowledge.	The operator cannot find a solution. The stress is a factor to consider in this situation.

Table 3 Errors and SRK model (Skills-Rules-Knowledge)

For Rasmussen, the appearance of errors happens when the configurations switch from a situation to another. It is a dynamic process (Largier 2008). This model is a sort of basis for many other models and tools in Human Factors. It concerns different fields of risk management: health (Sockeel, Chatelain et al. 2009), train transports (Wreathall, Roth et al. 2001) for instance. Rasmussen's SRK model was the beginning of the research in cognitive psychology. However, this model presents some limitations such as the fact that it is focused on the operator and does not take into account organizational causes of error.

2.2.2.5. Evolutions of Rasmussen's model: the James Reason's contribution

A more recent way to consider human error has been proposed by James Reason and is a compromise between different works (Reason 2008). He proposes three types of error; these distinctions come directly from Rasmussen's SRK model.

- Knowledge based: actions are governed by conscious attention, which is limited. It relies upon conscious image, inner speech, instructions. Conscious is flexible, computationally powerful but it is also favorable to error.
- Skill-based performance: for Reason, it corresponds to an automatic behavior. The conscious is at its lowest level.
- Rule-based performance: corresponds to a mix between automatisms and consciousness: if some parameters, events are satisfied, then operators know which action must be performed.

The most interesting contribution of Reason to human error is the introduction of the concept of “intention.” For Reason, if there is an error, then there must be an intention. Otherwise, it is about an involuntary action or an automatism. This concept comes from the level of consciousness that is required for the different actions, based upon the SRK model.

The classification of errors can be done in function of the actions, such as omissions, intrusions providing information about the process (plan formulation for instance). This stage is cognitive. The classification of errors can give contextual factors such as anticipation and preservation (an actor that says the lines of the next action because of similarity with another situation that he/she has already experienced). Errors may be classified according to outcome categories, such as free lessons, accidents and incidents.

As far as the violations are concerned, Reason considers that they happen for different reasons, depending on the considered level:

- At the skill-based level: the operators are following the path of least effort between two last-related points. A “routine violation” is mainly promoted by inelegant procedures;
- At the rule-based level: the violation might occur because of the constraint represented by safety procedures, rules and regulations;
- At the knowledge based level a violation might be due to calculated risk: the situation is unusual and might to overpass the rules.

With this study, Reason introduced the context in the parameters to consider in understanding the black box and the error or the violation. To do so, the context must be studied. The context can be divided into two components (Rousseau and Largier 2008):

- The immediate context composed of the organizational and cultural dimensions when they are applied to the work shift (group, service, shift, etc.);
- The global context: social, cultural, economic, political, etc.

Consequently, the human operator is now considered in a social, cultural and technical system that allows one to consider all the dimensions of an accident.

2.2.2.6. From Human Factors to Organizational factors

The work organization has been changing (Stellman 1998; Hollnagel, Woods et al. 2006; Largier 2008). From the 50's on, the nature of work has changing, passing from mainly physical activities to activities with a dominant cognitive part. Robots and electronics are becoming more important. The operators are dealing with the processing of information, memorizing, diagnostics, etc. Operators are sometimes away from the process and are working thanks to a mental image of what is taking place. This evolution has some collateral consequences such as those described by (Stellman 1998): the direct safety of workers is improved (since the operators are no longer as involved in the process; they are watching it).

(Hollnagel 2004) tries to give the main reasons that may generate an accident and proposes a list of potential causes including a lack of training and inappropriate work schedules. (Rousseau and Largier 2008) propose "pathogen organizational factors", or organizational factors that have negative consequences on the reliability of the system (page 4). This list will be used to build the model of example MERMOS analyses and give interesting insights about the context that may see the appearance of an accident.

- Lack of anticipation and detection of errors;
- Experience feedback systems are not working;
- Lack of responsibility by the people in charge;
- Unreasonable expectations in terms of productivity (objectives too high regarding the resources available);
- Incapacity to maintain the individual competences;
- Incapacity to use collective competencies;
- Too many procedures;
- Lack of dialogues between the individuals and services;
- Lack of communication and interactions between different services/departments.

It appears that the results proposed by (Rousseau and Largier 2008) and (Hollnagel 2004) are very close: this list is an application of the list of Hollnagel, applied in the context of nuclear power plants. This list will be used directly in chapter 3 in order to model the parameters used in MERMOS.

2.2.2.7. How to fight against accident: toward a general consensus

All researchers agree on the impossibility to design a system with 0 probability of accidents. Accidents will happen, sooner or later. Since the accidents are considered as “normal” (Perrow 1984), the objective has evolved. All systems need to be able to survive to local failures so that incidents do not become accidents. The improvement of “the general safety of a system deals with the improvement of systems to survive to any perturbation” (Hollnagel 2004). (Hollnagel, Woods et al. 2006) propose to define a “safe system as a system which impervious and resilient to perturbations”. In other words, even if things go wrong, which will certainly happen one day, the system is still safe and able to work. (Westrum 2006) describes resilience as the ability to prevent something that has already happened from becoming worse, and the ability to recover from something bad once it has happened.

Abilities	Tools used to make it possible
Prevent something bad from happening	Experience feedbacks Anticipation
Prevent from becoming worse	Flexibility Rapidity of reaction Evolution
Recover after something bad	Repairing after a catastrophe

Table 4 Main precepts of resilient engineering adapted from (Hollnagel, Woods et al. 2006)

2.2.2.8. Human error, models and references

Search Principle	Model type sequential models Specific causes and well defined links	Epidemiological models Carriers, barriers and latent conditions	Systemic models Tight coupling and complex interactions

Analysis Goals	Eliminate or contain causes	Make defenses and barrier stronger, stop the propagation of accidents	Identify socio-technical contexts creating accidents, monitor
Examples	Chain or sequence of events (domino), tree models, networks models	Latent conditions (Swiss Cheese Model) pathological systems	Control theoretic model
References	(Stellman 1998) especially for event trees and causes trees, (Hollnagel 2004; Le Bot 2005; Hollnagel, Woods et al. 2006)	(Reason 2008) (Hollnagel 2004; Le Bot 2005; Hollnagel, Woods et al. 2006)	(Leveson 2004; Hollnagel, Woods et al. 2006)

Table 5 Main models of accident and references

2.3. MERMOS: a second generation HRA

EDF decided to develop a second generation Human Reliability Assessment method in the context of the development of the N4 generation of pressurized water reactors. Basically, this new method has been created to better take into account the technical evolutions of this new reactor. Nowadays, MERMOS is being used for all the French reactors.

In the previous part of the chapter 2, the main concepts related to accident modeling and human errors have been presented. Now, the focus is clearly on the subject of this internship, namely the MERMOS method and the identification of example scenarios.

2.3.1. MERMOS: concept and principles

2.3.1.1. MERMOS and other HRA

In a Probabilistic Safety Assessment (PSA) of a nuclear power plant, evaluating human failures that increase global risk is essential. There are different HRA methods such as MERMOS or its American competitor ATHEANA described in (Forester, Kolaczkowski et al. 2007) and (Wreathall, Roth et al. 2001), or influence diagram influence approach, described by

(Humphreys 1987). The general purpose of the HRA tools and methods can be expressed as (Le Bot 2005):

- Identify actions carried out by human operators in normal situations or in accident situations that have significant consequences on the safety of the reactor, in case of failure;
- Evaluate the probability of failure of every action that has been identified previously and incorporate them into the PSA;
- Collect data.

The HRAs consider three different types of errors that can be due to human operators (Le Bot 2005).

Type A	Errors in normal situations that imply availability of pieces of equipment of the safety systems, latent errors
Type B	Actions that lead to trigger an initiator
Type C	Failure of actions after the triggering of the initiator

Table 6 Types of errors considered in HRA, from (Le Bot 2005)

For EDF, evolutions of technologies such as simulators of nuclear power plant control room and automatic displaying of procedures made their THERP-like method irrelevant. The analysis of accidents shows that the management of the operations in the nuclear power plant results from a team consensus: in other words, individual errors are not sufficient to understand and explain accidents (Le Bot 2003; Le Bot 2005). Consequently, MERMOS was born in order to take into account the relationships between operators, procedures and interface, in the context of the type C error, and managed to overpass the individual error perspective. Considering that errors happen as a collective process rather than as the consequence of the behavior of an individual is clearly an important development in the field.

2.3.1.2. MERMOS: a collective-error based approach

MERMOS considers that an accident is composed of periods of stability separated by reorganization of the configuration. A period of stability is described by a CICA (Key Configuration for Accident Management, or *"Configuration Importante de la Conduite Accidentelle"*). This method allows EDF to evaluate the probabilities of failure of a system composed of the team in the control room, the procedures they use, and the human-machine interface. Field workers and a crisis team are components of the environment or can be considered as resources used by the operating team. The model implied by this method is relying on the next key assumptions as described in (Le Bot 2005; Le Bot, Meyer et al. 2007):

- Individual human error is not predominant. The management of the operations is decided by the operating team and not by only one individual. In each failure scenario, the system is robust and thanks to redundancies and other defenses, an individual error cannot lead to an accident. It would be corrected by the rest of the operating team (De la Garza and Le Bot 2006);
- Progress of operation through time is a sequence of phases of stability consisting in focusing on a specific aspect of the situation. Between two periods of stability, the system restructures itself and a new orientation is chosen.

2.3.1.3. Accident modeling in MERMOS

In order to do so, scenarios are imagined; these scenarios are potential ways to conduct to the failure of the mission and correspond to identified degraded modes. MERMOS is, first of all, a succession of steps that leads analysts to get to a scenario leading to the failure of a human factor mission. The probability of failure of the scenarios is calculated by means of situation features, CICAs and a probability of maintaining a given CICA through time (Meyer, Le Bot et al. 2007). The situation features describe the situation that may lead to the appearance of a certain configuration of the team regarding objectives, described by CICAs. In other words, it is because of the context that the team decided to adopt a certain configuration. The circumstances (a "specific combination of events" (Le Bot, Meyer et al. 2007)) induce the system to adopt modes of organization that lead to mission failure. Because this configuration is not adapted to the current circumstances, if the configuration is not changed, then the accident will occur: this notion is contained in the probability of maintaining a CICA through time. In order to imagine the scenarios, the analysts are asked to consider that the operating system must accomplish three functions:

- To diagnose the situation of the nuclear power plant and the situation of the state of the nuclear process by means of indicators and control panels in the control room. In order to carry out the mission, the operating system must be aware of what is going on. The mental representation plays an important role in the ability of the operators to make the good choices and to take the good decisions;
- To have a successful strategy: this strategy explains how to manage the mission regarding the diagnosis made by the team;
- To take actions: these actions are the steps in the application of the strategy.

The failure of one of these functions implies the failure of the realization of the mission.

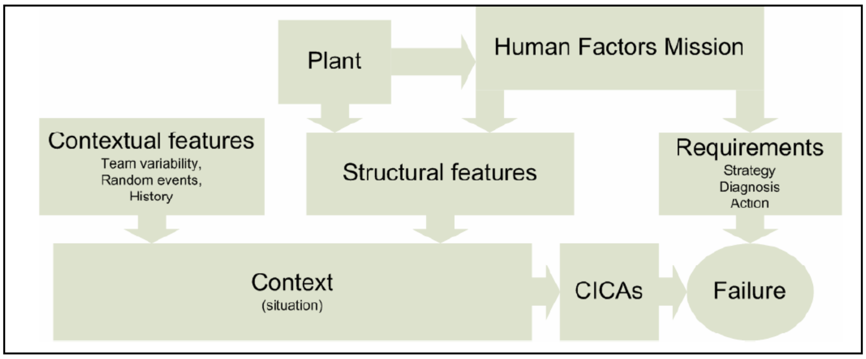


Figure 1 Failure Scenarios global view, from (Le Bot, Meyer et al. 2007) (page 269) used under fairuse.

2.3.1.4. Description of the data

2.3.1.4.1. Mission

At EDF, human reliability assessments are carried out in the context of more general probabilistic reliability assessments. These analyses correspond to a specific mission of human operators in a degraded mode. Probabilistic safety assessments are used to estimate the core meltdown risk, by means of sequential analyses of accidents. Consequently, any scenario is associated to a certain degraded mode, corresponding to specific unavailable components. In addition, a mission corresponds to a specific type of reactor, and a family of HRA analysis (corresponding to a type of generator).

2.3.1.4.2. Scenario

A scenario is associated to a mission. More specifically, a scenario corresponds to a possible way to fail a mission: it is a failure mode which can explain how one of the three requirements may not be satisfied (Actions, Diagnosis and Strategy). Main failure modes have been identified and organize a systematic research of possible scenarios.

Strategy	**Action**	**Diagnostic**
No strategy	No action	Misrepresentation of the situation
Erroneous strategy	Erroneous action	Misrepresentation of the state
		No diagnostic about the situation

Table 7 Failure modes

In addition to failure modes, analysts consider the requirements which would avoid failure if they are satisfied. The non-satisfaction of these requirements corresponds to a possible path which leads to the mission failure.

2.3.1.4.3. Situation features

A scenario involves a context. This context is composed of situation features. They correspond to the characteristics of the situation which are necessary to explain the appearance of the CICAs and why they are maintained though time. Two main categories can be considered. On one hand, situation features can be structural characteristics to the mission, such as time requirements to perform the mission. This category of situation features concerns all the scenarios which correspond to the same mission (for all the scenarios corresponding to the mission "Activate the feed and bleed in less than 35 minutes", the time requirement is 35 minutes). On the other hand, the second category deals with contextual characteristics. In this case, situation features are more specific to the scenarios: for instance, they can describe some special characteristics of the team, or special behavior of members of the team.

2.3.1.4.4. CICAs

A CICA describes an orientation or a configuration of the operating system, maintained through time. A CICA corresponds to a strategic orientation (a certain way, manner or objective that lead the management of the operations) and use of resources. Configuration corresponds to internal properties of the operating system, such as making up a team, kinds of relationships among its members, available operating instruments, etc. Orientation is the operating system's positioning with respect to the situation: its interpretation of the situation, objectives and its priorities, and its attitude towards the operating tools (e.g. violation VS procedures followed step by step).

