ELSEVIER

Available online at www.sciencedirect.com

SCIENCE DIRECT®

Reliability Engineering and System Safety 83 (2004) 153–167

RELIABILITY ENGINEERING & SYSTEM SAFETY

www.elsevier.com/locate/ress

Human reliability data, human error and accident models—illustration through the Three Mile Island accident analysis

Pierre Le Bot*

EDF Research and Development, 1 Avenue du General de Gaulle, F-92141 Clamart, France

Abstract

Our first objective is to provide a panorama of Human Reliability data used in EDF's Safety Probabilistic Studies, and then, since these concepts are at the heart of Human Reliability and its methods, to go over the notion of human error and the understanding of accidents. We are not sure today that it is actually possible to provide in this field a foolproof and productive theoretical framework. Consequently, the aim of this article is to suggest potential paths of action and to provide information on EDF's progress along those paths which enables us to produce the most potentially useful Human Reliability analyses while taking into account current knowledge in Human Sciences.

The second part of this article illustrates our point of view as EDF researchers through the analysis of the most famous civil nuclear accident, the Three Mile Island unit accident in 1979. Analysis of this accident allowed us to validate our positions regarding the need to move, in the case of an accident, from the concept of human error to that of systemic failure in the operation of systems such as a nuclear power plant. These concepts rely heavily on the notion of distributed cognition and we will explain how we applied it. These concepts were implemented in the MERMOS Human Reliability Probabilistic Assessment methods used in the latest EDF Probabilistic Human Reliability Assessment. Besides the fact that it is not very productive to focus exclusively on individual psychological error, the design of the MERMOS method and its implementation have confirmed two things: the significance of qualitative data collection for Human Reliability, and the central role held by Human Reliability experts in building knowledge about emergency operation, which in effect consists of Human Reliability data collection. The latest conclusion derived from the implementation of MERMOS is that, considering the difficulty in building 'generic' Human Reliability data in the field we are involved in, the best data for the analyst consist of the knowledge built up through already existing probabilistic analyses.

Keywords: Human Reliability assessment; MERMOS; Human Reliability data; Three-Mile Island accident

1. First part: human reliability data, human error and accident models

1.1. Taking into account Human Reliability in PSAs

The Human Factor (HF) is taken into account at two levels: normal operation and emergency operation. In both cases Human Reliability is concerned with the understanding of 'human error' mechanisms in order to model it. Based on these models, Human Reliability Probabilistic Assessment methods propose ways of collecting Human Reliability data and of calculating failure according to the data.

1.1.1. Normal operation Human Reliability analysis

Normal operation Human Reliability analysis evaluates human activities during normal operation which have an impact either on the occurrence of an accident—meaning, from the point of view of PSAs, the frequency of initiators—or on the conditions for controlling the accident through the deterioration of the availability of the systems necessary for mitigating its consequences.

For instance, the following event initiated by a human error, which occurred in 1993, was used to calculate the initiator 'homogeneous dilution of the primary circuit with RRA system connected':

The unit is under intermediary shutdown in RRA conditions, with RRA connected.

Following an injection of lithine, the on-site agent forgets to close the REA 13 and 122 VD valves. During the following watches, the appearance and disappearance of successive 'abnormal boron content' alarms are attributed to the borometer behavior. Only on the following day, when the borometer indication has dropped below 1900 ppm, is the dilution noticed and stopped.

Generally, the frequency of initiators is studied statistically with no distinction between causes of a human or technical nature. However, it may be necessary

[*] Tel.: +33-1-4765-4546; fax: +33-1-47-6551-73.
E-mail address: pierre.le-bot@edf.fr (P. Le Bot).

0951-8320/$ - see front matter © 2003 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ress.2003.09.007

to understand how human activities contributed to the appearance of the initiator in order to study the dependancy between the circumstances of the accident and further operation.

The study of the deterioration of systems necessary for controlling the accident takes into account causes linked to HF, known in this particular case as 'pre-accident HF'. We must determine here how tasks carried out during common operation activities can render unavailable certain functions that are useful in controlling an accident when they are prompted (this is also referred to as latent error).

1.1.2. Emergency operation Human Reliability analysis

The study of PSA accident sequences helps to identify operation missions whose failure has an impact on how the accident scenario develops. The operating missions correspond to functional objectives for the control of the installation for which the control room operating crew were responsible following the initiator. They are in most cases associated with a performance time frame. There are several methods for carrying out this probabilistic evaluation, often relying on the assessment of human error probability or on broader research for plausible operating scenarios leading to failure (such as the latest method developed by EDF, the MERMOS method [1]).

1.1.3. Data sources

The collection of Human Reliability data is developed in the first place from the operation feedback of the units studied. But one of the most significant data sources is the observation of simulated emergency operation on a full-scale simulator, either during tests devoted to this objective or during operator training. Considering the resources necessary for this type of data collection, many methods rely on the kind of generic data proposed by internationally acknowledged methods such as Alan SWAIN's *Technique for Human Error Rate Prediction* (THERP [2]).

1.2. Data collection at EDF

1.2.1. Data for taking Human Factor into account in systems studies (pre-accident HF)

Today EDF relies on a simplified method for taking HF into account in systems studies. It is assumed that a basic probability covers all risks of error translated by the abnormal position of an actuator, whatever the precise nature of this actuator and the number and nature of manipulations it undergoes.

This basic probability of 3×10^{-2} is corrected, depending on the recovery factors, by a value ranging between 10^{-3} and 1 and according to the equipment involved. The functional study of devices allowing the recovery specific to each type of unit helps to define the value of each recovery factor based on qualitative considerations or on feedback from experience in the park. These parameters are reassessed for each unit after studying the specific recovery factors derived from the qualitative design data and from experience feedback.

1.2.2. Data for assessing emergency operation

EDF's first Human Reliability Probabilistic Assessments were carried out based on the method known as FH6 derived from the THERP and Human Cognitive Reliability (HCR [3]) methods, both based on the prediction of human errors according to the possible type of error and to the context for carrying out the task.

EDF has simplified these methods and uses its own statistics or evaluations by expert judgments, obtained by on-site observation of operating activities or through observation of emergency operation on a simulator, both essential to the collection of qualitative data.

For example, the temporal distribution of the time taken by the safety engineers to arrive in the control room was measured on site. The time taken to carry out specific tasks—such as putting safety equipment into service—was determined during simulations devoted to emergency scenarios. It is important to note that analysts are imperatively requested not to apply the quantitative models mechanically, and to systematically qualify the quantitative analyses they provide based on the wealth of qualitative data that EDF was able to obtain through these simulator tests.

1.3. Observation of emergency operation on simulator

1.3.1. An EDF specificity: MSR tests

MSR tests, initially *'Mise en Situation Réelle'*, or 'Actual Situation tests' later known as *'Mise en Situation Recréée'*, or 'Recreated Situation tests', lead to recommendations concerning organization, training and the design of operating tools. The second objective is to regularly collect quantitative and qualitative data on the performance of crews with respect to incident and emergency operation, in particular to provide information for the PSAs' HRA studies.

