157

INTERNATIONAL SEMINAR ON PSAs AND HUMAN RELIABILITY

Paris, November 21st-23rd 1994

Topic 4 : INCIDENTS ANALYSIS

P. FRANCOIS

CONTENTS

1. INTRODUCTION 4

1.1 CONTEXT 4

1.2 BACKGROUND 5

2. OBJECTIVES AND PROBLEMS RAISED BY PROBABILISTIC ANALYSIS 5

2.1 ASSESSMENT OF LEVEL OF SAFETY 6
2.1.1 Description 6
2.1.2 Problems posed 7

2.2 FEEDBACK ON ACCIDENTS 10
2.2.1 Description 10
2.2.2 Problems posed 11

2.3 SAFETY CULTURE 12
2.3.1 Description 12
2.3.2 Problems posed 13

2.4 EVOLUTION OF PSA 13
2.4.1 Description 13
2.4.2 Problems posed 13

3. EXAMPLES OF STUDIES, LESSONS, AND POSSIBLE CHANNEL FOR RESEARCH 14

3.1 INTRODUCTION 14

3.2 EXAMPLES OF STUDIES 14

3.3 A SPECIAL LESSON FROM INCIDENT ANALYSIS 15
3.3.1 An Indirect Lesson from Causal Analysis 15
3.3.2 Interpretation of Some Accident Scenarios 15
3.3.3 Lessons 16
3.3.4 Conclusion: A Qualitative Approach to Small Cutsets 17

4. OUTSTANDING QUESTIONS 18

4.1 HOW IS AN ANALYSIS PERFORMED ? 18
4.1.1 Introduction 18
4.1.2 Where Should Analysis Start ? 18
4.1.3 What Should be Varied 19
4.1.4 Generic, specific, average, or instantaneous data ? 20
4.1.5 Analysis Criterion 21

4.2 VALIDITY AND MERIT OF THESE ANALYSES 21
4.2.1 Validity and Merit of a Safety Indicator 21
4.2.2 Using these Analyses for Design and Operation 22
4.2.3 Safety Culture 22
4.2.4 Validation of PSA 22

5. CONCLUSIONS 23

APPENDIX 1 EXAMPLES OF STUDIES 25

GLOSSARY 29

1. INTRODUCTION

1.1 Context

When an incident occurs at a power plant, operators and safety experts are forced to ask the following questions:

- how could the incident have degenerated into an accident with much more serious consequences ?
- can one develop a means of measuring the difference in seriousness between the end of an incident and a potential accident with unacceptable consequences ? What would the meaning of this measurement be ? How can it be validated ?

Probabilistic incident analysis sets out to find a real answer to these questions. The method consists of applying event trees representing accident scenarios to a real incident: the real incident is considered to be an initiating event (this is the case of operating transients) and existing trees are modified to take account of the incident's effect on the impairment of safety functions (case of equipment unavailability).

The study is pursued to assess the conditional probability of core melt, thus identifying the seriousness of the incident and its main sequences, i.e. the most probable impairment modes which lead up to core melt.

This method of analysis complements the methods of analyzing the causes of incidents that are generally employed by EDF (and by many other companies). In fact, the methods generally used (fault tree analysis, preliminary risk analysis) are not designed to answer this sort of question, even if they can give qualitative information, however incomplete and imprecise in general terms.

Preliminary risk analysis methods also have the disadvantage of being essentially based on operating feedback: it is therefore necessary for the incident to have occurred at least once for risk analysis to be possible. They are therefore generally restricted to minor incidents. This is precisely the interest of using models that are based not only on feedback but also on knowledge of all aspects of the plant's accident-situation operating modes (physical, technological, organizational aspects, etc.).

1.2 Background

We undertook a study programme at the end of 1991. To start with, we performed some exploratory studies aimed at learning some preliminary lessons on this type of analysis:

- assessment of the interest of probabilistic incident analysis,
- possibility of using PSA scenarios,
- skills and resources required.

At the same time, EPN[1] created a working group whose assignment was to define a new approach for analysis of incidents on NPPs. This working group gave thought to both aspects of Operating Feedback that EPN wished to improve (Fig. 1):

- analysis of significant incidents
- analysis of potential consequences.

We took part in the work of this group, and for the second aspect, we proposed a method based on an adaptation of the event-tree method in order to establish a link between existing PSA models and actual incidents. Since PSA provides an exhaustive database of accident scenarios applicable to the two most common types of units in France, they are obviously of interest for this sort of analysis.

With this method we performed some incident analyses, and at the same time explored some methods employed abroad, particularly ASP (Accident Sequence Precursor, a method used by the NRC).

Early in 1994 EDF began a systematic analysis programme. The first, transient phase will set up methods and an organizational structure.

2. OBJECTIVES AND PROBLEMS RAISED BY PROBABILISTIC ANALYSIS

Identifiable objectives can be put in four main categories:

- Building a risk indicator, which we will call "quantitative risk analysis" or "incident gravity assessment". This indicator of the risk arising from incidents is used for **assessment of the level of safety of units**, or of all French nuclear power plants in general.