"*CICA are positive modes of operation and their faulty nature only appears in certain situations, corresponding to a specific combination of events liable to induce the system to adopt modes of organization – CICAs — leading to mission failure*" (Le Bot 2003), page 4. In other words, the decision taken by the team is conscious, and there are reasons that justify this choice (interpretation of the current situation, or just following procedures).

2.3.2. MERMOS: rules of implementation

2.3.2.1. Application of the method

MERMOS is first of all a systematic method that allows analysts to develop and imagine scenarios of accidents. This method can be divided into 4 main steps.

- Study of the requirements
  - The analysts define what the requirements are regarding the strategy, the action and the diagnostic. These three elements correspond to the functional requirements in order to accomplish the mission. If one is unsatisfied according to the previously described failure modes, then the mission fails.
- Qualitative analysis
  - From the requirements, analysts are deducing the context and the CICAs that may lead to the mission failure. Two situations are considered:
    - It corresponds to a new study: analysts cannot deduce from existing scenarios their studies;
    - This study is similar to a previous analysis and thus, they can partially or totally deduce their analysis from this older scenario.
- Quantitative analysis
  - Analysts express quantitatively the probabilities which are associated to the different elements of the scenario (CICAs, context and non-reconfiguration).
- Finalizing results
  - Analysts check the validity of their results.

2.3.2.2. Data collection: expert judgment

The MERMOS method requires from the analysts that they are proficient in reliability of systems, that they have knowledge in human factors, that they are confident in process management and in operations management. Besides, the expert must be able to appreciate the final probability of appearance of an event in order to correct it if necessary. MERMOS is a method of creation of knowledge from expert advice. In order to improve their expertise, analysts are trained with simulators (Le Bot, Pesme et al. 2008), have access to procedures, to previous accident reports and to previous analyses. Furthermore, a collective expertise takes an important role in the use of the MERMOS method. In order to make the exchange of knowledge possible between experts, the use of MERMOS is using a technique of comparison ("method by Delta") which consists of adapting a scenario to a new situation. An analyst reuses the work of a previous analysis.

In order to have a general view of this method, Appendix 2 proposes a figure which describes the different steps of creation of a new analysis. This figure is adapted from (Le Bot 2005; Pesme, Le Bot et al. 2007).

2.3.3. Quantitative risk assessment

The analysts can forget scenarios: the hypothesis is that some scenarios cannot be imagined. These scenarios are outside the limits of human intellectual projections (Le Bot 2005). Thus, the method considers a residual probability which corresponds to these scenarios. For the rest of this study, this probability will be noted: P_{res}.

Probability of failure of HF mission	Considered event E: "Failure of HF mission" $$P(E) = P_{res} + \sum_{i \in I} P_i$$ Where i corresponds to the i^{th} identified scenario. I is the set of these identified scenarios. P_i is the probability of appearance of the i^{th} identified scenario.
Probability of appearance of scenario	Let's call: - C_j : the j^{th} CICA (see the part dedicated to the CICAs) $P(C_j \vert S_{k1,k2,\dots}) = P_{C_j \vert S_{k1,k2,\dots}}$ and corresponds to the probability to have the event "the j^{th} CICA is relevant in this scenario". The j^{th} CICA may happen if and only if the context is favorable: in other words, if and only if the situation features that may generate the appearance of this CICA are true; - S_k : the k^{th} Situation Feature. $P(S_k) = P_{S_k}$ and corresponds to the probability to have the event "the k^{th} Situation feature is relevant in this scenario".

	- Finally: $P_i = [P_{nr}] \left[\prod_{j \in J} P_{C_j \mid S_K}\right] \left[\prod_{k \in K} P_{S_k}\right]$ Where P_{nr} is a probability of non-reconfiguration
About probabilities	The probabilities used are imposed: they either come from experience feedbacks or are given by data. In the first case, the expert must decide if the probability is very improbable, improbable, probable, very probable. In addition to this scale, analysts may add two steps, consisting in an impossible situation (0 probability) or a certain situation (1 probability). Respectively, when the analysts appreciate probabilities, the numeric values are: $\forall j, \forall k, (P_{nr}, P_{C_j}, P_{S_k}) \in \{0; 0.01; 0.1; 0.3; 0.9; 1\}$[3]

Table 8 Quantitative results given by MERMOS

2.3.4. Remarks about the quantitative analysis

2.3.4.1. Residual probability

Ideally, the residual probability should be decreasing while knowledge about scenarios leading to the mission failure is created. However, the reality is different: the number of scenarios for a given mission is not considered as important enough to change the value of this probability.

2.3.4.2. Situation Feature probabilities

It is interesting to notice that the situation features form all together the context of a scenario.

$$P_i = [P_{nr}] \left[\prod_{j \in J} P_{C_j \mid S_K}\right] \underbrace{\left[\prod_{k \in K} P_{S_k}\right]}_{\text{Probability corresponding to the appearance of the context.}}$$

The probability of appearance of the context consists of the simultaneous appearance of the different situation features which constitute together this context. In other words, this probability corresponds to the coexistence of the situation features.

$$P(\text{Context}) = P(\text{Situation Features 1} \cap \text{Situation Features 2} \cap \ldots \text{Situation Features K})$$

If situation features are independent, then:

$$P(\text{Context}) = P(\text{Situation Features 1} \cap \text{Situation Features 2} \cap \ldots \text{Situation Features K}) = \left[\prod_{k \in K} P_{S_k}\right]$$

The analyst is then estimating the probability of appearance of every situation features.

On the other hand, when the method has been constructed, the case of dependent situation features has been considered.

2.3.4.3. Independence of Variables

The MERMOS method may consider scenarios having more than one CICA. For such scenarios, CICAs are not necessarily independent. Research and Development team has advised analysts to complete scenarios respecting a hierarchy among situations features and CICAs. For instance, by considering a scenario composed of two CICAs and of two situation features:

$$P(\text{Cica 1 and Cica 2}|\text{Context}) = P((\text{CICA 2 }|\text{Context}) \mid (\text{CICA 1 }|\text{Context})) \times P(\text{CICA 1 }|\text{Context})$$

For the final formulation of the probability, let’s consider the next description of a scenario.

- “Accident” is the event which corresponds to the appearance of the event “mission failure”.
- S_i is the event which consists of the appearance of the event “Situation Feature i is relevant in the current scenario”.

$$P(\text{Accident}) = P(\mathrm{S}_1 \cap \mathrm{S}_2 \cap \mathrm{CICA}_1 \cap \mathrm{CICA}_2 \cap \mathrm{NR})$$

More practical expressions can be expressed as follow.

$$P(\text{Accident}) = P(\text{NR} \mid \text{S}_1 \cap \text{S}_2 \cap \text{CICA}_1 \cap \text{CICA}_2) \times P(\text{S}_1 \cap \text{S}_2 \cap \text{CICA}_1 \cap \text{CICA}_2)$$

$$P(\text{Accident}) = P(\text{NR} \mid \text{S}_1 \cap \text{S}_2 \cap \text{CICA}_1 \cap \text{CICA}_2) \times P(\text{CICA}_2 | \text{S}_1 \cap \text{S}_2 \cap \text{CICA}_1) \times P(\text{S}_1 \cap \text{S}_2 \cap \text{CICA}_1)$$

$$P(\text{Accident}) = P(\text{NR} \mid \text{S}_1 \cap \text{S}_2 \cap \text{CICA}_1 \cap \text{CICA}_2) \times P(\text{CICA}_2 | \text{S}_1 \cap \text{S}_2 \cap \text{CICA}_1) \times P(\text{CICA}_1 \, | \text{S}_1 \cap \text{S}_2) \times P(\text{S}_1 \cap \text{S}_2)$$

Next expression allows to see the hierarchy among the different parameters to consider: firstly, S_2 is quantitatively defined. Then, knowing that S_2 is realized, S_1 is quantitatively defined. Then knowing that S_1 and S_2 are realized, CICA_1 is quantitatively defined. The same operation is performed until every parameter is quantitatively defined.

$$P(\text{Accident}) = P(\text{NR} \mid \text{S}_1 \cap \text{S}_2 \cap \text{CICA}_1 \cap \text{CICA}_2) \times P(\text{CICA}_2 | \text{S}_1 \cap \text{S}_2 \cap \text{CICA}_1) \times P(\text{CICA}_1 \, | \text{S}_1 \cap \text{S}_2) \times P(\text{S}_2 | \text{S}_1) \times P(\text{S}_1)$$

Analysts give probabilities knowing that the other elements of the scenario they are creating are realized. MERMOS deals only with conditional probabilities.

In case of independence between variables, this formula is still true. Consequently, it is possible to consider the independent case as a specific situation of this more general formula which considers the dependent cases. In details, the different terms of this last expression can be described as follow:

- The term $P(\text{NR} \mid \text{S}_1 \cap \text{S}_2 \cap \text{CICA}_1 \cap \text{CICA}_2)$ correspond to the probability that the system does not change its configuration, regarding this configuration and the context.

- The term $P(\mathrm{CICA}_2|\mathrm{S}_1 \cap \mathrm{S}_2 \cap \mathrm{CICA}_1) \times P(\mathrm{CICA}_1\ |\mathrm{S}_1 \cap \mathrm{S}_2)$ corresponds to the probability that the system adopts a certain configuration described by $\mathrm{CICA}_1 \cap \mathrm{CICA}_2$ in this given context.
- The term $P(\mathrm{S}_1|\mathrm{S}_2) \times P(\mathrm{S}_2)$ corresponds to the probability of appearance of the context.

In a scenario with more CICAs and situation features, the probability of appearance of an accident is given by the next formula.

$$P(\text{Accident}) = P(\bigcap_k \mathrm{S}_k \cap \bigcap_i \mathrm{CICA}_i \cap \mathrm{NR})$$

What corresponds to:

$$\begin{aligned} &P(\text{Accident}) \\ &\quad = P(\mathrm{NR}|\bigcap_k \mathrm{S}_k \cap \bigcap_i \mathrm{CICA}_i) \\ &\quad \times \prod_{i\prime} P\left(\mathrm{CICA}_{i'}|\bigcap_k \mathrm{S}_k \cap \bigcap_{i<i'} \mathrm{CICA}_i \right) \times \prod_{k\prime} P\left(\mathrm{S}_{k'}|\bigcap_{k<k'} \mathrm{S}_k \right) \end{aligned}$$

2.4. Limits of the MERMOS approach

MERMOS is a method which allows the analysts to express subtleties in their analyses. That is why the scenarios may be extremely accurate, describing a specific context that may lead to the accident. Research and Development team has imagined MERMOS as a dynamic system where analysts would use previous analyses to feed their current analyses. Every analyst increases his or her knowledge about HRA and would increase the quantity of information contained in the database.

However, these subtleties cannot be systematically considered: the quantity of pieces of information which has been created for last 12 years of use represents thousands of lines in the database. This amount of information generates problem of research of relevant information in a partially structured database: analysts answer specific parameter about a scenario (CICAs, situation features, requirements, etc). However, the way to describe these parameters is not prescribed. Clearly, a method to identify when a scenario is similar to an existing one must be defined. It would significantly decrease the time spent by the analysts to perform an analysis, since they would just have to adapt an existing one to their current situation. This difficulty in the research of similar analyses must be connected to the size of the database.

The database is composed of 45 tables. The tables used for the model are described in the next table.

NAME OF TABLE	RECORDS	MEANING
CICAS	3801	Configuration and orientation of the team explaining how the mission can be failed.
HRA family	21	HRA families correspond to the reactor type that is studied and to the context of the assessments (assessing fire hazards in a type of reactor for instance)
Requirements	7619	Requirements correspond to what must be done in order to succeed the mission.
Failure mode	8	Failure modes are linked to required functions (Strategy-Diagnostic-Action) and correspond to identify way to fail these requirements.
Initiators	957	Correspond to the initiators from the technical part of the probabilistic reliability assessment. Initiators may be used by analysts to identify a mission.
Unavailable components	956	When the human factor missions begin, the system is in a degraded mode: some components are not available. These systems may be used by the analysts to identify a mission.
Mission	957	A mission is composed of scenarios corresponding to possible ways to fail the mission.
Situation Features	13165	Situation features describe the context of appearance of the scenario

Table 9 Database overview

At the beginning of the deployment of the method, 15 standards HF missions were given to analysts in order to give them a minimum of guidance (Le Bot, Bieder et al. 2000). Originally, “this refinement was required to compensate for the perceived complexity of the method.” In addition to this database, guidelines had been developed to allow an analyst to derive the whole analysis of a HF mission from a standard HF mission. “The principles relied on the identification of discrepancies between the HF mission to be analyzed and the standard HF mission used as a base, and on guidelines provided to modify the source analysis accordingly” (page 4). As the analysts have gotten more experienced, the use of the database changed; it became a source of general ideas, whereas its first use was to be a source of scenarios. Last but not least, the database helped to compensate the difference of expertise between analysts.

2.5. Conclusion

EDF has passed from a THERP-like method (called FH06) to MERMOS. The advantages of Mermos over the previous method have been indentified in (Le Bot, Pesme et al. 2002), and can be summarized as:

- the systemic perspective of the approach since MERMOS is a step-by-step method which helps to imagine and described failure scenarios;
- the realism of the modeling, consisting in imagining and describing the context leading to an accident;
- the applicability of the method both in terms of usability and cost: MERMOS can be easily deployed. It does not require any modeling of the activity like THERP does;
- the richness of the analysis;
- the traceability of the analyses since all the results are supposed to be justified.

However, from a practitioner’s point of view, THERP has advantages over MERMOS. The data come from tables and once the process is modeled, getting results is easy. However, the preparation work is significantly long. The difficulty to set up a THERP-like method gives to MERMOS a serious advantage by comparison which can produce subtle analyses.