The tests take place on a full-scale simulator under conditions that are as representative of reality as possible. The teams are the ones that usually operate in nuclear power plants. The documents used are those used on site. The operators are not informed of the scenarios. The only instruction they are given is to behave as if the simulated event occurred in their own installation. 'The world outside' the control room (auxiliary operators, chemists, etc.) is simulated by the trainers. The tests last between 1 and 3 h. Over 300 tests have been performed since 1984.

1.3.2. A reorientation for observing simulator tests

Owing to its specificities, EDF has the means to regularly set up MSR-type dedicated test campaigns. Abroad, large-scale studies of the same type are less frequent: the collection of data on post-accident HF is often carried out through the observation of operator training sessions on full-scale simulators.

This option was also taken at EDF in recent years in order to make it easier to collect data for HRA, thereby taking advantage of training. Observations are generally made during Situation training; under conditions close to MSRs. Taking advantage of simulator tests is nothing new. Simulator tests on S3C, a prototype used to validate the N4 unit computerized control room, constituted the first source of information about emergency operations specific to the N4 unit and helped to refine the MERMOS method.

1.4. Specificities of Human Reliability data

1.4.1. Trade-offs between the generic aspect of the models and the size of the samples

If the constitutive elements of the model are not generic enough, a large number of tests is necessary to obtain enough samples for making statistical inferences. However, if operator behavior is described too generically even if the robustness of the method is enhanced—the latter becomes barely sensitive to the specificities of the operation studied and less representative of the reality of this behavior. One of the major drawbacks then is that the quantitative results do not take into account improvements brought to operation. This problem is crucial for instance in the United States, where operators using methods such as THERP—or similar methods—have difficulty in assessing the impact of improvements effected through reorganization and training, or through the refinement of procedures.

1.4.2. Rapid obsolescence of data

To avoid relying on models which are too generic, one may be tempted to model erroneous behavior closest to the characteristics of the operation specific to the nuclear unit analyzed. For instance, the FH6 method relies heavily on departures from procedure. The behavior described is, therefore, far from being universal enough to be lasting. A modification of the procedures, such as the one carried out when EDF moved from an event-based approach to a state-based approach, requires re-examination not only of the model, but also of the data.

1.4.3. Collection biases

Several biases inherent in the collection of HF data *make* it more difficult than collecting equipment reliability data (re. article by P. Boutin and R. Nunez, IRSN, in the file ‘Man, organizations and safety’ [4]):

- *Volatility of what is observed*: by contrast with equipment failures, observations often bear on facts devoid of physical manifestation. A fact related to human reliability is rarely immediately accessible, recordable or memorizable; it is ‘developed’ rather than collected.
- *Involvement of the players observed*: observation implicates people directly. It is therefore difficult to escape any individual evaluation. The necessary fear of sanctions aside, the players obviously modify their behavior knowing that they are being observed. Issues of ethics and confidentiality obviously arise. Today, testing protocols make it possible to control this bias.
- *Observers’ competence*: the observation and analysis of emergency operation are doubly complicated by the necessity to understand both rare and complex technical phenomena, as well as human behavior that is even more complex and difficult to access. Only close collaboration between HF specialists and emergency operation specialists allows us to achieve these objectives.

1.5. What is Human Reliability data?

1.5.1. Alternative between consensual data and representative data

Conventional methods such as THERP are very successful for two reasons: the generic aspect of their underlying models makes them easy to implement and therefore robust. Ideally (see Fig. 1), to take advantage of data collection and be able to compare data and models, a generic model of human error should be made available to the analysts together with a database supplied by data collected continually from various horizons.

Whenever an analyst wanted to carry out a predictive analysis, he would then simply apply this model and use generic data according to the characteristics of the analysis to be performed. But what is the validity of this data with respect to the diverse fields in which it will be used? This data may be considered more valuable as a consensual reference than as actually representative of human functioning; it essentially helps to rank and compare Human Reliability assessments, which is a very important industrial and safety objective. On the other hand, very specific quantitative data, such as simulator observations of a nuclear unit, are not often transposable to other fields (other units) given their dependence on the refined specific modelization carried out for measuring and quantifying. Today, methods often reach a trade-off between consensus and representativity.

1.5.2. Qualitative data and quantitative data

No Human Reliability figure can be obtained in a mechanical way from the observation of operation, and given the nature of the quantified phenomena, no direct use of figures obtained in other ways can reasonably be made without being adapted, corrected and validated by an expert analyst. In fact, qualitative considerations, based on qualitative observations, are much more significant for determining the final probability than the rough figure obtained from observation.

1.5.3. Importance of the expert

Rather than talking about the collection of HRA data, one should talk about the development process of knowledge regarding Human Reliability (qualitative as well

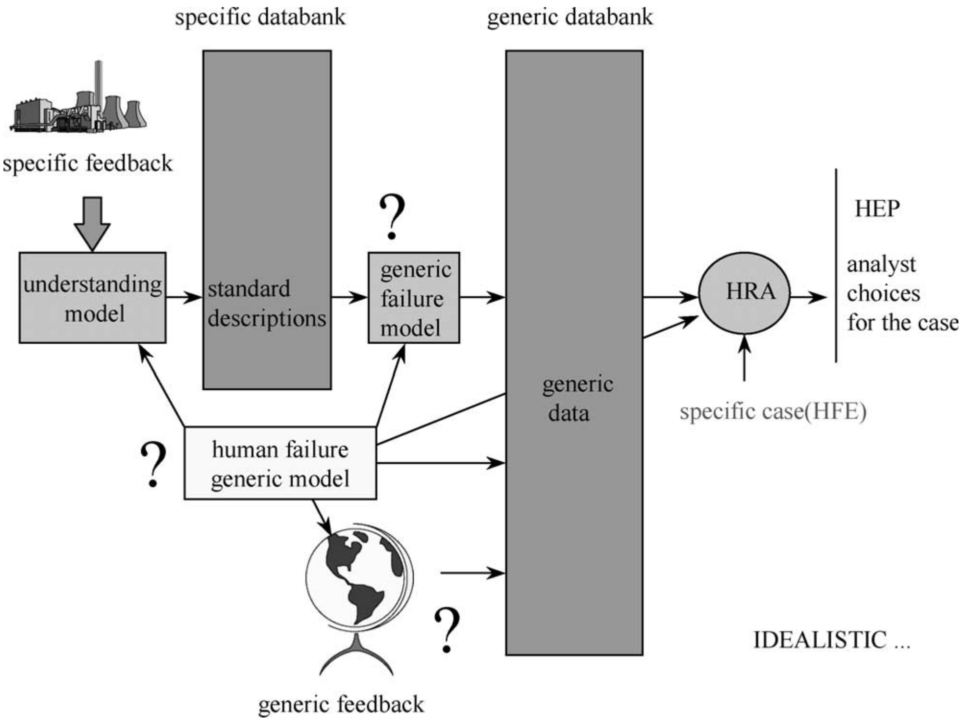


Fig. 1. Ideal approach to the use of generic data in HRA.

as quantitative), and the essential work of the expert at each stage of the process up to the evaluation of possible failure modes and their quantification.

1.5.4. Beyond the data

Human Reliability data collection has extremely positive spin-offs (even if they are not easily…quantifiable). Indeed the necessary collaboration between specialists, the demanding confrontation with the reality of sites and men, involving in particular the repetition on simulator of experiments that are as realistic as possible, all contribute to enriching the company's safety culture and help to spread a more realistic understanding of the HF.