- Looking for qualitative lessons to be drawn from actual incidents taken as precursors of potentially more serious "unoccurred" accidents. This is what we call "qualitative incident analysis" or "**accident feedback**".

---

1 *EDF's Nuclear Power Plant Operations Division*

- Promoting a new method for unit operation analysis by operators, which involves criteria drawn from probabilistic methods for decision support or risk assessment. This objective is part of the movement towards a "**probabilistic safety culture**".

- Lastly, the fourth category is more especially intended for reliability specialists, unit incidents being a means of comparing PSA with reality. Precursor analysis is a means of **enhancing PSA**.

The four types of objective discussed in this document are presented from the point of view of direct utility to the operator; no judgement is intended on the interest of developing other types of objective.

2.1 Assessment of Level of Safety

2.1.1 Description

This objective is the one that most closely resembles what is done in the United States (Accident Sequence Precursor (ASP) programme). The principle involves assessing the seriousness of the incident on the basis of its conditional probability of core melt. The sum of the conditional probabilities for all the sequences initiated by the incident gives a measurement of the seriousness of the incident. In other words, the incident is represented by a figure which totalizes all the scenarios identified as being the most probable which might lead to reactor core meltdown.

In the ASP programme, incidents are sorted, and only those deemed to be the most serious are actually analyzed.

The ASP method consists in sorting the most striking incidents of all American power plants (selection of about 100 incidents from the 8,000 declared every year). These incidents are then analyzed using five simplified trees to determine about thirty precursors which are ranked in accordance with their conditional probability of core melt. The values associated with the incidents are then added together to determine indicators for individual plants, for each type of plant, or for all American NPPs.

On the basis of this brief description, one can debate the validity of this sort of safety indicator. Are the 30 precursors representative of the overall risk of all the power plants ? Should all 8,000 declared events be analyzed ? Can one apply to a given unit what would be valid for all reactors as a whole ? Isn't there a minimum number of incidents that should be analyzed if the indicator is really to be valid ? How valid is an indicator that is based exclusively on incidents, without taking account of equipment unavailability for example ?

An incident can be assessed in several ways:

- process the events studied in the context of the plant where they occurred, taking account of all known parameters giving the fullest possible description of this context,

- step back from the context by transposing events to another plant or to another unit status (how serious would the incident have been if it had occurred on another plant or when the plant status was different ?),

- choose standard, average models and data to describe the installation, which amounts to considering that the event occurred on an "average" unit like that taken into account in PSA.

A study of the seriousness of an incident can therefore give several different results, all of which in principle have their utility. These different types of studies can correspond to different objectives: assessment of the generic risk, of the specific risk for a given unit, and even of a particular risk (concerning specific staff of a plant). Similarly, users can be different (experts at the national level, site managers, unit operating staff).

In other words, it can be said that the risk "point of view" of a national expert (covering all nuclear power plants) and that of an operations crew faced with a particular incident may not be the same.

Several levels of analysis of increasing complexity can also be envisaged: a simplified ASP-type analysis could give a conservative result which could then be made less conservative by a more thorough analysis.

From assessment of the conditional probability of core melt can be deduced an assessment of the safety of a plant, by adding together the values for several incidents. In this way one could assess the probability of core melt for one year of operation of a given plant (particular indicator for a unit), for a given unit, type of unit, or for all the nuclear power plants in a system.

This assessment enables intercomparison of incidents or of types of analysis: it would give a tool for quantitative assessment of safety, which would be a means of dialoguing with other NPP operators and with Safety Authorities since the authorities are developing similar tools.

This assessment tool could be associated with a scale of seriousness. For example: level of the incident = $(6 + \log_{10}(\text{total probability of Unacceptable Consequence}))$. Level 6 of this scale (the highest level for a level-1 PSA, corresponding to effective meltdown of the core) is equivalent to level 4 on the DSIN* scale or levels 4 or 5 on the INES* scale.

2.1.2 Problems posed

The description in the above paragraph includes a number of questions. They are taken up again here, detailed, and complemented.

It has been seen (this is the first problem) that **the assessment could result in several values, depending on the assumptions chosen.**

It thus depends very much on the reliabilistic assumptions chosen: should one choose data specific to the incident (difficult to get hold of) or more generic data from PSA (known) ?

---

* *Asterisks indicate terms defined in the glossary at the end of this communication.*

These assumptions depend on what one is trying to find out: the potential consequences of the incident on the plant where it occurred, in the status of the unit in which it occurred, and - in as far as possible - given the exact status of equipment at the time it occurred. This amounts to deliberately setting the probability of all the events actually observed to 1 and keeping values from operating feedback for events that did not occur.

Here we are obliged to specify what is to be changed in a standard PSA tree:

- to reflect the incident as well as possible, unfavourable incidents are "forced" to 1. This is the method recommended by the NRC.
- one can also modify the standard tree and introduce everything that is typical of the incident situation, without asking if the elements one is adding are favourable or unfavourable.

In a first approximation, the difference between these two approaches introduces a variation in the margin of conservatism.