In order to identify pattern over the analyses, it is necessary to categorize the parameters that have an influence in a mission: MERMOS is unique; its database is unique and represents at least 12 years of advance over any competitors in the world corresponding to 12 years of acquisition of data. The previous literature review will be used to create a model of the example MERMOS analysis, based on the previous analyses, which do not exist yet. More specifically, the model of example analyses corresponds to the way MERMOS is used by analysts and will be built regarding the existing analyses. The research involves a modeling of example MERMOS analyses.

3. Systematization of the analyses in MERMOS

3.1. Introduction

According to the HF team, analysts search similar analyses using 3 different manners. First of all, they may be looking for missions containing in their labels a specific key word. Other techniques of research concern a research based on unavailable components and subsystem (a MERMOS mission takes place in a degraded context) or on initiators.

Now, the database is used in order to deduce an analysis from existing missions or scenarios. The “delta method” described in (Pesme, Le Bot et al. 2007) consists of using an existing analysis and adapting it to the context of the studied analysis. However, this reuse is not systematic, or at least presents some unexpected bias. Analysts are using the general sense of previous analyses; but the label is not exactly the same. Consequently, from a database point of view, it is as if they were created new values for a given parameters. An immediate consequence deals with the difficulty to research missions in the database.

For the purpose of this study, identifying patterns implies finding a way to overpass the immediate difference between the analyses and regroup the ones which are different because of vocabulary problems rather than a conscious will of the analysts to differentiate them. Clearly, the objective is to identify the pieces of information contained in the analyses in order to create groups of similar analyses. However, this objective generates questions, such as:

- How a group of analyses is defined?
- How to solve problems of spelling and vocabulary?

Scenarios are different or similar to each other because of the presence or of the absence of certain values for parameters, such as failure modes, requirements in terms of function to perform to satisfy the missions, a time window, CICAs and context. These parameters are key parameters in the identification of patterns among previous analyses.

In addition, the quality of entries of the database is variable. In order to fix some problems due to spelling error algorithms described in (Damerau 1964) have been used.

3.2. Homogenization and classification of the key parameters

3.2.1. Modeling CICA

3.2.1.1. Categories

A first study on the CICA revealed that they show a pattern. A CICA corresponds to an action, specified by some complements, such as temporal ones. During this study, it has been shown that the number of actions used for the CICA is finished, and corresponds to 14 actions families. These families present similarities which have been exploited to create 5 CICA categories. Actions families have been built regarding only the data: It is just the translation of recurrent pattern in the way analyses are performing HRA. On the other hand, CICA categories are linking CICA with models identified previously. The CICA categories are a practical applications of the works of (Perrow 1984) in order to consider complexity, of (Largier 2008; Reason 2008; Sockeel, Chatelain et al. 2009) about the erroneous interpretation of a situation, and of (Hollnagel 2004; Hollnagel, Woods et al. 2006; Hollnagel 2009) since it corresponds to a certain configuration that would make barriers and protections ineffective.

- Category A
  - The action has a strong temporal dimension, expressed by a delay. Analysts want to emphasize how operators manage tasks in time. However, every CICA has a relation with time, since a CICA reveals that it is irrelevant regarding a given situation because it was maintained for too long. But the CICA might concern the time dimension of the management by the team in the control room. The work of (Perrow 1984) about system complexity and coupling gives an insight about the reasons that would make management of operations in time irrelevant regarding a situation.
- Category B
  - The action is defined by its cognitive dimension: the team must interpret the situation; the situation might be described by a lack of understanding. This CICA category can correspond to collective K errors (Knowledge: understanding and interpretation of the current situation. in order to get an original and adapted

solution to the situation) or S error (Skills: automatic answer from the team or inability to identify the current situation as an emergency situation). This CICAs category is related to the work of (Reason 2008).

    - The team determines objectives, which are linked to the understanding of the situation. This CICA category is thus concerned by the way the team manages these objectives and how it understands the situation.

- Category C
    - Procedures and the way the team is following procedures may play a significant role in accidents. This CICA category describes the positioning of the team regarding rules. It might be an R-error (Rules: inappropriate procedure applied in a given situation), or waiting attitude from the team toward the procedure. It is important to separate the case where the CICA concerns the necessary time to apply the procedure (Category A) with the case emphasizing the attitude of the team toward the procedure. This CICA category might deal with the context; for instance, it might be related to the unusual aspect of the accident, and the team might be working under stress. As a general rule, this category allows to make a connection between failure of the HF mission, rules, and the positioning of the ream regarding these rules. This CICA category is related to the work of (Reason 2008) about violations, of (Rousseau and Largier 2008) and (Hollnagel, Woods et al. 2006).
- Category D
    - The team is in constant interaction with the technical side of the nuclear power plant. The positioning of the team regarding technique might play a role in the appearance of the accident. This CICA category does not imply the team to have any understanding of what is happening; it just describes how the team uses technical resources or a part of the system.
- Category E:
    - The team decides to delegate a task to a specific person or component. Because they are delegating, redundancies disappear: one person alone or an automatic component is having a responsibility that was shared by the whole team before. This CICA category may concern the human resources management by the team.

However, this classification does not support specific scenarios having two CICAs. For the “feed and bleed missions”, the next CICA couples have been identified:

- A-A: The crew postpones an action in order to keep performing or to start another action;
- A-B: The crew postpones an action because it feared that this action has an unwanted outcome;
- C-B: The crew applies a not adapted procedure to the current situation due to an erroneous representation and understanding of the situation .

3.2.1.2. Rules

The rules to automatically assign one CICA to a category are using the presence of key words. The strategy is to first identify the action family to which a CICA belongs. Since each CICA family belongs to a CICA category, the category is then known.

3.2.2. Modeling Systems and components

3.2.2.1. Categories

As described in (Electricité de France 1982; Bourgeois and Tanguy 1996; Libmann 1996), safety in a nuclear power corresponds to three functions:

- Controlling nuclear reaction;
- Cooling core;
- Isolating radioactive materials.

Other components do not fit with this categorization and correspond to support functions, such as interface. This vision gives a grid to list all the components that might have any kind of importance in human factor missions. For instance, the next table gives examples of components, which may be not available for a mission.

First safety function : controlling nuclear reactivity		
	RPN	Neutron activity measurement system
	FBA	Bore injection automatic system
Second safety function : cooling combustible		
	GMPP	Primary pump
	GV	Steam generators
	ASG	Auxiliary GV alimentation
	ARE	Water flows regulation system

Table 10 Systems and components modeling: examples

3.2.2.2. Rules

Each component of this system corresponds to a random variable, whose state space is binary corresponding to true or false. For a given mission, if RPN is “true”, then the neutron activity measurement system is unavailable for this mission. The rules are using the presence of keywords: the database contains a table listing unavailable systems for every mission.

3.2.3. Modeling Requirements

Requirements correspond to actions that the team must accomplish in order to get the mission done. These actions can be expressed by a verb: for instance, the requirement may be the opening of two valves over three of a certain component. Requirements correspond to a step in the use of MERMOS: formulating what is required to accomplish the mission helps analysts to deduce possible scenarios of non satisfaction of these requirements. In order to describe these requirements, analysts are generally using a verb of action, plus the object of the action: for instance: *“Make the diagnostic that the secondary loop is unavailable”*. Analysts are imagining how the team may not diagnose the unavailability of the secondary loop.

It appeared that the number of actions corresponding to requirements is finished and contains 18 items. The rules to state the category of requirements consists of testing the presence of these verbs of action, once the data have been prepared.

3.2.4. Modeling failure modes

Failure modes correspond to the non satisfaction of functional requirements, defined as Strategy, Diagnostic and Execution. In order to accomplish the mission, the team must apply a relevant strategy, perform a relevant diagnostic, and perform the appropriate actions.

Each of these functional requirements has failing modes, identified as:

Situation diagnostic is irrelevant
State diagnostic is irrelevant
Situation diagnostic is missing
Situation state is missing
Strategy is missing
Strategy is irrelevant
Execution is irrelevant
Execution is missing

Table 11 Failure modes

3.2.5. Context and situation features

The context of a scenario contains the specific part of the analysis. The situation features describe the necessary conditions for the CICAs to appear and are consequently highly variable. Their number is not constant, varying from 1 to 5 situation features for the missions “Feed and Bleed”. The probability of the context varies significantly, in function of the scenarios. For the missions “Feed and Bleed”, these probabilities vary from 0 (corresponding to situation where the analysts were not able to identify a possible scenario and so there is no identified context) to 1 (the context will happen surely regarding this situation).

It did not seem feasible to identify key words that would help to categorize them. However, main conceptual categories have been identified, depending on what the situation features are applied. Indeed, situation features describe the socio-technical environment in which human operators are working. As described by (Rousseau and Largier 2008; Hollnagel 2009), contextual features may play a role in accidents. It is clearly taken into account by MERMOS since the analysts have to imagine the context that may lead to a given CICA which may lead to an accident, corresponding to a mission failure.

Context	**Characteristics**	**Subject**	**Description**
Social and organizational context	Team characteristics	Training, experience and individual behavior	Situation features may be linked to the training of the members of the crew. A lack of training might lead to the appearance of a certain CICA. A lack of experience might be involved too. Individual reaction may lead to an accident; these individual reactions may be due to an extra work load, stress due to emergency situations, etc. Context may be concerning any style of leadership of engineers in charge of the crew, or the presence or the absence of the people in charge of the operations. This category of situation features is directly linked to the work of (Hollnagel 2003; Rousseau and Largier 2008; Hollnagel 2009) about the pathogen causes of organizations leading to accident.

	Characteristics of the way operations are managed	Information sharing	Information sharing concerns the way the team is sharing information between its members. Usually, when an analyst is describing information sharing in a situation features, the analyst is describing a situation where information flow is blocked by an individual. This individual does not show any will to transmit any pieces of information, because he/she did not identify these pieces of information as important. It may correspond to an S or R error as described by (Reason 2008; Sockeel, Chatelain et al. 2009). It may be a K error: (Hollnagel 2009) explain how human beings apply a filter to pieces of information.
		Work and tasks splitting	Because the team is in an accident mode, tasks might be reassigned. These changes might imply the suppression of redundancies between the members of the team. For instance, a technical engineer supposed to be helping the water/steam engineer, might be following the procedure. Consequently the redundancy water/steam engineer, technical engineer disappears. This way to consider redundancies is specific to MERMOS and is described in the articles presenting the method.
Technical Context	System characteristics	State parameters evolution	The team makes its decisions based on indicators which describe the process state. The process state might play a role in the decisions of the team, and thus is a part of the context. This category of situation features has been described a lot: it corresponds to the interaction side of the human factors. Clearly, today, the focus has been put on the sociological aspect of human error, as emphasized by (Reason 2008). This category can be linked to problems related to training: it corresponds to the understanding of the team of the state of the process.

		Material related events	Something related to components happens, such as a pump that stops working. Even if this event might be punctual, it can imply changes in the team.
		Technical actions	The team accomplished a technical action such as triggering a safety injection. The analyst considers that this action has a significant influence over the context.
	Characteristics of the available pieces of information	The available information in the control room	The team takes its decision on the light of indicators displayed in the control room. These indicators are known, and listed. They correspond to physical measures that allow the team to follow the process, and to the state of the system, to know how some technical components are working.

Table 12 Situation Features modeling

The freedom the analysts have to express the situation features makes technically impossible to define rules which assign each situation features to a category of the grid. Besides, the number of situation features is totally random. It generates difficulties to produce code to obtain automatically the situation features probabilities and to compare situations. However, it is possible to get interesting pieces of information from the label of the situation features, corresponding to the components which are involved in a given scenario, to specific members of the team, and to indicators. The rules are quite easy since they consist in testing the presence of specific keywords in character chains.

Indicators and measures of physical parameters
Steam generator (SG) level
Steam generator activity
Primary pressure
Steam pressure GV
Pressurizer level
Different tank levels
Core and other temperatures
Radioactivity
Pressure

Table 13 Indicators and measures

Pieces of information about the state of the system
Pumps situation
Level of tanks
Temperatures
Alarms corresponding to unavailable components
Logic feedbacks (position of valves for instance)

Table 14 Indicators about the state of the system

3.2.6. Evaluating rules of association

In order to automate the categorization of these different parameters, rules of association has been created. These rules test the presence of keywords in the labels. CICAs and situation features are specific in the sense they are fully expressed by the analysts. As explained previously, the automation of the categorization of situation features was not possible. For the requirement categories, no case with more than one key-word present in one scenario has been identified.

Rules for CICAs may be subject to mistakes: some CICAs contain more than one key word, and consequently they may happen to more than one CICA category. In order to better consider this situation, another rule has been created. This rule consists in considering that the CICA category is given by the first identified key word.

In order to appreciate the accuracy of the rules of associations for the CICAs, different indicators are developed as mentioned in (Rakotomalala 2008): the confidence, the support and the lift. Support describes how many times a rule has been applied. Confidence describes how many times a rule has been applied when it was appropriate. Confidence would require a study for every scenario: it is not possible to automate it. However, it is possible to create an interval for the confidence. Indeed, in a worst case situation, the specific rule used for the CICAs would generate systematic error. Thus, it is possible to write:

$$Conf \geq 1 - \frac{\text{Number of times of application of second rule regarding this association}}{\text{Number of scenarios dealing with this association}}$$

Confidence is an indicator related to a conditional probability. For instance, if the rule is:

R=(If the word “Valve” is present, then the category is “Open”)

Then the confidence of this rule is (Rakotomalala 2008):

$$\begin{aligned} Conf(\mathrm{R}) &= Conf(\text{If the word “Valve” is present, then the category is “Open”}) \\ &= \mathrm{P}(\text{Category is "Open"}|\text{"Valve" present}) \end{aligned}$$

The lift must be superior to 1 if the rule is relevant. It corresponds to an odd-ratio: the lift is an indicator explaining the likelihood of the rules. It appeared that the rules are relevant and quite accurate, according the appreciation and examples given in (Srikant, Vu et al. 1997).