1.5.5. Retrospective knowledge and predictive knowledge

In conclusion, we consider at EDF's R&D that, rather than talking of Human Reliability data, one should talk of 'knowledge'. This knowledge concerns human behavior during emergency operation, for instance, for MERMOS today. Though the analysis of past events (incidents, accidents) is essential, it is difficult to extrapolate this retrospective data in a speculative way with respect to other contexts, such as that of accident scenarios envisaged in the PSAs. This expert work is considerable: if it is well described qualitatively, it constitutes in the end a very rich body of knowledge on the possibilities of operation failure under PSA circumstances, known as predictive knowledge. To facilitate and reinforce the experts' work, it is essential to reuse the development work of predictive knowledge already carried out in the PSAs, reasoning by comparison and modification of the analyses based on the particular context of the study. This process is put into place with the MERMOS method (see Fig. 2).

1.6. A central industrial concept: failure

The very essence of the industrial process relies on the control of a standard world achieved through as simplified a reality as possible. The objects in that world—factory machines installed in enclosed spaces allowing stable operating conditions to be maintained—consist of elements which have been studied and can be replaced by elements with identical characteristics. Productivity depends on removing uncertainty and on the industrialist's ability to ensure the expected behavior.

In such a world, conforming to a model is essential and determines efficiency. Simplification of the real world helps to foresee and control the system's behavior through a robust causal system allowing actions to be taken. This requirement reaches its peak in high-technology industries, as can be seen for instance in the extreme concern for confinement and cleanliness and the elimination of the slightest speck of dust in nuclear power plants or electronic laboratories.

However, reality is stubborn and both engineers and workers well know that it always succeeds in foiling the best designs and operations. The gap between equipment behavior and margins anticipated from its modeling while operating under the expected conditions is unavoidable and is commonly known as failure. The causal meaning of failure is that dysfunctions occur through an unknown cause or one deliberately overlooked owing to simplified model.

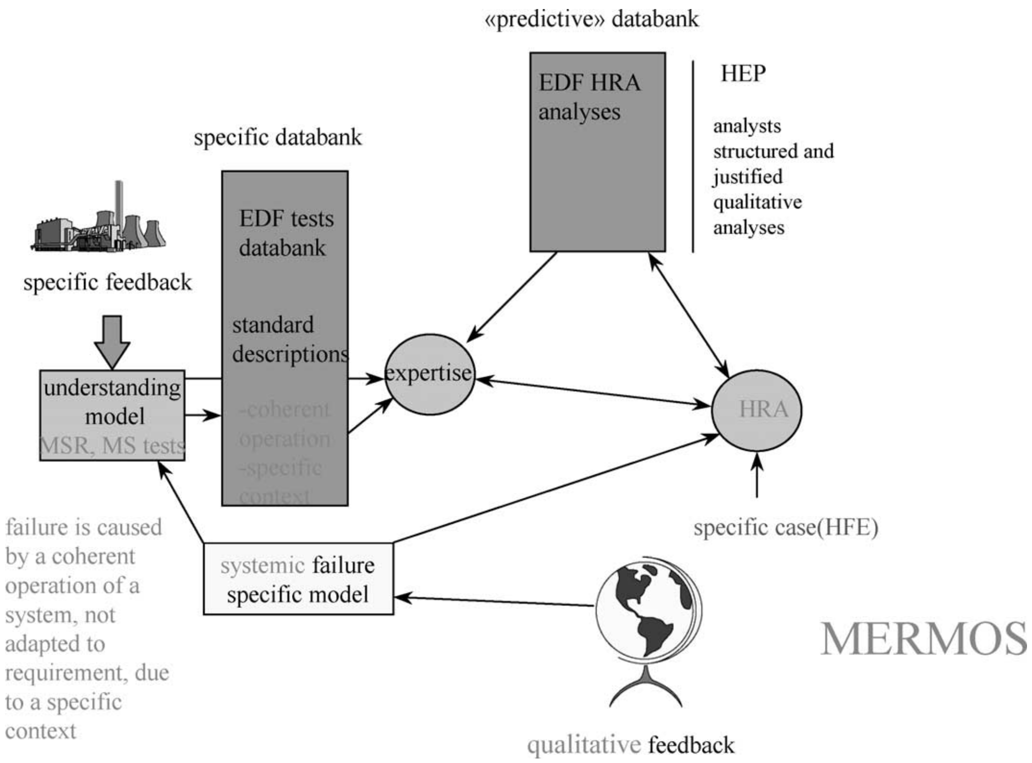


Fig. 2. Approach using MERMOS.

For instance, even if this is considered as most unlikely to happen, the pump of a reactor's safety system may not start on request although it has been properly maintained, its supply is nominal, and control/command has perfectly forwarded the starting order. Post-failure analyses are always able to find the cause if sufficient means are set in motion for the investigation, and the mechanical physics, electrical and thermo-hydraulic laws are never invalidated. For instance, one can highlight the example of sticking due to the loss of the oil film on a shaft. Moreover, it is always possible to argue with hindsight that the cause could have been eliminated before it induced the failure. But this is not possible a priori. Or else the design model should have included the level of knowledge required for post-event analysis, i.e. a more complicated model would have been needed (for instance by taking into account an additional operating condition such as 'presence of an adequate oil film on the pump shaft'), as well as an additional preventive technical device entailing higher cost. In fact, the lack of knowledge about the cause was a risk taken by the industrialist, in the form of potentially random behavior on the part of the equipment. Failure is envisaged before it occurs, as a risk where chance is a causal 'joker' (Lorigny [5]).

Probability may be attributed to failure a priori: it can be extrapolated subjectively from failure statistics of identical equipment in identical conditions.

This notion of failure, typical of the industrial world, is of greatest significance in the approach of risk control based essentially on a priori measurements. The deliberate limitation of reality through modeling introduces an element of randomness into the behavior of the systems designed. It is to be noted that the concept of failure is subjective and totally different depending on whether you consider it before or after the event has occurred. It derives from an arbitrary 'spatial' division of the faulty system and is characterized by a break in time (before and after failure).

However, the notion as described here 'goes astray' in practice. It is commonly thought that faulty equipment leads to the failure of other equipment, which it supplies, for instance. Here, the notion of failure is more generally associated with the equipment's unexpected functional unavailability.

1.7. Use of the notion of failure in the approach to nuclear safety

The first stage of the approach to nuclear safety consists in identifying possible dangerous events. The determinist industrial approach will reduce the number of such events to a list of major events, which could lead to the release of unacceptable radioactive effluents (simplification through modeling of the infinity of potential major events is a risk which can be assessed through the probabilistic approach: such risks actually exist at every stage of modeling in the approach). Then, an acceptable level of risk is defined (and therefore accepted) for each of these events depending on their estimated frequency. It is the designer's task to set up responses according to the in-depth defense concept, so that the installation presents an acceptable risk. This is the initial design of the installation. To lower the risk to an acceptable level, in-depth defense consists in putting in place several successive lines of defense, which means that a faulty line of defense is replaced by the following one, at each industrial phase (design, construction, operation) and according to three categories (preventing failures, monitoring the occurrence of any deterioration, means of action in case of deterioration).

This is translated at design by the 'barrier' system and the fact that each equipment system that contributes to a line of defense must fulfill the single failure criterion. This means that it must fulfill its function even in case of failure in one of its components. During construction, in-depth defense relies essentially on the quality of the system, i.e. on the formulation of requirements and their verification. A safety reference guide, a set of prescriptions, is defined for operation: the mitigation of accidents is ensured by several lines of defense, from automatic actions supporting the emergency crew to the implementation of procedures. 'A priori' safety demonstration relies on the guarantee that requirements are met.

1.8. Man's role gradually taken into account in emergency management

In the early 1970s the poor performance of computer science (by comparison with today) and the absence of emergency experience feedback actually restricted knowledge about accidents. Simulations of accidents through calculation codes were either highly simplified or very brief (a few dozens minutes). Modeling of the complex interactions between automated systems or human actions was mostly ignored. Design relied on the principle that control of an accident was very quickly ensured by the automatic trigger of safety systems, all of them designed for the situation considered most likely to happen, namely full power. In the event of an accident, the operator's role with respect to safety was very limited. It consisted mostly in shutting down the automatic systems as soon as their operation was no longer useful. Training for incident or emergency situations consisted in 'going through' the maximum transients through a simulated course restricted to the first few minutes depending on the initiator or about a dozen transients per hour. Moreover, the operator was responsible for shutting down these systems in the numerous situations where they were triggered inappropriately, owing to the conservatism of the design of the starting automatisms. The teams were also in charge of preventing the systems from starting during the complex starting and shutdown phases of units. In fact, operators were asked to hamper the operation of the safety systems. According to this logic, the procedural system was underdeveloped, most procedures were drafted during the starting of the unit, and they relied on the operators' experience and know-how for operation. The interface was not actually designed for beyond the short-term and deteriorated operation. Information supplied was meant, therefore, for a nominal operation mode.

If the accounts of the Three-Mile-Island and Tchernobyl accidents were to be summed up functionally, this angle would be particularly enlightening. In the first case, the operators interrupted the functioning of the safety injection system, remaining long minutes without realizing the state of deterioration of the reactor. They had been provided neither with training nor with procedures suited to the accident, which was an 'exception', a specific situation no more 'serious' than the cases of breaks provided for in the design, the major events dreaded at design. In the second accident, they hampered the starting of all the safety systems, actually in accordance with what was most often expected from them, also in a not very serious initial situation, but which they contributed in deteriorating.

What were the consequences of Three-Mile-Island? On the one hand the significance of the role of the operator was acknowledged. Emergency operation became an object of design, together with the operating crew, its procedures, and adapted interfaces. The need for its study was also acknowledged for safety demonstration. On the other hand, each operator was ultimately associated with a safety system in which the same imperatives of modeling were carried over. The expected operator behavior was enriched by its effects on the system. But lacking physical laws for modeling this behavior, and considering the complete inability to build operator behavior in the same way as for a machine, his 'model' behavior has been defined as the implementation of the prescriptions with training. Operator failure was taken into account as a departure from the implementation of operation as defined in the procedures. Several lines of defense were put into place, from the addition of a redundant safety engineer to the development of procedures taking into account operator failures such as State-by-State Approach procedures developed at EDF. The failure of each line has been envisaged, and assessed through the emerging Human Reliability Assessment method.

Naturally one attractive alternative might have been to do away with the operator by extending automation. In addition to its cost, this solution comes up against the complexity of the necessary solutions and the need to provide for the failure of such automatisms. In the same way, the development of supports to operation (in the sense that these devices are not part of the operating system and their use is optional) came up against the fact that they were either essential, and therefore couldn't be optional, or superfluous and therefore useless.

1.9. 'Traditional' relationship between performance and accident

Therefore, today, in a deteriorated situation safety is ensured by an emergency operating system consisting of an organized team of operators supplied with a set of procedures and an interface dedicated to the management of these emergency situations. According to this logic the performance of operators with respect to safety is associated with correcting the implementation of means of action specified in the safety reference guide, meaning compliance with the procedures and the prescribed organization. This point of view is supported by the inability to assess the safety of operation through the result, owing to the high performance level of this system. Even on a simulator it is very rare, if not impossible, to observe the degeneration of a deteriorated situation up to the feared accident. And for a deteriorated situation not to degenerate, an operation is necessary (translated by actions as well as absence of actions). Failure of this operation is associated with a succession of operator failures (usually, at least a 'macro error' not followed by recovery in time: cf Fig. 3). To assess the probability of this failure, in the absence of observable data a human failure model will have to be built based on observable and therefore quantifiable behaviors: usually these will consist in observable departures from the expected operation in actual operation or on simulator, which will be called 'errors'. A direct link is thus established between errors made in observable operation and the probability of occurrence of an accident. To work out the probability of this error, it will be assumed that in a context deriving from a deteriorated situation, characterized by a finite number of factors (PSF: 'Performing Shaping Factors'), there exists a probability of operator error. The most sophisticated models will assume a mechanism for the production of errors making it possible to determine a direct relationship between the degree of PSFs in a situation and the probability of error.

1.10. Limits of the traditional approach

Experience acquired at EDF's R&D in the analysis of actual and simulated events shows the poor productivity of this model which relies on the notion of human failure or error in the field of probabilistic accident forecast. Though it is undeniable that errors (as understood by psychologists) are observable in quantity, no mechanism of error production was evident; nor was it quantifiable, except through a simple statistical process. Moreover, the causal links put forward in the processes for the prediction of accidents (succession of failures) are difficult to observe in actual incidents.

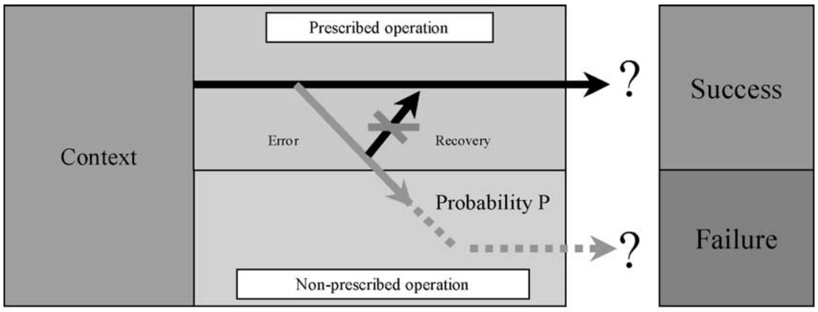
The ergonomic analysis of the operating activity on simulator revealed the complexity of the operators' behavior in such situations, which is certainly not reducible to a binary model of the proper behavior for carrying out the expected operation versus an erroneous behavior, such as that of a machine. Links between situation characteristics and the activity of each operator are hardly reducible to a causality relationship (where the presence of the necessary causes inevitably produces the effect, and the absence of effect requires the absence of at least one cause).

However, knowledge of the current processes allows us to state that an operator failure is not enough to lead to the dreaded accident and that, seen under this angle it would require a set of failures involving all the lines of defense consisting of self-recovery, redundancy in the team, redundancy of procedures, etc. However, the assumed independence of the failure mechanisms makes it impossible for these 'events' to occur simultaneously. Obviously dependency exists between these failures, which denies the independent random character of these failures, or rather invalidates the model used.