CICA categories	category A	category B	category C	category D	category E
Support	15%	26%	37%	5%	17%
Confidence	91%	81%	99%	90%	85%
Lift	5.96	3.13	2.69	17.17	5.00

Table 15 Rules evaluation

3.3. Method for identifying similar scenarios

3.3.1. Bayesian network: a promising tool

A Bayesian Network is a directed acyclic graph of “nodes” and “links” that conceptualize a system. The nodes express random variables which belong to different sets of states. Each relationship between nodes is expressed by conditional probability that gives the dependencies between nodes(Corset 2003; Department of the Environment 2009).

Bayesian networks are used in order to represent the knowledge obtained from the model defined in phase 1. The objective of this study is not to develop any improvement about Bayesian modeling but to use in order to identify recurrent patterns among the existing analyses: The literature deals with techniques of modeling with Bayesian networks, such as (Corset 2003) and (Lauritzen and Spiegelhalter 1988): these two documents give a first introduction to Bayesian networks: definitions, interesting properties, evidence propagation. Other articles such as (Hojsgaard 1996) are more focused on strategies to develop a model using Bayesian networks. The problem with Bayesian networks is the numerical explosion that makes it necessary to find a compromise between reality and a reasonable model.

3.3.2. Objectives of the Bayesian Network and the research algorithm

According (Rakotomalala 2008; Department of the Environment 2009), the first step consists in defining the objectives of the Bayesian network. In the context of this study, it is a tool that represents analyses. If some parameters are specified, some key configurations will appear in the Bayesian network.

A family of missions corresponds to a set of missions having similar properties. These properties are identified by the method of search of similar missions carried out by the analysts. They are looking for missions having given unavailable components and given initiators. They can be looking for missions with key words (for instance, the missions which contain the words “BORE” in their labels). In order to find sets of example missions the method consists in looking for missions having components in the same state:

1. Initializing: there are J components that might be unavailable. $j \in [\![1; J]\!]$
2. Imposing the component j as unavailable; other components are available.
3. Identifying all the missions involving the component j as unavailable.
4. Identifying the missions in 3 which are similar from a meaning perspective.

5. Deducing the appropriate key words from the missions identified in 4, if it is appropriate. If not, go to 1, with $j = j + 1$
6. Perform a research based on these key words to identify the missions belonging to this set (or example mission category): check that the obtained missions constitute a set of mission and thus can be used to create an example mission. Go to 1, with $j = j + 1$.
7. Stop if all the components have been studied (when $j = J$).

A mission belongs to a mission category if and only if the label of this mission contains the key words defining this mission category. Inside the mission category there are some subparts corresponding to unavailable components. Looking for keywords is necessary, because missions are not described with the same quality and some components might have been written as available even if they are not. Once the key words are identified, it is then possible to assign a rule: IF (presence of key words in the label of the mission) THEN (the mission belongs to the category of missions). The rest of the study is focused on a specific example mission, corresponding to the feed and bleed missions, as described previously.

3.3.3. Construction of the influence diagram

3.3.3.1. Influence diagram based on current practices

The way the research is accomplished reveals connections between parameters. When analysts are applying the delta method, they start to look for the missions having a specific key word. Then, the research is getting more accurate thanks to unavailable systems and initiators. Once analysts have a set of potentially appropriate missions, they look for the best one thanks to the scenarios, by means of a research based on CICAs and requirements.

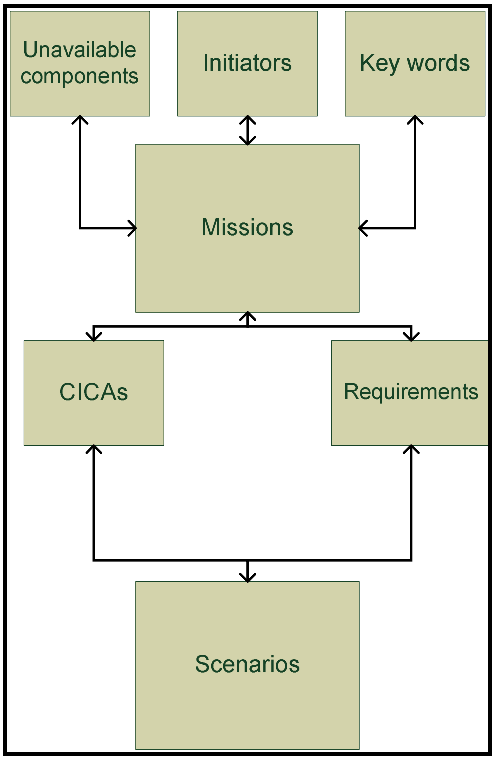


Figure 2 Relationships given by the way analysts use the database

3.3.3.2. Building the model for the example mission "GAVE-OUVERT" (GO) or "Feed and bleed"

Missions containing the key words "GAVE-OUVERT" compose the set of missions corresponding to the example "feed and bleed" missions. These missions are linked to two components: ASG and ARE. Depending on the states of these components, 3 main patterns are identified:

- ARE and ASG are TRUE: it corresponds to 68% of the "feed and bleed" missions;
- ARE is TRUE and ASG is false: it corresponds to 24% of the "feed and bleed" missions;
- ARE is false: it corresponds to 8% of the "feed and bleed" missions.

However, the pattern of research described previously does not allow one to identify configurations having a significant weight in the set of the "feed and bleed" missions. It means that relationships are missing. When an analyst works on a mission, he/she considers every failure modes, and then imagines requirements from these modes. The non satisfaction of a requirement is a way to find the failure modes. In the MERMOS method, as described in the bibliography related to the method, a CICA corresponds to configurations that make possible the non-satisfaction of the requirements. Consequently, a CICA is connected to requirements and to failure modes; requirements and failure modes are connected too.

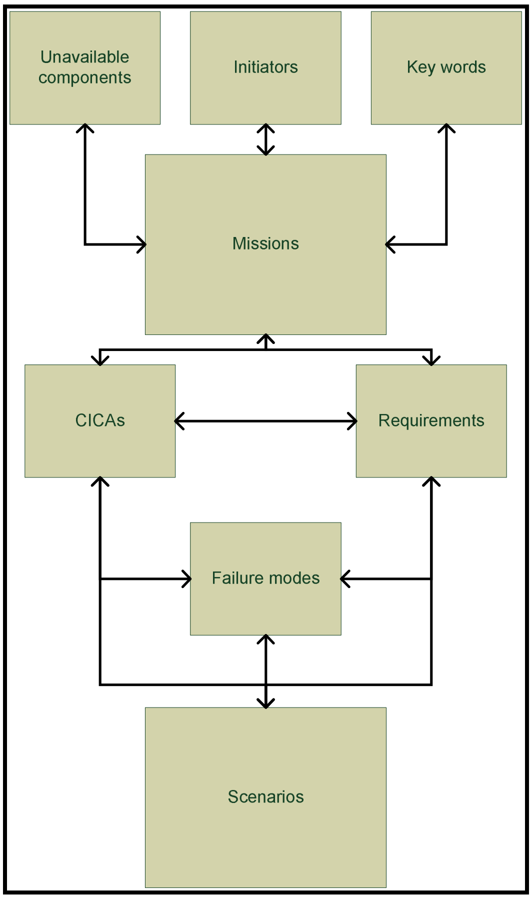
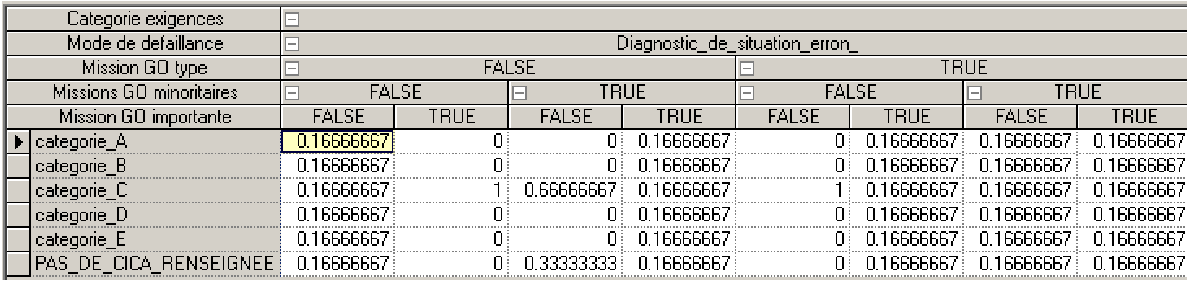


Figure 3 Relationships given by accident theories complete the previous model

3.3.3.3. Getting conditional probabilities

Conditional probabilities are obtained from the database, and correspond to weights of each parameter regarding all the configurations seen in the “feed and bleed” missions. It is important to underline that these probabilities are not the probabilities estimated by the experts. Clearly, these probabilities are just used to identify the recurrent patterns among the scenarios.



Categorie exigences	⊟							
Mode de defaillance	⊟ Diagnostic_de_situation_erron_							
Mission GO type	⊟ FALSE				⊟ TRUE			
Missions GO minoritaires	⊟ FALSE		⊟ TRUE		⊟ FALSE		⊟ TRUE	
Mission GO importante	FALSE	TRUE	FALSE	TRUE	FALSE	TRUE	FALSE	TRUE
categorie_A	0.16666667	0	0	0.16666667	0	0.16666667	0.16666667	0.16666667
categorie_B	0.16666667	0	0	0.16666667	0	0.16666667	0.16666667	0.16666667
categorie_C	0.16666667	1	0.66666667	0.16666667	1	0.16666667	0.16666667	0.16666667
categorie_D	0.16666667	0	0	0.16666667	0	0.16666667	0.16666667	0.16666667
categorie_E	0.16666667	0	0	0.16666667	0	0.16666667	0.16666667	0.16666667
PAS_DE_CICA_RENSEIGNEE	0.16666667	0	0.33333333	0.16666667	0	0.16666667	0.16666667	0.16666667

Figure 4 Conditional probabilities: screenshot of the conditional probabilities table from (GENIE-SMILE 2009)

Let's explain the two first column values.

- The first column corresponds to the case:
  - Requirement is : "PROCESS FASTER"
  - Failure mode is: "Inappropriate situation diagnostic"
  - The states of ASG and ARE do not correspond to a possible case. However, the software needs to know the repartition, even if this case will never happen.
- The second column corresponds to the case:
  - Requirement is : "PROCESS FASTER"
  - Failure mode is: "Inappropriate situation diagnostic"
  - The mission is a main one: the components ASG and ARE are both unavailable.
  - All the missions corresponding to this configuration concerns systematically a CICA of category C.

Technically, getting these probabilities is not difficult since it is easy to specify research based on the states of the variables and to count occurrences satisfying a given state. However, the number of probabilities to obtain is enormous: for the table of probabilities of the CICA, 2430 probabilities are required.

3.3.4. Limit of this approach

Until that point, a method to identify example missions and scenarios has been identified and implemented over the GO missions. However, this method does not consider the quantitative knowledge contained in the database. An analyst does not simply describe the situation that might lead to a failure of the mission; the analyst quantifies this risk too. This Bayesian network may be seen as a map which proposes paths that lead from a certain configuration of parameters such as unavailable systems, failure modes and requirements, to the failure of the mission, specified by a scenario and probabilities which have been estimated by the analysts. By means of a Bayesian network, it has been possible to identify patterns among the qualitative part of the analyses performed by the experts.

The objective is now to study if the identified categories can explain the quantitative results. In other words, if the categories make sense, then the scenarios corresponding to a same category (defined by a category of CICAs, a category of requirements and the sates of the unavailable components) must have similar probabilities.

The next chapter will show that other pieces of information are missing and must be considered in order to explain, partially, the quantitative results given by the analysts.

3.4. Extended method for improving quantitative analysis: a data centered approach

3.4.1. Introduction

The problem involved with this project is to map some low-level data into other forms, corresponding to example missions and example scenarios. (Fayyad, Piatestsky-Shapiro et al. 1996) propose a methodology to achieve this purpose: indeed, this objective is exactly in the field of Knowledge Discovery in Database (KDD); data mining is a step in the KDD process. The main steps are selecting the data of interests and processing it. The operation of data mining follows. The final step is a phase of evaluation and interpretation of the results. It is in the phase of data mining that the use of the knowledge related to accidents theories is required in order to explain relationships among data.

Indeed, it is important to keep in mind that the model does not necessarily corresponds to reality: the purpose is not to create a model of accidents in a nuclear power plant; but to develop a model of how analysts are performing analyses in order to help them in this task. Consequently, even if two parameters might be highly correlated in the data, it is important to not create any shortcut rules. The analysts must follow the method described by MERMOS. If the aim was to create a model from data without considering any other pieces of information, the method would have been different. It is even truer since the data are not showing the same quality.

Consequently, the connections between variables must exist because they make sense to the analysts rather than because there are mathematical indicators saying so. However, methods such as multivariate analysis of variance (MANOVA) can be used (Minitab 2007). The objective is to check if the model can explain quantitative results. More specifically, MANOVA tests check if the model explains the variance of the data. It allows to test hypotheses regarding the effect of one or more independent variables on two or more dependent variables.

3.4.2. Positioning the problem about quantitative results

Getting quantitative results has sense only if it is possible to give them with a certain level of trust, or at least with indicators that allow analysts to appreciate their accuracy. This level of trust is directly dependant on the variability of the probabilities that are used to get this result and to the number of records matching the configuration corresponding to the category. The idea is thus to find categories where the entities present close probabilities, without getting sets too small. The question behind that part is dealing with the reuse of the probabilities of the different parameters: is it possible to reuse entirely the analyses already performed, including the probabilities?

3.4.3. Probabilities corresponding to the CICAs

CICA probabilities depend on different parameters: category requirements, the failure mode, the type of mission, and the category of CICA. These intersections correspond to the actual representation of CICA in the model, based on analysts use of the database, and on accident theories. In order to identify the parameters that are supposed to have an influence over the probabilities of the CICAs, a general MANOVA test is performed: it appears that as expected, time requirements does not explain the values of the CICA probabilities. A CICA is thought as a consequence of the context (Bieder, Le Bot et al. 1999). It might be tempting to include the type of reactor in the model. The reactor type might have an influence, but if this criterion was considered too, the number of values to specify would pass from +100,000 to +700,000; the parameters that are considered now correspond to the main ones (MANOVA test results are displayed in Appendix 3).

3.4.4. Probabilities of situation features

The context is related to the type of reactors. Initially, MERMOS has been constructed in order to better take into account the changes of interface and control in the N4 type reactor (Pesme, Le Bot et al. 2007).

Reactor type name	Number of scenarios
LO_N4_EPR	19
LO_900_CPY	8
LO_900_POST_VD3	8
LO_1300_POST_VD2_(incendie)	25
LO_CPY	166
LO_PQY_DPY	143
LO_1300_VD2_REX	223
LO_N4_POST_VD1	234
LO_N4	212
LO_Type	21

Table 16 States corresponding to the different types of reactors, with the number of occurrences

In order to decrease the number of states, 900MWe reactors and 1300MWe reactors are regrouped. The possible states for the random variable corresponding to the kind of reactor are thus:

Reactor type name	Number of scenarios
LO_N4_EPR	19
LO_900_POST_VD3_CPY	16
LO_1300_VD2_REX_POST_VD2_(incendie)	248
LO_CPY	166
LO_PQY_DPY	143
LO_N4_POST_VD1	234
LO_N4	212
LO_Type	21

Table 17 Grouped states corresponding to the different types of reactors, with the number of occurrences

The situation features are extremely variable: they are describing the context that might see the appearance of the CICA leading to the accident. Consequently, it is necessary to study these contexts one by one in order to identify similarities for the scenarios corresponding to a given example scenario. Situation features correspond to a context: MERMOS gives accurate and subtle results (Pesme, Le Bot et al. 2008) because it is possible to imagine the context that might lead to the appearance of a certain configuration of human operators, leading to the mission failure.

Since it is asked to analysts to imagine this context, they may have an influence on the quantification of the probabilities. However, a procedure has been deployed in order to validate the analyses: a first analyst performs the study. Then, a second analyst checks this result; the research and development team may check the analysis. Then, a final analyst, specialist of human factors studies, validates the study.

3.4.5. Probabilities of non-reconfiguration

In order to consider these probabilities, it is necessary to include other parameters to the model. The probabilities of non reconfiguration give an idea of how likely the system would not change its configuration, what may lead to the failure of the mission. Time occupies an important part in this configuration: with an infinite time, the system will surely reconfigure. On the opposite, the shorter the mission is, the more unlikely the mission changes and thus the lower the probability of non-reconfiguration is. Consequently, time requirements are added to the model to explain these probabilities (details of MANOVA test are given in Appendix 3).

3.5. Global view over the model

Consequently, the most important part of the model is dealing with the type of reactor, the CICAs, the requirements, the failure modes, and the time requirements. It gives contextual elements, and probabilities corresponding to the states of the different parameters of the system, helping to deduce the catastrophic scenario. The next figure gives a global view over the model.

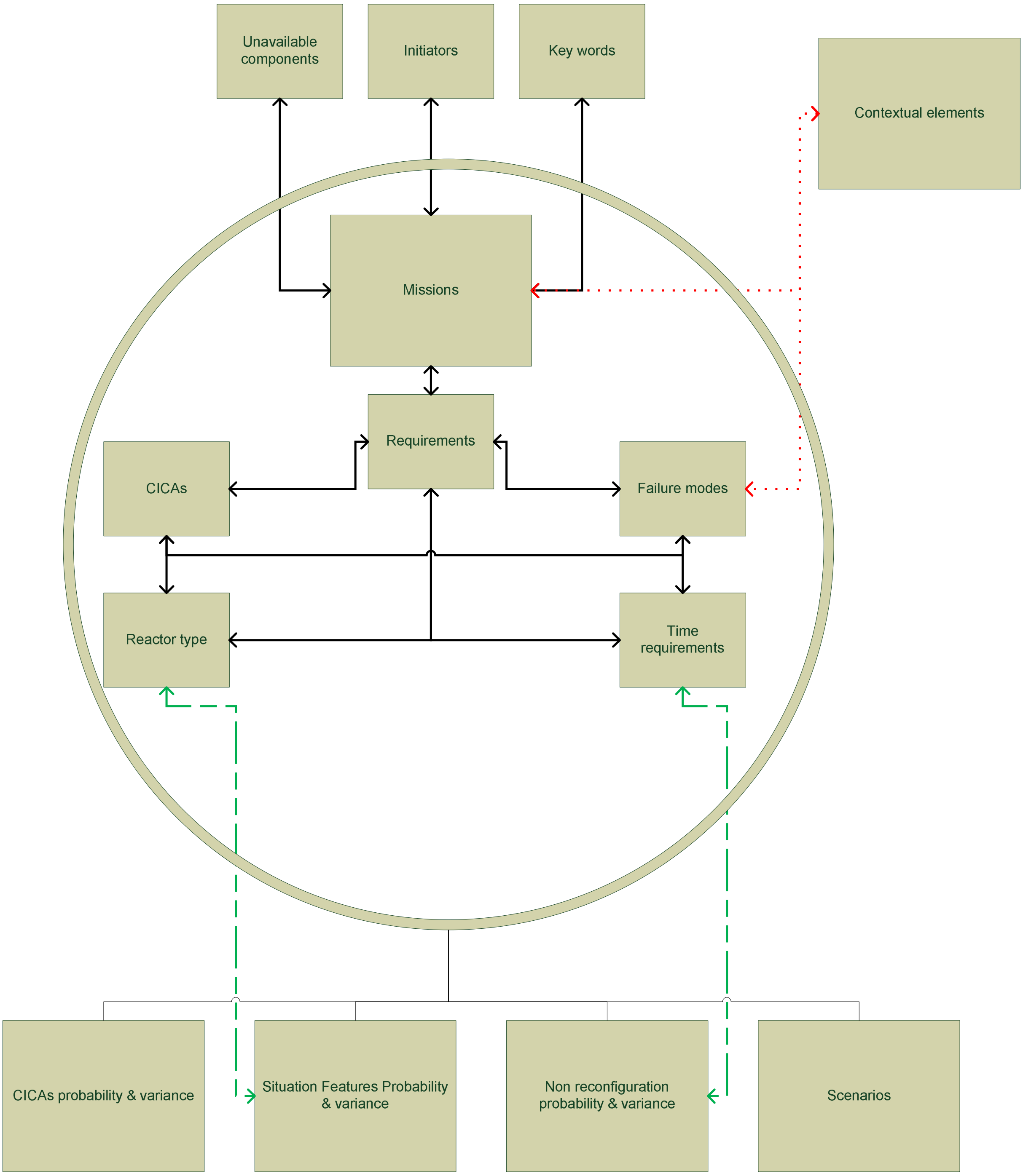


Figure 5 Global view over the model

3.6. Relation with other models

In order to understand the model of the MERMOS analyses, it is interesting to compare it with another model. Until that point, the methodology consisted in starting from the analyses and to create a more general representation (approach “bottom-up”). Now it is interesting to fit this approach in a “top-down” context in order to explain this representation in a more generalist way.

In (Le Bot and Pesme 2009) a model of errors of commission is proposed in the context of the analyses developed with MERMOS. The next figures summarize this approach. It is interesting to notice that the results found with the model developed for this study are compatible with those presented in (Le Bot and Pesme 2009). In addition, it gives an interesting direction to organize the example scenarios. As an illustration, the next figure describes the matching between the model developed for this study and the one describing the connection between errors of commission and MERMOS. Next figure only deals with execution failures.

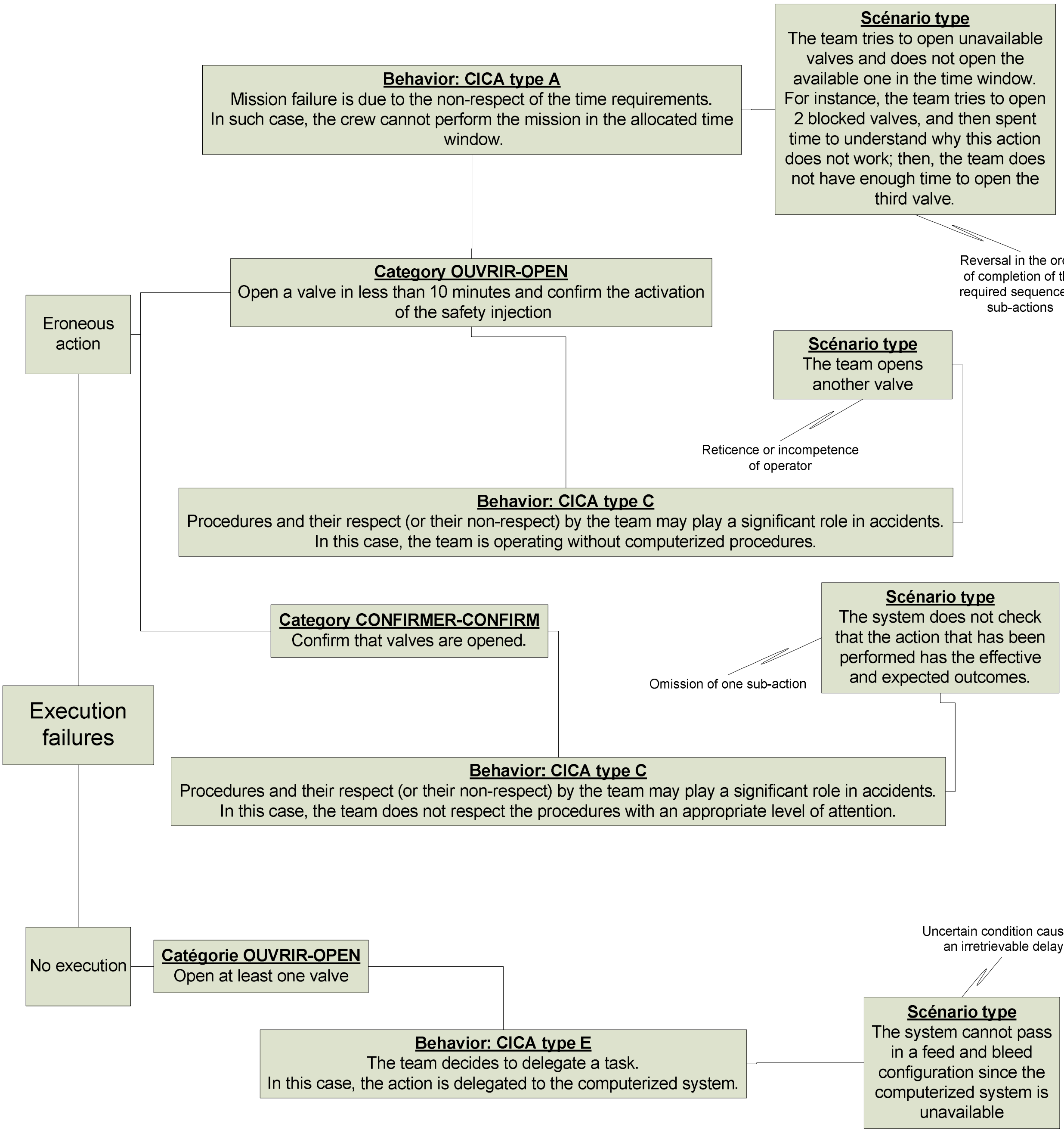

Scénario type
The team tries to open unavailable valves and does not open the available one in the time window. For instance, the team tries to open 2 blocked valves, and then spent time to understand why this action does not work; then, the team does not have enough time to open the third valve.
Behavior: CICA type A
Mission failure is due to the non-respect of the time requirements. In such case, the crew cannot perform the mission in the allocated time window.
Reversal in the order of completion of the required sequence of sub-actions
Category OUVRIR-OPEN
Open a valve in less than 10 minutes and confirm the activation of the safety injection
Eroneous action
Scénario type
The team opens another valve
Reticence or incompetence of operator
Behavior: CICA type C
Procedures and their respect (or their non-respect) by the team may play a significant role in accidents. In this case, the team is operating without computerized procedures.
Scénario type
The system does not check that the action that has been performed has the effective and expected outcomes.
Category CONFIRMER-CONFIRM
Confirm that valves are opened.
Omission of one sub-action
Execution failures
Behavior: CICA type C
Procedures and their respect (or their non-respect) by the team may play a significant role in accidents. In this case, the team does not respect the procedures with an appropriate level of attention.
Uncertain condition causing an irretrievable delay
No execution
Catégorie OUVRIR-OPEN
Open at least one valve
Scénario type
The system cannot pass in a feed and bleed configuration since the computerized system is unavailable
Behavior: CICA type E
The team decides to delegate a task. In this case, the action is delegated to the computerized system.