A new point of view was therefore necessary. This step was covered on the occasion of the Human Reliability Assessment of operation in the computerized control room of the last EDF nuclear units.

1.11. Evolution at EDF in analyzing the reliability of computerized operation [6]

In the N4 nuclear unit control room equipped with a computerized interface called 'KIC', reliability is distributed throughout the system. Automatic checks of the various



A single context
P= probability of a non recovered departure from the prescribed operation
Prescribed operation = operation avoiding an accident
Non prescribed operation = dreaded accident

Fig. 3. Failure model based on error.

steps of procedure computerized by the KIC are a redundancy factor, which contributes to reducing errors in carrying out low-level actions according to procedures. However, errors detected by the KIC, but confirmed by operators, reflect deliberate operator choices, and correspond to an additional redundancy level. Moreover, since it structures more significantly the operators' action than in conventional control rooms, the technical system reflects quite directly the design choices and the designers' outlook on the operation to be adopted depending on the state of the unit. Operators can rely, therefore, on an operation recommended at design, adapting it to specific circumstances, which add an additional redundancy element to the system.

At any rate, the operation produced will be the result of the multiple interactions between the diagnostic developed by the operators and that derived from the implementation of the procedures, between the operation strategy envisaged by the operating crew and that inherent in the procedures, and between the means mobilized by the crew and those provided for in the procedures. In a computerized operation environment, such as that of the N4 unit, it is even more difficult than in conventional environments to look at the crew's performance as independent of the organization, and vice versa: to define the border between the crew's field of action and that of the technical system; to isolate the contribution of the organization from that of the operating crew and each of its members.

1.12. Distributed cognition; a theoretical framework for understanding operation

The theoretical framework, which is better equipped to conceptualize the rich interaction between the operation players and the technical environment of the N4 control room, is distributed cognition as developed by Hutchins in his book 'Cognition in the wild' ([7]) and in a series of articles including 'How the cockpit remembers its speeds' ([8]) translated into French. Distributed cognition is defined as a new branch of cognitive sciences dedicated to the study of (i) the representation of knowledge both in the mind of individuals and in the world; (ii) the spreading of knowledge among individuals and between individuals and artifacts; (iii) transformations that structures of knowledge undergo when implemented by individuals and artifacts.

Three properties of this theoretical framework are particularly relevant for the study of operation carried out by a system where agents and artifacts are so closely associated.

1.12.1. A supraindividual unity of analysis from the outset

In one of Hutchins' recently mentioned works, the cockpit is the unit the structure and behavior of which are studied. During landing maneuvers, control of the essential parameter of the opening of the wings with respect to the weight and speed of the aircraft is carried out through the integration, by the pilot, of information provided by the interfaces, piloting guidebooks, and the co-pilot. The form and robustness of this integration process depend on the particular information format and the context in which this maneuver takes place. The N4 computerized control room constitutes also a distributed cognition unit gathering a phenomenal knowledge of operation not only mastered by the agents, but also deposited, and made available by other operating experts, in the artifacts of which it is made.

1.12.2. The unity of analysis is defined through the functions it fulfils

The control room, as the cockpit, was designed and developed through time in order to solve specific problems raised by the operation of nuclear units. It is a repository of solutions to operating problems, developed and passed on by the organization. The artifacts, which constitute the control room, play a tremendous mediation role between the operators who use them and the designers and users of this same artifact who contributed to creating and shaping it. By interacting with artifacts, operators integrate a share of other operation experts' knowledge and know-how. Hutchins refers to this in speaking of collaborative manipulation: 'the process through which we take advantage of artifacts designed by others, sharing ideas through time and space'. One of the examples given by Hutchins is that of a sea map; each time it is used, the cartographer who drafted it contributes to the navigating activity, thereby creating a type of long-distance collaboration.

1.12.3. Operator behavior within the operating system

Within the operating system, the functioning of operators has two essential properties. It is both collective, since the unit consists of all the participants in operation, whether or not they are all present in the control room. It is not necessarily deliberate, since artifacts partly control behavior, guiding the choice of certain actions and monitoring their implementation by the operator.

1.12.4. Reliability of the operating system

Each nuclear park unit therefore determines a specific version of the operating system designed and built to fulfill the function of maintaining and recovering the safe and normal operation of nuclear units. These socio-technical systems invariably comprise a psychological dimension, an organization, complex control/command technical systems, interfaces, instructions, operation rules and documentation, as well as a cultural dimension expressed through practices and shared values.

1.13. What is the framework for defining reliable operation?

What do we mean by reliable systems? How can we judge the reliability of a system? And how can we improve it? We have just defined reliability as a property of the distributed system fulfilling the operating function through the multiple interactions of its components (neither the operators' actions, nor the organization, nor the technical systems only). In order to assess whether a system is reliable and to what degree, one must begin by laying out a frame of reference, that is to say a normative operation model against which the operation carried out by the system can be assessed.

1.13.1. What is prescribed?

In the traditional approaches to reliability, the 'reliable operation' model most often used has been that provided by the operation procedures. The closer the operation carried out by the system to the one prescribed by the procedures, the more reliable the system is considered. Conversely, the more the operation conducted departs from what was prescribed, the less reliable is the system considered. This approach, relying on two strong hypotheses, assumes that for any operation situation there is an appropriate procedure, and that in the end operation is but a choice of this procedure and its proper application. However, we know that a procedure is always defined for a class of situations, and that phases of interpretation and adaptation are necessary before it can be applied to a specific situation. We also know that, in certain cases, following the procedure does not produce the relevant operation. This has produced the paradox of adequate actions, from the safety point of view, classified as commissioning errors because they correspond to departure from the prescribed. The last argument, which convinced us of the need for laying out an alternative reference framework, is the fact that the prescribed framework is an integral part of the operating system such as we have just described it. We would, therefore, have found ourselves in the situation where one of the components of the system constituting operation would also be the model of the operation to be followed, *therefore at the same time judge and jury.*

1.13.2. What is required?

In the field of production of nuclear energy, just as in any other domain of hazardous industries, the missions to be carried out by the operation system to ensure safe functioning are known, and usually modeled in functional terms. It is these missions that constitute the reliability reference framework—required operation as opposed to prescribed operation—which is the objective of the design of operation systems and criterion for the assessment of their performance.

We classify here below the requested operation in task forces:

1.13.3. Task of preserving the situation

These are the tasks carried out to prevent a situation from evolving into a deteriorated situation where a state function would no longer be ensured leading rapidly to the uncovering of the core.

1.13.4. Task of preventing deterioration

These tasks ensure the availability of the necessary means for carrying the above tasks. They consist in monitoring the functioning of the means in service and their efficiency as well as ensuring the availability of the replacement means to be used when one of the means in service becomes unavailable. The failure of these tasks undermines the progress of the previous tasks if the situation ultimately leads to the unavailability of the means used.

1.13.5. Task of improving the situation

These tasks attempt to remedy the deterioration of the situation and their ultimate goal is to eliminate failures and their effects.

1.14. Modeling of the operating system

Once the reliable operation model has been defined, the functioning of the operating system as a whole must be modeled in order to understand its internal logic. Then, the actual operation must be compared with the required operation. Starting from the hypothesis that the system was designed, put in place and modified through time in order to fulfill the operating functions in a safe way, its mode of operation must be studied and its performance assessed in terms of reliability. The operating system always reacts to a situation by mobilizing the available resources, creating a representation of the situation, and putting in place and implementing an operating strategy. Grasping the system's understanding of the situation and the reasons for its operating choices are so many essential elements for understanding the reasons for an eventual operation failure.