Figure 6 EOC and the model of the example MERMOS analyses

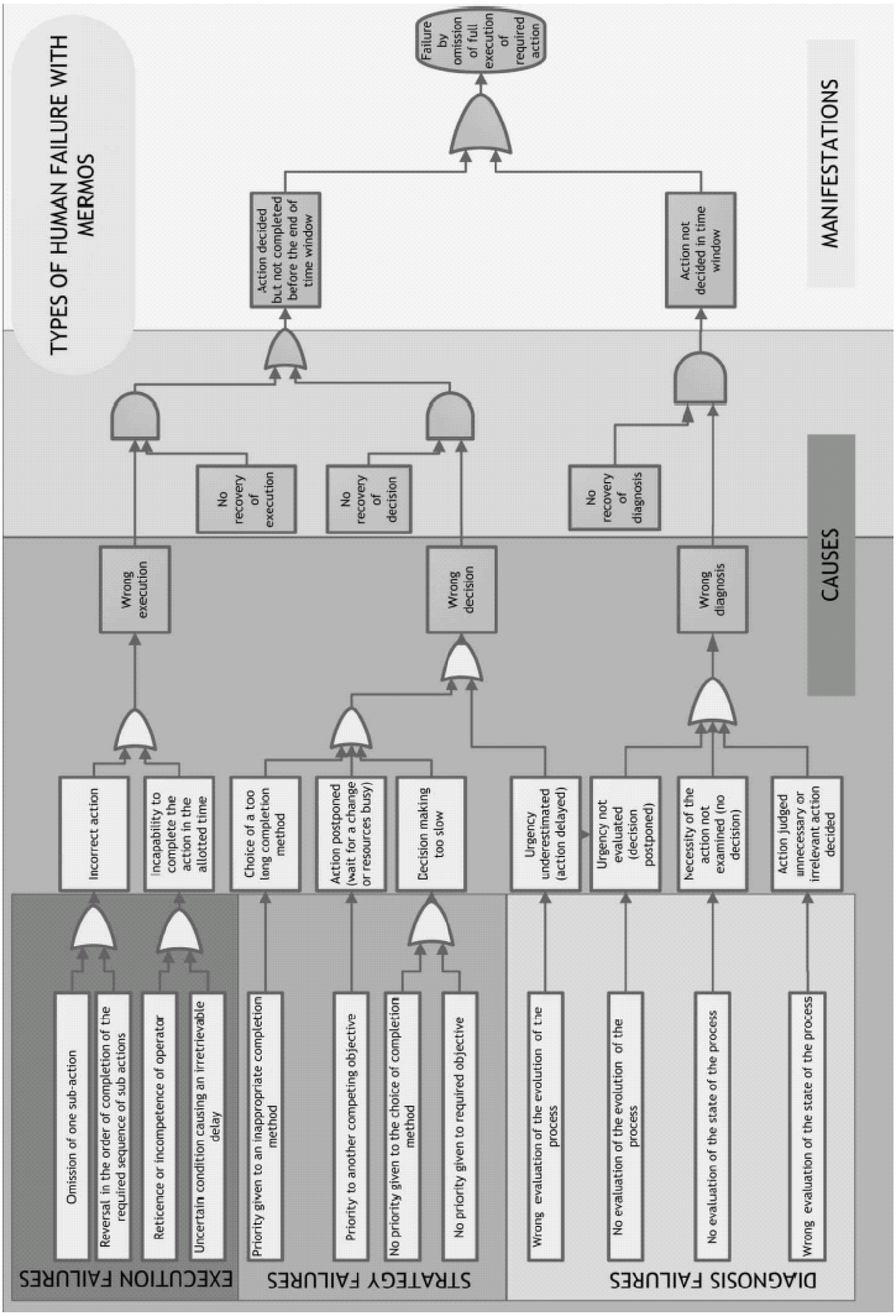

TYPES OF HUMAN FAILURE WITH MERMOS
Failure by omission of full execution of required action
Action decided but not completed before the end of time window
Action not decided in time window
MANIFESTATIONS
No recovery of execution
No recovery of decision
No recovery of diagnosis
CAUSES
Wrong execution
Wrong decision
Wrong diagnosis
Incorrect action
Incapability to complete the action in the allotted time
Choice of a too long completion method
Action postponed (wait for a change or resources busy)
Decision making too slow
Urgency underestimated (action delayed)
Urgency not evaluated (decision postponed)
Necessity of the action not examined (no decision)
Action judged unnecessary or irrelevant action decided
Omission of one sub-action
Reversal in the order of completion of the required sequence of sub actions
Reticence or incompetence of operator
Uncertain condition causing an irretrievable delay
Priority given to an inappropriate completion method
Priority to another competing objective
No priority given to the choice of completion method
No priority given to required objective
Wrong evaluation of the evolution of the process
No evaluation of the evolution of the process
No evaluation of the state of the process
Wrong evaluation of the state of the process
EXECUTION FAILURES
STRATEGY FAILURES
DIAGNOSIS FAILURES

Figure 7 Manifestations and causes of failure from (Le Bot and Pesme 2009) page 6, used under fairuse

3.7. Final representation of the systematization method

Thus, this study revealed that it is possible to build example scenarios respecting a certain structure as described in the next figure. This structure corresponds to a certain hierarchy among the identified key parameters of the example MERMOS analysis. It appears that an example scenario depends qualitatively on a required function, a failure mode, a requirement category, a CICA category. Quantitatively, it depends on some component states, time requirements and of the type of reactor.

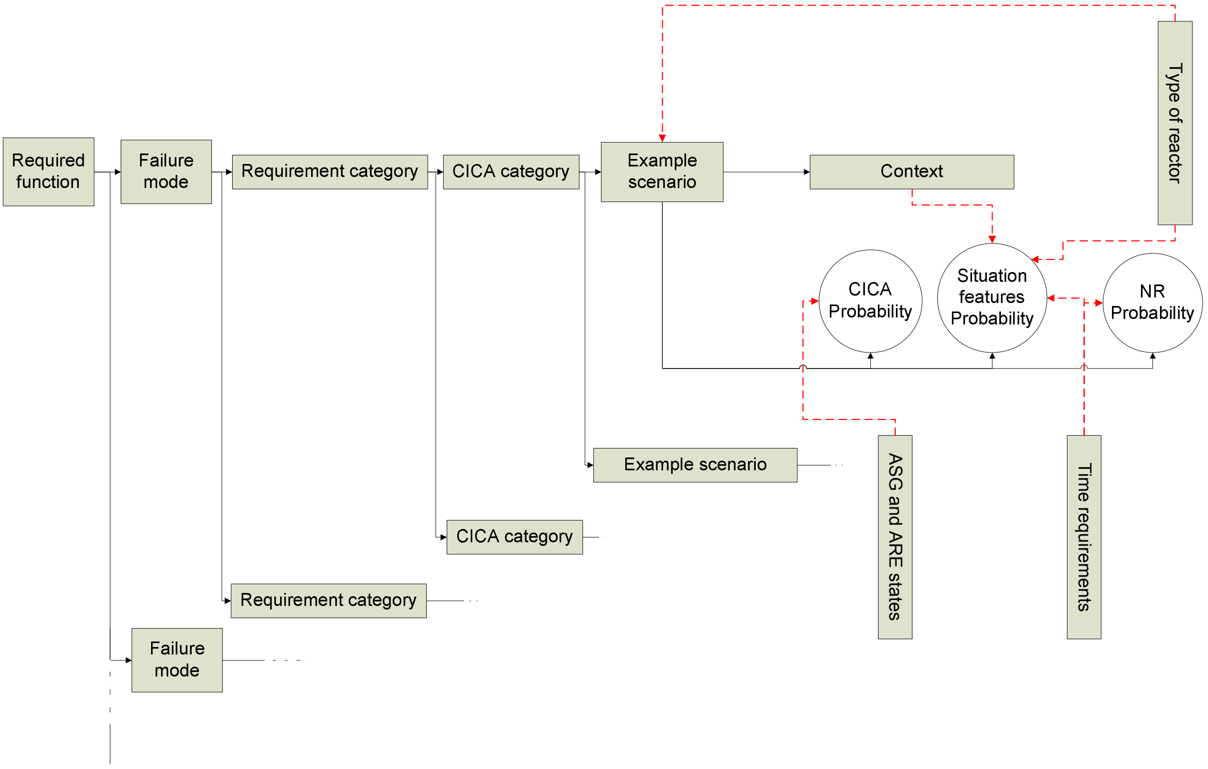


Figure 8 Overview on the systematization method (red links correspond to quantitative relations and the plain black ones to qualitative relations)

4.Evaluation of the systematization method

4.1. Introduction

MERMOS is used in an industrial context and thus must present a compromise between the cost to use it and the quality and the quantity of the outcomes. As mentioned in (Le Bot, Pesme et al. 2002), the limits of this method come from “the cost overrun due to the quality of the required analyses”. This thesis outlined several points expected to decrease the time spent and the requirements in terms of background of the analysts. (Spurgin 2009) identified cons for the use of MERMOS. These cons are described in page 100 and deals mainly with the protection of the method by EDF: the data and the method are proprietary contents. (Bell and Holroyd 2009) emphasizes the necessary resources to use the method.

4.2. Evaluations

The three elements that have a significant impact in the time spent to perform an analysis are:

- The analysts’ experience;
- The originality of the analysis to perform;
- The validation of the analysis.

Without considering example scenarios, in the context of a first analysis, 4 days/man are necessary in order to collect the necessary data and to perform the first step of the mission, consisting in identifying and defining the HF mission through a functional analysis. When it is about reusing an existing analysis, 1 day/man is necessary (Le Bot, Pesme et al. 2002).

Comparisons	Expected evolution with the potential evolution identified in this thesis	Reasons of saved resources
The analysts' experience	The methodology presented in this thesis helps to identify example scenarios. These example scenarios will help analysts to deduce more easily new analyses from the existing ones. Consequently, experts will be relying less on their own expertise and more on the knowledge acquired by the engineering departments doing the human reliability studies. It means that junior analysts will be more likely to be able to perform analyses.	Example scenarios give the general pattern of any scenario. The analysts select the appropriate example scenario regarding the specificities of the study they are performing. Example scenarios can be seen as grids of analysis.
The originality of the analysis to perform	If the analysis to perform corresponds to an innovative study, then this analysis is outside the scope of this thesis. However, by being able to identify if the analysis to perform corresponds to an innovative case or not quickly, the time of research of similar example scenarios is then decreased.	The time to perform an innovative analysis is not changed. However, the time spent to identify an innovative situation is decreased.
The validation of the analysis	Since the example scenarios are composed by certified scenarios, it seems reasonable to expect a decreased time spent to check the validity of the analyses if, and only if the example scenario is used without any changes.	The examples scenarios have to be validated by experts. Any analyses deduced from an example scenarios will be checked regarding the context of application. If the example scenario is used without any changes, only the context would have to be checked since the rest of the analysis corresponds to an example scenario already certified through the validation process. If the analyst changes the example scenario in order to make it fit the current analysis more closely, a complete verification must be performed.

Table 18 Outcomes of the study

By identifying example scenarios, the robustness of the method is increased. The analyses will be carried out regarding specific configurations, and thus it will not be possible to have different quantitative results for a same configuration. Clearly, creating example missions and scenarios will force analysts to consider the general consensus when they are quantifying the probabilities of their analyses.

4.3. General implementation: feasibility and overview

This thesis has been focused on the “feed and bleed” missions only. A systematic approach has been proposed in order to identify example scenarios for this family of missions. The implementation would start with a bottom-up approach to identify all the mission families. It consists in varying unavailable components in order to identify patterns (such as the pattern linking the “feed and bleed” missions with the components ASG and ARE). The implementation of example scenarios for the entire database would respect the next plan:

- Identifying keywords which define a mission family
    - By means of unavailable components by considering missions having a common unavailable components and then by identifying the common points they are sharing;
- Obtaining the analyses containing these keywords and checking they belong to the mission family;
- Then, each scenario of this mission family is processed:
    - identification of the CICA category;
    - identification of the context category;
    - identification of the requirement category;
    - identification of the failure mode;
    - identification of the HRA family;
    - identification of the time requirements.
- Identifying example scenarios as the intersection of a CICA category, a requirement category and a failure mode category;

- For a given configuration, corresponding to a type of reactor, a failure mode, a requirement category, a CICA category, evaluating the probabilities corresponding to the CICA;
- For a given configuration, corresponding to time requirements, a failure mode, a requirement category, a CICA category, evaluating the probability of non-reconfiguration;
- For each example scenario, studying the context in order to identify the main situation features and their probabilities, in function of the type of reactor and the time requirements.

The work to identify examples missions and example scenarios is considerable. However, the potential saved resources to perform future analyses justify this investment. Next table gives estimations of the expected resources necessary to the deployment of the methodology.

Task	Expected time	Expertise	Results
Identifying keywords which help to identify a mission family			
By considering missions having common unavailable components and then by identifying the common points they are sharing.	1 week	**High level of expertise**: The analyst must be able to understand and to explain conceptual sense of relations between missions sharing common unavailable components. It implies to be proficient in understanding the relations between technical components and procedures.	List of all the mission families (such as "feed and bleed")
Then, each scenario of this mission family is processed:			
Identification of the CICA category	3 days per mission family	**Low level of expertise**: It corresponds to an automated task consisting in looking for already identified keywords. No background in nuclear reliability is mandatory. The work involving the modeling of the safety systems has already been carried for the purpose of this thesis.	A database containing categorized scenarios for a given family mission
Identification of the context category			
Identification of the requirements category			
Identification of the failure mode			
Identification of the HRA family or of the type of reactor			
Identification of the time requirements			
Identifying example scenario as the intersection of a CICA category, a requirement category and a failure mode	2 days per mission family	**Medium to high level of expertise** The analyst must identify similar scenarios corresponding to a given configuration. Background in nuclear power plant may be necessary in order to sum up several scenarios.	List of example scenarios of the mission family

For a given configuration, corresponding to a type of reactor, a failure mode, a requirement category, a CICA category, evaluate the context probabilities	1 day per family mission	**Low level of expertise** It is an automated task consisting in looking for already identified keywords	Example scenarios with quantitative results
For a given configuration, corresponding to time requirements, a failure mode, a requirement category, a CICA category, evaluate the probability of non-reconfiguration			

Table 19 Resources

4.4. Use of this work for IDAFH

IDAFH (Data & Human Factors Analyses Integration) is the piece of software currently deployed at EDF in the engineering departments performing HRAs. It will be used to perform any new analysis and to justify it by means of data and documents.

As it has been described, the MERMOS method corresponds to a dynamic process of creation of knowledge about human reliability. The tool that the analysts are going to use will help to justify analyses from both qualitative and quantitative points of view. The access analysts have to knowledge is made easier by means of data contained in the database. This knowledge includes both data on potential behavior (the existing MERMOS analyses), and data on known behavior (the reports of observations of behavior in a simulator or during real incidents, and the information needed to estimate how frequently the contexts causing the failure scenarios occur). Consequently, IDAFH will help to capitalize analyses and data and make easier the access to them (Le Bot 2005).

However, because of the variability of the data contained in the database, any research based on keywords does not return all the appropriate analyses. Besides, the research tool included in this software does not correspond to the way researches are performed regarding the example scenarios. Thus, an evolution is clearly dealing with the freedom of specifying quantitative and qualitative results: if an analysis corresponds to an example scenario, then the analyst should define it as the example scenario he or she is referring to.