Finally, the factors accounting for the mismatch between the required operation and that deployed must be examined. Why, in short, the operating system failed in its safety missions. These factors are located at the level of the various system components: the background of the unit, the interfaces, procedures, training, roles, crew dynamic and its members' personalities and backgrounds. But also at the level of the situation features the system is confronted with, such as a slow evolution of the process or a plurality between several transients.

1.14.1. Important characteristics of emergency operation

The temporal dimension is essential to understand the origins of failures in the operation of hazardous industrial installations. We will remember, for instance, the diagnostic failure which, in the framework of the Three-Mile Island accident, went on for more than 2 h. To penetrate the mechanisms of operation progress, we introduced the concept of Important Configuration of Emergency Operation (CICA or, *Configuration Importante de la Conduite Accidentelle*); an ad hoc concept built for the needs of reliability analysis, deriving its meaning with reference to the operating system defined in the previous sections. This concept enables us to express the fundamental interactive nature of the operating process, stemming from the relationships and exchanges between its various components: for instance, the monitoring of an equipment relying both on human actions and machine operations (KIC/State Based Approach) with, as a background, man/machine relationships (trust, sharing tasks).

1.14.2. Configuration

A CICA corresponds to a functioning pattern of the operating system through time. This pattern consists of a specific organization mode, known as *configuration*, and positioning with respect to the situation, known as *orientation*. The concept of configuration refers to the internal properties of the operating system such as making up a team, kinds of relationships between its members, and the available operating instruments. For instance, a team consisting of two agents has a different configuration than a team of four agents; the same team at the KIC will have a different configuration than at the Auxiliary Panel.

1.14.3. Orientation

The concept of orientation, on the other hand, refers to the operating system's positioning with respect to the situation: its interpretation of the situation, its objectives and priorities, and its attitude towards the operating tools, such as following the procedures step by step.

1.14.4. Inertia

The existence of a configuration and orientation adopted by the operating system is not extraordinary as such. The system has a certain element of inertia, a kind of coherence with respect to the evolution of the process. Each of its transformations takes a considerable amount of time to be prepared and carried out, and involves a large amount of systems and equipment. Operation in the framework of an emergency procedure is a good illustration of the idea of configuration and orientation of the system, i.e. a phase of operation focused on following up a certain number of parameters and unravelling a sequence of specific actions. The transition from one procedure to the next describes, however, the other phase of the system's functioning: reconfiguration and reorientation.

1.14.5. Phases of stability and breaks in the progress of operation

The progress of operation through time may be described as a sequence of phases of *stability* consisting in focusing on a specific aspect of the situation, in following a certain course of action and in creating teams, as well as of phases of *break* in which the system is restructured and a new orientation is set up. Control of time factors is an essential condition for adapted operation. A CICA adopted by the system may be appropriate initially, and subsequently become inadequate once confronted with a new situation; or it may be inappropriate from the start and remain so for a certain length of time. Therefore, CICAs strive to detect the modes of operation, which lead to mission failures in the particular circumstances of an accident. CICAs do not refer, however, to modes of operation that are intrinsically doomed to failure. On the contrary, they 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 organisation—CICAs—leading to mission failure.

1.14.6. Situation properties account for the CICAs

The difficulty now is to explain the choice and, above all, the maintaining of a CICA through time. Through which mechanisms is an orientation maintained and what factors contribute towards its maintenance. In reviewing all the factors—*the system's components as well as the environment*—which may have an influence on the system's functioning and structure, properties are identified that may play a part in the manifestation and maintaining of CICAs. The main components examined are:

- procedures,
- training,
- control/command systems,
- process dynamic,
- formal organization,
- orientations given by management,
- group structure and dynamics,
- group members' profiles and backgrounds.

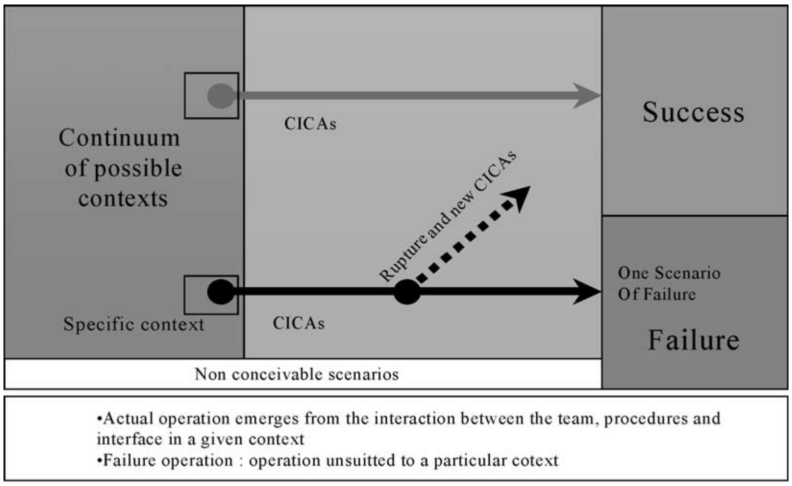
We will illustrate this method through the Three-Mile-Island accident analysis in the second part of this article.

1.15. New pattern for explaining accidents

The traditional model based on error as a human failure does not explain the relationship between erroneous operation and failure. It assumes a single context deriving from the mission to be carried out and characterized by factors influencing performance (cf Fig. 3). Failure is generated by human variability.

Our systemic model assumes that failure originates in an operation which is not faulty as such, but inappropriate considering the particular context in which it is set in motion (cf Fig. 4): it would succeed in a slightly different context under the same original conditions. This concept is very important for data collection: indeed, one will not concentrate on observing 'human failures' (or human errors). Of course these will be recorded and analyzed (generally a very simple statistical analysis is enough to provide elements for HRA analysis). They are considered as specific situation elements that may contribute to a situation liable to failure, but insufficient on their own to lead to it.

However, great effort will be devoted to understanding the behavior modes (described therefore by the CICAs) which the crew might adopt in interaction with



•Actual operation emerges from the interaction between the team, procedures and interface in a given context
•Failure operation : operation unsuitted to a particular cotext

Fig. 4. Systemic model of failure.

the procedures and the interface. It will be needed to collect the situation elements that may bear on this behavior, i.e. its emergence and possible maintaining through time while unsuited to the circumstances, and there is therefore no break in operation, reconfiguration of the crew or more generally of the operating system.

2. Retrospective analysis of the three-mile island accident

To illustrate the modeling of operation and reliability assessment we propose, let us examine the functioning of the Three-Mile Island 2 (TMI) operating system during the 29 March 1979 accident. In 1979, the nuclear energy industry was in full expansion, supported by great confidence in the efficiency and robustness of the protection barriers available to the system (Kemeny [9]; EPRI/NSAC [10]). The TMI accident revealed the weakness of these defenses and led to an in-depth redesigning of the operating system.

2.1. Operation progress

Two periods of stability and three breaks were identified while the accident was taking place. The operating system, which was involved in routine actions, reacted to the tripping of the turbine with a series of reflex actions (Break 1 at 04:00, transition from the system configuration for normal operation to incident configuration). In a second step (Stability 1 between 04:03 and about 04:16), the system concentrated on managing Safety Injection considered overabundant. After resetting the Safety Injection to standard make-up the system reconfigured itself to stabilize the unit (Break 2 at about 04:16). From 04:20 onwards, the parameters of the reactor remained stable and investigations for restarting were carried out (Stability 2). Following the worsening of vibrations on the primary pumps, and activity noticed on Steam Generator B (Break 3 at about 05:10), we observed another period of break during which the primary pumps were stopped and Steam Generator B was isolated (05:27). From then on, the operating system strayed off completely. It was confronted with a series of multiple phenomena (increase in activity, increase in containment pressure, drying out of Steam Generator A) and was unable to control them up to the uncovering of the core at 05:41.

The detailed description is given in the table in Appendix A.

2.1.1. Modeling of operation by the CICAs

Modeling through the CICAs presented in the Appendix A highlights three significant phenomena generally overlooked in existing TMI-2 analyses (Daniellou [11]; Nicolet et al. [12]; Llory [13]). It shows that the shutdown of the safety injection was part of a complex set of actions for adjusting the pressurizer level, including increasing the RCV letdown flow. The operating system therefore did more than deprive itself of an essential means for protecting its water inventory, i.e. safety injection. It carried out an operation strategy in conflict with what was required by the situation.

Modeling also highlights the fact that the operating system made wrong priority choices. In a prolonged critical phase of the accident, it deprived itself of an essential redundancy component—the supervisor—main actor in the coordination of the crew. After diagnosing a successful stabilization, the supervisor turned to the initiating incident and the recovery of the water supply. The supervisor of the neighboring unit, who had been called for support, doesn't seem to have played either an effective part in operation, or developed a specific point of view on the event, as he was busy collecting information and managing the printer.

Following the 'vibrations on primary pumps' alarms, the system was disoriented and lost its cohesion. Actually, tripping the primary pumps came in conflict with the orientation towards stabilization taken by the unit after emergency shutdown. The system no longer followed an overall logic linking together the various operating actions. It assumed contradictory hypotheses, set out on various paths, and was unable to make sense of the situation. It did not understand what was going on (the primary was saturated), and was unable to develop a suitable operating mode.

2.2. Accounting for the emergence and maintaining of the CICAS

According to CICA modeling, the operating system failed in their performance of two major safety missions: 'Maintaining Safety Injection' because it set out on 'managing overabundant Safety Injection', and then sought 'Stabilization'; and 'Isolation of the leak' because it set out on an operating strategy which, however, complex, overlooked the existence of a leak. Properties specific to the operating system and the situation it was confronted with enable us to understand why the system set out on these CICAs and maintained them through time (NUREG/CR-1270 [14]).

2.3. Emergence of the CICA 'management of safety injection'

Among the properties accounting for the emergence of the CICA 'Management of overabundant safety injection' we identified:

- the operating system taken in a broad sense, including all its participants—management, trainers, designers—did not have a representation of a 'pressurizer steam break'.
- The interface didn't provide any measurement for the primary mass.
- Procedures do not cover 'pressurizer break in steam phase'.
- The operating crew had learned to manage transients through reflex actions and always give priority to preventing the pressurizer from filling up.
- The operating crew was used to transients with the opening and closing of valves.
- The operating crew, together with the interface, set aside the problem of an incoherent drop in primary pressure.

2.4. Maintaining the CICA 'Managing safety injection'

Among the properties that can be mentioned to account for maintaining the CICA 'Management of overabundant safety injection' we find: a feature contingent to the process (a momentary drop in pressurizer level noticed after the safety injection was shutdown), equipment failure (activity in the containment went undetected), an attitude developed by the operating crews in connection with the unit's background (information on the temperature of the blowdown line is underestimated), and the limitation of the interface design, i.e. a lack of data on the evolution of parameters.

2.5. Emergence and maintaining the CICA 'Stabilization'

Regarding the second CICA, 'Stabilization', its emergence can also be accounted for by a feature contingent to the process (apparent stability of the primary), a lack of knowledge—at the level of the crew as well as that of the interface, and probably of the organization as a whole—about the behavior of the primary at saturation (pressure/temperature relationship), the apparently successful reflex management of the initial transient, and being used to transients with opening and closing of the valves. What contributed to maintaining this CICA are the apparent stability of the primary and the lack of redundancy among the crew, with the SS out of the control room for about forty minutes.

2.6. Mission failure 'isolation of the leak'

All the CICAs mentioned in the modeling are involved in accounting for the 'Isolation of the leak' failure. Emergence and maintaining refer to specific properties in addition to those already mentioned. The apparent rise in pressurizer level, the lack of a representation for 'pressurizer with steam break', the interface which does not provide for detecting the deterioration of the water inventory, the background of the valve which opens on tripping, the inability to detect activity, all play an essential role, as well as the apparent closing of the blowdown valve (for both emergence and maintaining), underestimation of the fire alarms in the containment, and a background which conceals the rise in temperature of the blowdown line.

2.7. Evaluation of operation reliability

Operating carried out during the TMI-2 accident is assessed with respect to the three following task groups.

2.8. Carrying out preservation missions

The operating system failed in maintaining safety injection as a means of ensuring the water inventory. It encountered great difficulty in carrying out the 'Ensure sufficient cooling through the steam generators' mission. Although rapid resupplying of the Steam generators was achieved within 8 min after tripping, drying out of the Steam Generators occurred later. Then, in the disorientation phase, while a leak was suspected on Steam Generator B, this generator was isolated and Steam Generator A simultaneously dried out. As to the effectiveness of cooling, the operators stabilized the temperature until 05:00. After which time, stabilization of the primary parameters was mostly due to the primary reaching saturation, which the system was not aware of. At this stage, the break released the greater part of primary energy. In short, ES was not recovered in time, and even though EFW was rapidly recovered, cooling by the SG doesn't seem to have been very effective.

The 'Limiting reactor coolant letdown' mission failed completely because the operators, who were unaware of the deterioration of the water inventory, maintained a maximum letdown flow practically until the beginning of the uncovering of the core. In order to carry out the EPS HF 'removal of residual power by the Steam Generators' mission, the system must keep the Steam Generators available. This mission came close to failure. Indeed, the operators inappropriately isolated a steam generator because they suspected it had a steam leak, only possibility accounting for the deterioration of the containment conditions, without detection of a rise in activity, which would have revealed a break on the primary. After isolating this Steam generator, manipulation errors (attributable for the most part to the design of the control room) led to the emptying of Steam Generator A. In this a situation, the operators wanted to stop the EFW flow to the isolated steam generator, but they handled the wrong control and did the reverse. The correct flows were restored within 18 min. Thus, for a short period of time, the system made the secondary totally unavailable, with Steam Generator B isolated and Steam Generator A partially dried out. In a fortuitous way, the 'Primary activity' task was successfully achieved. The operators, suspecting a leak on the joints, launched two emergency borations. However, we lack sufficient technical information to know whether there was a separate stock of water for emergency supply or whether this system used the same source as normal supply, because in the latter case the recovery operations carried out by the supervisor would have come under this mission. In short, safety injection was kept available (reused at a later stage), maintaining the Steam generators available was close to failure (two Steam generators unavailable), and the attempt to limit letdowns was a clear failure.