4.5. Conclusion

In this chapter, the feasibility and the interest of this method to get example scenarios have been studied. It appears that the positive outcomes are clearly of interest, but that they represent a significant investment in terms of resources. In addition, it will increase the general knowledge about human reliability in the nuclear power plants. IDAFH will be used to reuse example scenarios.

5. General conclusion

Research and innovation are a priority at EDF; the willingness to improve reliability of nuclear power plants impulses the exploration of human reliability. The creation and the implementation of the MERMOS method illustrate this concern. However, it is necessary to consider the context of application of the method. The use of MERMOS in an industrial context showed some weaknesses that would be decreased if its robustness and its reproducibility would be increased. This thesis has proposed some ways to increase these two aspects of the MERMOS method.

A model explaining relationships between parameters of the MERMOS example scenarios has been built. This model was used to identify example scenarios and clearly showed the possibility to create a model of these analyses using a bottom up approach. The example scenarios will help analysts to deduce more easily an analysis from a given context. However, the general implementation has still to be done. But even if it represents a significant quantity of resources, the expecting saved resources would justify this investment.

In addition to this work, opportunities for further researches have been identified. Once all the example scenarios are known, it will be interesting to find elements influencing the performance of the team. More specifically, this work would be an opportunity to regroup several works and researches about performance shaping factors (PSF). As described in (Groth and Mosleh 2010), the term PSF encompasses the factors that may affect human performance and can change the likelihood of appearance of errors. In the context of the example MERMOS scenarios, identifying them would be made easier and it would be possible to identify their influence on a final probability of appearance of accidents. It would be an interesting decision making tool that would be used in the risk management of the nuclear power plants.

References

Bell, J. and J. Holroyd (2009). Review of human reliability assessment methods, HSE. **RR679**.

Bieder, C., P. Le Bot, et al. (1999). What does a MERMOS analysis consist in ? PSA'99. Washington, USA.

Bourgeois, J. and P. Tanguy (1996). La Sûreté Nucléaire en France et dans le Monde, Polytechnica.

Corset, F. (2003). Aide à l'optimisation de maintenance à partir de réseaux bayésiens et fiabilité dans un contexte doublement censuré. Mathématiques appliquées. Angers, Joseph Fourrier. **Docteur de l'université Joseph Fourrier**.

Damerau, F. J. (1964). "A Technique for computer detection and correction of spelling errors." Communications of the ACM **7**(3 (March 1964)): 171-176.

De la Garza, C. and P. Le Bot (2006). L'analyse de situations de simulation en conduite incidentelle/ accidentelle dans le nucléaire : mise en évidence d'une performance collective. ERGO IA. Biarritz.

Department of the Environment, W., Heritage and the Arts of Australia (2009) "Technical Report no 9 A beginners guide to Bayesian network modelling

for integrated catchment management."

Dhillon, B. S., - (2009). Human reliability, error, and human factors in engineering maintenance with reference to aviation and power generation. Boca Raton :, CRC Press.

Electricité de France, D. d. l. é. (1982). Eléments de Sûreté et de radioprotection des centrales nucléaires de 1300 MW.

Fayyad, U., G. Piatestsky-Shapiro, et al. (1996) "From Data Mining to Knowledge Discrovery in Databases." American Association for Artificial Intelligence (AI magazine) **Fall 1996**, 37-54.

Forester, J., A. Kolaczkowski, et al. (2007). ATHEANA User's Guide, Final Report. NRC. Washington, DC, 20555-0001.

GENIE-SMILE (2009). GENIE SMILE, University of Pittsburgh Decision System Laboratory.

Groth, K. and A. Mosleh (2010). A Performance Shapping Factors Causal Model for Nuclear Power Plant. PSAM 2010.

Hojsgaard, S. (1996) "Learning Structures from Data and Experts." Mathematics and Computers in Simulation **42**, 143-152.

Hollnagel, E. (2004). Barriers and accident prevention.

Hollnagel, E., - (2003). Human reliability analysis in support of risk assessment for positive train control

Human reliability analysis : context and control. Washington, DC : Cambridge, MA :

London ; San Diego, CA :, U.S. Dept. of Transportation, Federal Railroad Administration, Office of Research and Development, Research and Special Programs Administration ; John A. Volpe National Transportation Systems Center

Academic Press.

Hollnagel, E., - (2009). The ETTO principle : efficiency-thoroughness trade-off : why things that go right sometimes go wrong. Farnham, England ; Burlington, VT :, Ashgate.

Hollnagel, E., D. D. Woods, et al. (2006). Resilience engineering : concepts and precepts. Aldershot, England ; Burlington, VT, Ashgate.

Hood, C. and D. K. C. Jones (2001). Accident and Design. Contemporary debats in risk management, Routledge LTD.

Humphreys, P. (1987). Human Reliability Assessors' Guide.

Largier, A. (2008). Organisations A Risques, Cours Ecole des Mines de Nantes. Nantes, Ecole des Mines de Nantes/ IRSN.

Lauritzen, S. L. and D. J. Spiegelhalter (1988). "Local Computations with Probabilities on Graphical Structures and their Applications to Expert Systems." Journal of the Royal Statistical Society. Series B (Methodological) **50, No 2**: 157-224.

Le Bot, P. (2000). La prise en compte du facteur humain: de la defaillance humaine a la dafaillance du systeme de conduite. MRI. EDF, EDF.

Le Bot, P. (2003) "Human Reliability data and accidents models; illustration throught the TMI accident analysis." Reliability Engineering and System Safety **83 (2004)** 153–167.

Le Bot, P. (2005). La prise en compte du facteur humain: de la defaillance humaine a la defaillance du systeme de conduite. Fiabilite humaine. E. RetD.

Le Bot, P. (2005). The Use of Expert Judgment in Decision Making; Using expert judgement with MERMOS : from static assesment towards knowledge capitalisation. European Commission. Aix en Provence.

Le Bot, P., C. Bieder, et al. (2000). Feedback from the actual implementation of the MERMOS method. PSAM 5. Osaka, Japan.

Le Bot, P., P. Meyer, et al. (2007). The CICA concept for use in the MERMOS method redifined by a new organisational reliability model. congrès IEEE / HPRCT. Monterey CA, USA.

Le Bot, P. and H. Pesme (2009). How to Deal with Commission and Omission Errors in HRA. ESREL. Prague.

Le Bot, P., H. Pesme, et al. (2008). Collecting data for MERMOS using a simulator. PSAM 9
Hong Kong.

Le Bot, P., H. Pesme, et al. (2002). Methodological Validation of MERMOS through 160 analyses. PSA. Detroit, USA.

Le Bot, P., C. Remond, et al. (1996). Plus de 10 ans de simulation de scenarios accidentels: un bilan des essais "MSR". congrès IERE. E. RetD. Tokyo.

Leveson, N. (2004). "A New Accident Model for Engineering Safer Systems." Safety Science **42**(4).

Libmann, J. (1996). Eléments de Sûreté Nucléaire, Les Ullis.

Meyer, P., P. Le Bot, et al. (2007). MERMOS : an extended second generation HRA method. congrès IEEE / HPRCT. Monterey CA, USA.

Minitab, I. (2007). Minitab. 14.

Perrow, C. (1984). Normal accidents : living with high-risk technologies. New York :, Basic Books.

Pesme, H., P. Le Bot, et al. (2007). Little stories to explain Human reliability Assessment : a practical approach of the MERMOS method. congrès IEEE / HPRCT. Monterey CA, USA.

Pesme, H., P. Le Bot, et al. (2008). Insights from the “HRA international empirical study” : how to link data and HRA with MERMOS. ESREL. Valencia.

Rakotomalala, R. (2008). "Les Regles d'association." Retrieved April 2nd 2010.

Reason, J. T. (2008). The human contribution : unsafe acts, accidents and heroic recoveries. Farnham, England ; Burlington, VT :, Ashgate.

Rousseau, J.-M. and A. Largier (2008) "Industries à risques : conduire un diagnostic organisationnel par la recherche de facteurs pathogènes." les Techniques de l’Ingénieur **AG 1 576**.

Sockeel, P., E. Chatelain, et al. (2009). "Les chirurgiens peuvent apprendre des pilotes: place du facteur humain en chirurgie." Journal de Chirurgie **146**(3): 250-255.

Spurgin, A. J. (2009). Human Reliability Assessmen Thoery and Practice CRC Press.

Srikant, R., Q. Vu, et al. (1997). Minin Association Rules with Item constraints. KDD 97, AAAI**:** 67-73.

Stellman, J. M. (1998). Encyclopedia of Occupational Health and Safety. I. L. Office. Geneva, Intenational Labour Office. **2**.

Swain, A. D. (1976). Shortcuts in human reliability. Generic techniques in systems reliability assessment. E. a. L. J.W. Leyden: Noordhoff**:** 393-410.

Swain, A. D. (1990). "Human reliability analysis: Need, status, trends and limitations." Reliability Engineering and System Safety **29**(3): 301-313.

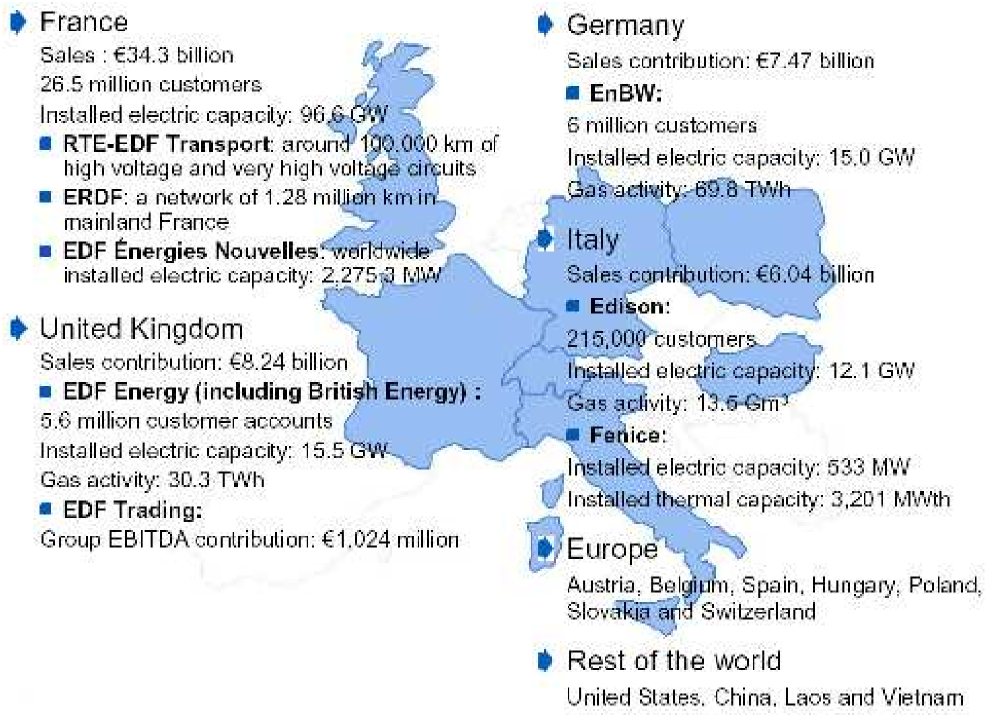
Westrum, R. (2006). Topology of Resilience Situation. Resilience Engineering: Concepts and Precepts. D. W. Erik Hollnagel, Nancy Leveson, Ashgate.

Wreathall, J., E. Roth, et al. (2001). Human Reliability Analysis in Support of Risk Assessment for Positive Train Control, Human Factors in Railroad Operations, U.S. Department of Transportation, Research and Special Programs Administration, John A. Volpe National Transportation Systems Center.

Appendix

1. Key figures about EDF

1.1. Worldwide activities



France

Sales : €34.3 billion

26.5 million customers

Installed electric capacity: 96.6 GW

- **RTE-EDF Transport**: around 100.000 km of high voltage and very high voltage circuits
- **ERDF**: a network of 1.28 million km in mainland France
- **EDF Énergies Nouvelles**: worldwide installed electric capacity: 2,275.3 MW

United Kingdom

Sales contribution: €8.24 billion

- **EDF Energy (including British Energy) :**

5.6 million customer accounts

Installed electric capacity: 15.5 GW

Gas activity: 30.3 TWh

- **EDF Trading:**

Group EBITDA contribution: €1,024 million

Germany

Sales contribution: €7.47 billion

- **EnBW:**

6 million customers

Installed electric capacity: 15.0 GW

Gas activity: 69.8 TWh

Italy

Sales contribution: €6.04 billion

- **Edison:**

215,000 customers

Installed electric capacity: 12.1 GW

Gas activity: 13.6 Gm^3

- **Fenice:**

Installed electric capacity: 533 MW

Installed thermal capacity: 3,201 MWth

Europe

Austria, Belgium, Spain, Hungary, Poland, Slovakia and Switzerland

Rest of the world

United States, China, Laos and Vietnam

Figure 9 International activities of the group (from the group website, http://www.edf.com, visited February 2010)

1.2. Status of EDF

Until November 19, 2004, it was a government corporation, but it is now a limited-liability corporation under private law (*société anonyme*). The French government partially floated shares of the company on the Paris Stock Exchange in November 2005, although it retains 84.66% ownership.

EDF was an EPIC (public establishment with industrial and commercial character), and as such, it was subject to the "principle of specialty", that is it had the right to sell electricity; the purpose of this principle of specialty was to prevent EDF competing in an unfair way on their own markets.

2. MERMOS: general use of the method

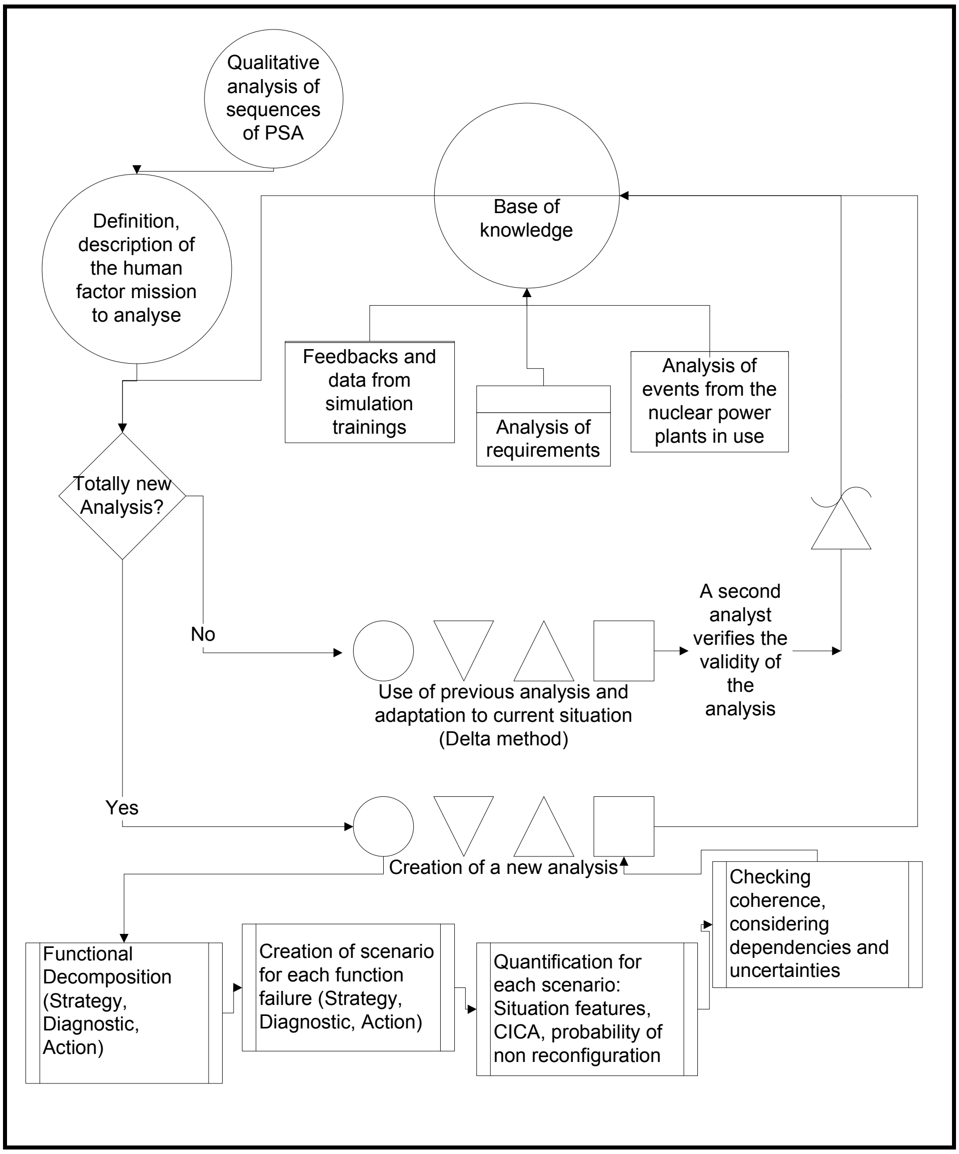

Qualitative analysis of sequences of PSA
Base of knowledge
Definition, description of the human factor mission to analyse
Feedbacks and data from simulation trainings
Analysis of requirements
Analysis of events from the nuclear power plants in use
Totally new Analysis?
No
A second analyst verifies the validity of the analysis
Use of previous analysis and adaptation to current situation (Delta method)
Yes
Creation of a new analysis
Checking coherence, considering dependencies and uncertainties
Functional Decomposition (Strategy, Diagnostic, Action)
Creation of scenario for each function failure (Strategy, Diagnostic, Action)
Quantification for each scenario: Situation features, CICA, probability of non reconfiguration

Figure 10 MERMOS: process of analysis

3. Probabilities: a model giving quantitative results

3.1. Quantitative results about probabilities of non-reconfiguration

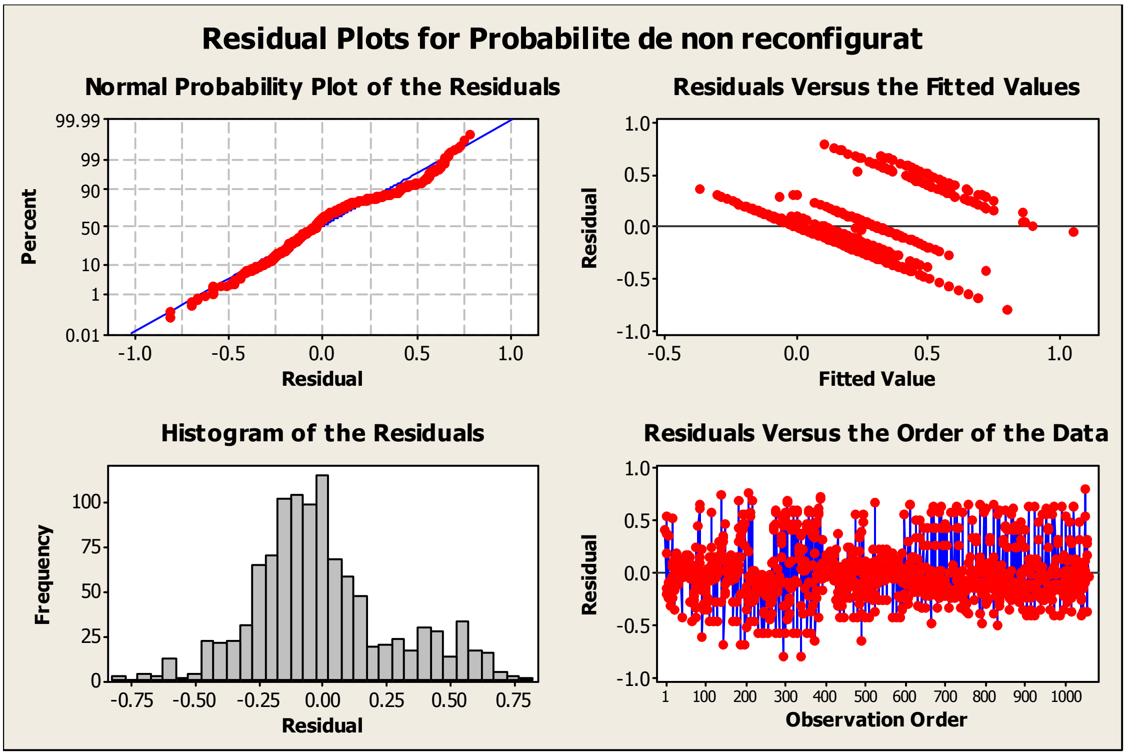


Figure 11 Residual Study for the situation features probabilities

```
Source                       DF    Seq SS   Adj SS  Adj MS      F      P
Time requirements             5   10.7337   9.0975  1.8195  23.30  0.000
Type of reactor               7    3.9370   3.6672  0.5239   6.71  0.000
Failure mode                  7   17.6112   2.2863  0.3266   4.18  0.000
Requirements Categories      17    8.4982   8.1519  0.4795   6.14  0.000
CICA Categories               5    2.7467   2.4520  0.4904   6.28  0.000
Mission                       2    0.6362   0.6362  0.3181   4.07  0.017
Error                      1015   79.2518  79.2518  0.0781
Total                      1058  123.4148


S = 0.279429   R-Sq = 35.78%   R-Sq(adj) = 33.06%
```

3.2. Quantitative results about CICAs

MANOVA results for the model explaining CICA probabilities values:

```
Source                        DF     Seq SS    Adj SS   Adj MS       F       P
Cicas Categories              5    69.6530   20.9523   4.1905   96.03   0.000
Requirements Categories       17    24.3794    8.0277   0.4722   10.82   0.000
Failure modes                  7     5.0377    4.8053   0.6865   15.73   0.000
Type of Reactor                7     0.7041    0.5746   0.0821    1.88   0.069
Time requirements              5     0.1253    0.1345   0.0269    0.62   0.687
Mission                        2     0.0386    0.0386   0.0193    0.44   0.643
Error                                            1015    44.2892   44.2892   0.0436
Total                       1058   144.2273


S = 0.208889    R-Sq = 69.29%    R-Sq(adj) = 67.99%
```

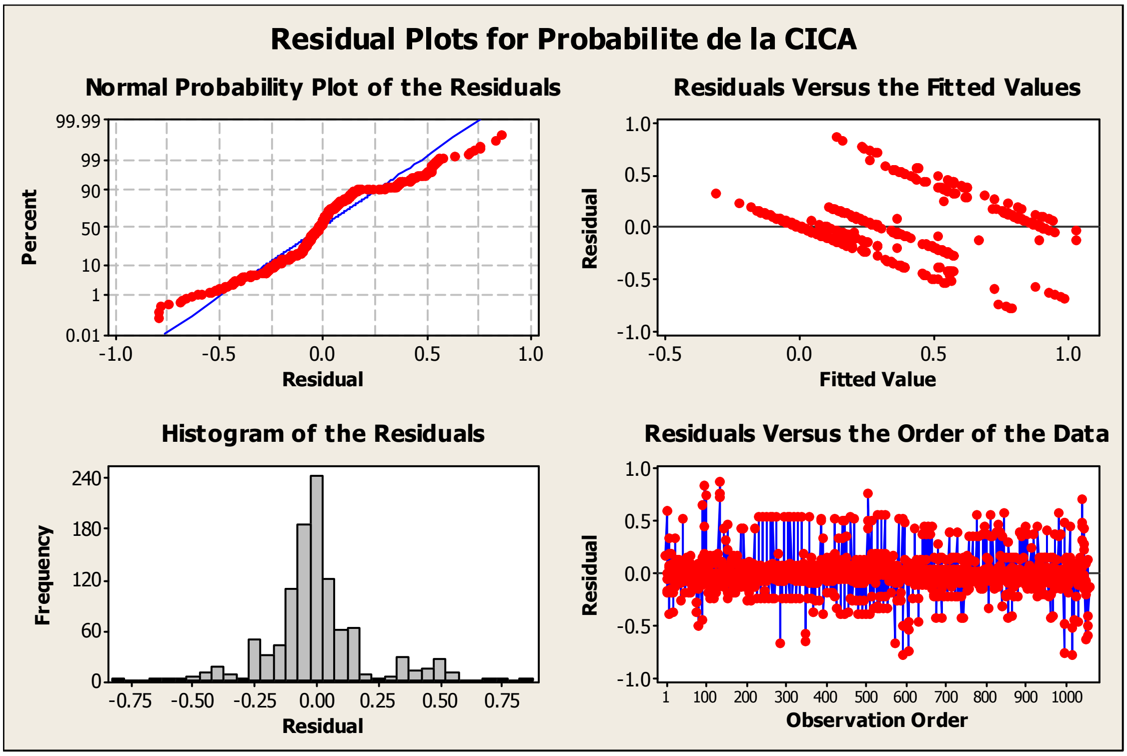


Figure 12 Study of residuals for CICA Probabilities

3.3. Quantitative results about CICAs

```
Analysis of Variance for Produit des probabilites des PS, using Adjusted SS for
     Tests
```

```
Source                              DF     Seq SS     Adj SS     Adj MS        F
nombre propriete de situations       1   0.078593   0.000050   0.000050     0.03
Probabilite du scenario              1   3.416457   2.609578   2.609578  1479.34
Probabilite de la CICA               1   0.022973   0.007564   0.007564     4.29
Categorie de CICAs                   5   0.053513   0.013757   0.002751     1.56
Categorie exigences                 17   0.099981   0.053671   0.003157     1.79
Mission                              2   0.000110   0.000679   0.000339     0.19
Palier                               7   0.051533   0.051468   0.007353     4.17
Mode de defaillance                  7   0.012085   0.012085   0.001726     0.98
Error                             1017   1.794000   1.794000   0.001764
Total                             1058   5.529246

Source                              P
nombre propriete de situations  0.866
Probabilite du scenario         0.000
Probabilite de la CICA          0.039
Categorie de CICAs              0.169
Categorie exigences             0.025
Mission                         0.825
Palier                          0.000
Mode de defaillance             0.445
Error
Total


S = 0.0420001   R-Sq = 67.55%   R-Sq(adj) = 66.25%
```

The next graphs suggest that the model is not sufficient to explain the values:

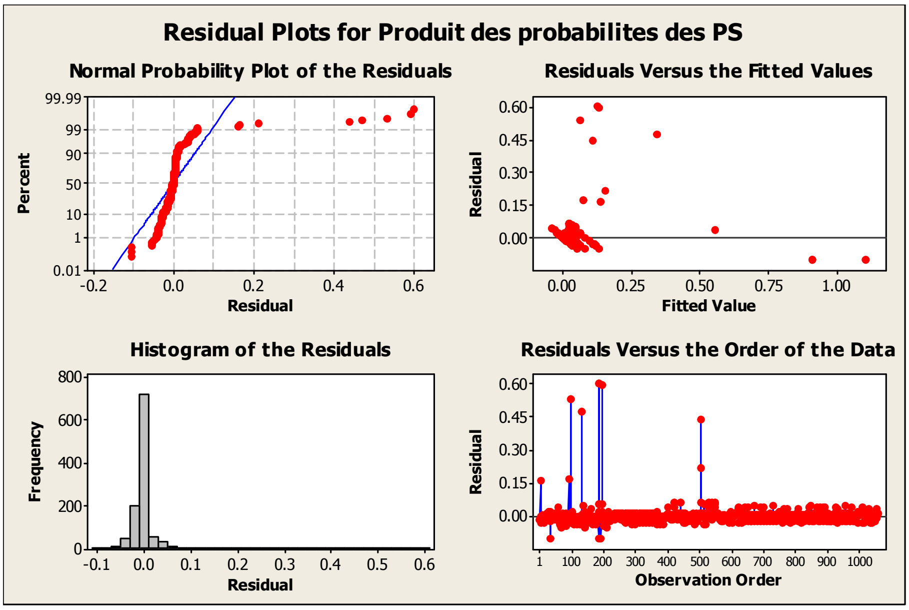


Figure 13 Residual study, Situation Features Probabilities