2.9. Carrying out preventive missions

Though reactivity was brought under control and the effectiveness of safety injection was maintained, that of the diesels was not, because they were not shut down properly. Some questions remain unanswered as to the effectiveness of the water inventory management and attempts to prevent safe shutdown under RHR conditions of the cooling system, in case of total consumption of EFW. Finally, questions also remain concerning the shutdown conditions of the primary pumps, monitoring of the operating pump, and keeping a back up pump available.

2.10. Carrying out improvement missions

The main improvement mission concerns the diagnostic, localization, and closing of the leaking valve. This mission was only fulfilled after the uncovering of the core for reasons that remain unclear to this day. While the isolation of the maximum containment by-pass was achieved, the saturation margin was never recovered.

3. Conclusion

The retrospective analysis of the TMI-2 accident shows that the operators' mode of operation resulted from an overall logic, reflecting emergency operation logic upon which the design of the operating system was based. It helps to get out of the deadlock reducing the TMI-2 accident either to a commissioning error of the type 'Inappropriate shutdown of the safety injection' or to an error of diagnostic and misrepresentation of the situation, since we know (and the first analysis of the event already showed this clearly) that the operating system was faulty at nearly all levels: from training to procedures and from interfaces to organization. This was already an underlying paradox in the Kemeny report ([9]) where we read at the same time that: 'While material faults initiated the event, the main cause of the accident was an 'operator error'. If the operators (or those who had a supervising role) had kept safety injection in operation during the first stage of the accident, TMI would have only led to an incident of little significance…. 'We also read: 'While the main factor which turned this incident into a serious accident was an inappropriate operator action, multiple factors contributed to the operators' action, such as inadequate training, the lack of clarity of their procedures, failure of the organizations to derive knowledge from previous incidents, and insufficient design of the control room'.

By replacing operators' actions within the operating system and considering them as the products of the interaction between the operators and the technical devices (interfaces, procedures), and organizational roles (management of transients, training), the inadequacy of the operating system, as a support environment to the proper management of operation, becomes obvious. The operating system was not designed to manage a situation involving a significant loss of water inventory, as occurred at TMI-2. The operating system did not foresee the means that were actually necessary to fulfill the mission required by the situation.

Appendix A

Table A1

Table A1

Time	Operation			Overlooked operating options and comments
	RECONFIGURATION (‘normal operation → emergency operation’)			
	Reflex action: application of emergency procedures (EP) with failure to restart pump A (make-up pump)			‘It must be noted that at the beginning of the accident the operator thought he was confronted with a known situation, since he performed several manual operations provided for in the instructions as early as second 12 of the accident, and it doesn’t seem that he gave in to panic at any time.’ (Cogné [15] 1979)
	Reflex action: verification of the starting of the SGs auxiliary feedwater supply			
	CICA 1, management of safety injection (ES) considered overabundant	CICA 2, recovery of the SGs auxiliary feedwater supply (EFW)	CICA 3, Stopping of actions related to emergency shutdown	
	RECONFIGURATION (‘stabilization → preparation for restarting’)			
04:16	Transition of auxiliary controls to auto (EFW)			
04:20	SS ‘leaves the control room’			
	CICA 4, stabilization	CICA 5, recovery of the water supply	CICA 6, postponement of actions related to emergency shutdown	
	UNFOCUSED OPERATING SYSTEM’S ACTIONS			
05:14	CICA 7, progressive transition to thermo-siphon Shutdown of the primary pumps (RCP) loop B following the vibration alarms.			‘After some time the reactor coolant pumps began to vibrate and procedure demanded that they be shut down. I felt uneasy, there was a tiny voice telling me not to do it. I and some of the other operators argued against it. The procedure won over our protestations’, (Frederick [16],) Overlooked operation: possibility of re-starting
05:17		CICA 8, cooling on only one SG Isolation of SG B assumed to be leaking (steam leak in containment)		Following the diagnosis of a steam leak in the containment
05:21			Start of CICA 9, investigation on the closing of the pressurizer relief valve Verification with a calculator of the pressurizer blowdown line parameters (temperatures)	Overlooked operation: pressurizer relief valve remained open
05:34		Continuation of CICA 8, recovery of the SG A level		No SG available
05:40			Start of CICA 10, boration emergency boration Assumption of a leak on the joints	Fear of renewed criticality through dilution owing to an assumed leak on the joints
05:41	Detection of the loss of natural circulation in the core Continuation of CICA 7 shutdown of the primary pumps (RCP) loop A			
05:42			Continuation of CICA 10, second emergency boration	
05:52		Continuation of CICA 8, attempt at cooling by SG A		To recover natural circulation and residual heat removal

References

[1] Le Bot P, Desmares E, Bieder C, Cara F, Bonnet J-L. MERMOS: un projet d'EDF pour la mise à jour de la méthodologie EPFH. Revue Générale Nucléaire 1998;1.

[2] Swain AD, Guttman HE. Handbook of human reliability analysis with emphasis on nuclear power plant applications—Final Report. Nureg CR-1278, US Nuclear Regulatory Commission; 1983

[3] Hannaman BW, et al. Human cognitive reliability model for PRA analysis. NUS-4531, EPRI; 1984

[4] Boutin P, Nunez R. Le retour d'expérience dans le domaine des facteurs humains et organisationnels. Difficultés et risques de biais, Revue Contrôle, Dossier: L'homme, les organisations et la sûreté 2001;39–41.

[5] Lorigny J. Les systèmes autonomes. Paris: Dunod; 1992.

[6] Cara F, Le Bot P, Bieder C, Desmares E, Lagrange V. Nouvelles perspectives sur la fiabilité de la conduite des centrales nucléaires. 34ème congrès de la Société d'Ergonomie de Langue Française: Caen; 1999.

[7] Hutchins E. Cognition in the wild. Cambridge: MIT Press; 1995.

[8] Hutchins E. Comment le cockpit se souvient de ses vitesses. Sociologie du travail, vol. 4. Paris: Dunod; 1994.

[9] Kemeny et al. The need for change: the legacy of TMI. Report of the President's; 1994

[10] EPRI/NSAC. Analysis of Three Mile Island Unit 2 accident. Report NSAC-80-1/NSAC-1. Palo Alto (CA): Electric Power Research Institute/Nuclear Safety Analysis Center; 1980

[11] Daniellou F. 1986. L'opérateur, la vanne, l'écran. Montrouge: Editions de l'ANACT; 1986

[12] Nicolet JL, Carnino A, Wanner J-C. Catastrophes ?Non merci!. Paris: Masson; 1990.

[13] Llory M. L'accident de la centrale de Three-Mile Island. Paris: L'Harmattan; 1999.

[14] NUREG/CR-1270, Human Factors Evaluation of Control Room Design and Operator Performance at Three Mile Island-2, vol. I, II, III. Washington, DC: NRC; 1980.

[15] Cogné F. L'accident d'Harrisburg. Notes d'Information du CEA n°9

[16] Frederick ER. Design, training, operation: the critical links. An operator's perspective. International Symposium on Severe Accidents in Nuclear Power Plants, Sorrento 21–25 March; 1988.