A second problem comes from the level of detail of what one decides to model. Some analysis experiments have shown that the end result could be very sensitive to the level of detail.

An outstanding example of the variability of the result is the case of the incident on a 900 MW PWR unit on (27-hour loss of the LHB switchboard due to a short-circuit). The conditional probabilities of occurrence of sequences H3* and H1* can vary by several orders of magnitude, depending on the method for calculation of the common mode between emergency switchboards LHA* and LHB. The most robust assessment is based on the analysis of the failure of the internal component of the electrical cell which caused the short-circuit, on the basis of models with a non-constant failure rate (see § 3.2. below).*

Another problem posed by this type of risk indicator is that it is founded on the implicit assumption that the risk is entirely within operating incidents detected and declared by power plants. In the strictest terms, this sort of assumption can only be false, but it can be supposed that declared incidents are "representative" of the most significant fraction of risk; failing anything better, the only observable fraction at the current time, together with that due to the unavailability of important safety-related equipment.

If one supposes that incidents are representative of the overall risk, one must again ask **in which incidents the most significant part of the risk due to the incidents is to be found.** In other words, is the risk in a large number of harmless incidents, or is it concentrated in a small number of serious incidents ?

Therefore, one cannot know whether the risk is represented by all the incidents, by the declared incidents, or by the most striking incidents.

It can thus be said in conclusion to this aspect that the risk of making a mistake is high (results can vary over several orders of magnitude) but that the consequences of these mistakes are restricted to uncertainty over the indicator and its utilization. The magnitude of error can be limited by defining precise standards for the analysis method. It remains that the essential problem is that of the indicator's **meaning**, particularly in its wide variations from one year to the next.

2.2 Feedback on Accidents

2.2.1 Description

If assessment of the seriousness of an incident consists in representing it by a number that one can rank on a scale of seriousness, it causes us to lose a great deal of the information the value represents. A probabilistic description of the incident can give us information on the **causes** of its seriousness and on the **manner** in which it could have degenerated.

Thus, since the event tree for the incident is a quantitative and **qualitative** representation of the incident, it can tell us about the sequences that represent the risk:

- is the risk distributed across several sequences, or is it essentially concentrated on one of them ?
- what are the generic events with the most weight, what are the associated lines of defence (in particular, are they automated procedures or manual actions) ?
- are there common sequences (or common generic events) for incidents deemed to be very different ? Can one derive useful statistical information from it ? Can one deduce as-yet-unidentified cause-and-effect relationships or common modes from it ?

From preponderant sequences for degradation of an incident into an accident one can identify the weak spots (and strong points) in a plant and the manner in which it is operated, and assess the "lines of defence" set up during design and operation. One can therefore draw lessons concerning the way the incident is handled (particularly with respect to operating procedures), organization of maintenance, and even on the design or modifications of the plant.

In § 2.1. it was seen that the different ways of calculating an indicator (choice of initial conditions that are average or unit-specific, transfer of the event studied to another plant) could lead to several different risk indicator values giving information on the types of preponderant sequences, depending on the assumptions used. There is therefore continuity between these two objectives, i.e. the indicator and operating feedback.

One can thus envisage the possibility of a "semi-deferred-time" decision-support system for operators (comparable to the ESSM in the long term). This would involve providing the ISR[2] (for example) with a means of identifying the main possible degradation sequences and sensitive equipment to be monitored especially closely, which would help engender a "probabilistic safety culture" (cf. § 2.3.).

More generally, if it is assumed that PSAs are models simulating reality, then probabilistic analysis is a means of knowing the potential sequences of an incident without them actually occurring. This method of analysis allows a form of "feedback" based on events that have not actually occurred; it enables us to learn from what has not happened in the same way as we usually learn from what happens every day. Event-tree sequences are investigation tools that can consequently provide information that is more than just a simple measurement of the seriousness of incidents, since they give us insight into the possible modes of degradation of incidents, while sparing us their potential consequences.

This objective is therefore more ambitious than just quantitative analysis of the seriousness of an incident, even if it is restricted to analysis of a few incidents considered to be "significant". In particular, it is a tool for dialoguing with the Safety Authorities (ranking on the INES scale, steps to be taken in terms of operating feedback, etc.)

2.2.2 Problems posed

Here we find the same objections as those encountered in § 2.1.2. Is PSA a good simulation of reality ? To what extent can the most probable PSA sequences be assimilated to potentially realizable events ? These problems do indeed exist, but are of lesser importance:

- More thorough analysis on a limited number of incidents means the PSA event trees can be adapted to make a more realistic assessment of the differences due to the underlying assumptions. An example is the Bugey incident of 14.4.84 (slow degradation of the LCA*) which led to the construction of a totally case-specific tree involving a sequence of total loss of electrical sources and three thermohydraulic sequences (LOCA, RTGV*, and loss of GV* supply).

- Since the incident is treated by specific means, the problem of its representativity relative to the global risk of the plant is not an essential problem. Moreover, the qualitative lessons it gives are generally valid, the problem being that not all the lessons are drawn and that quantification or ranking can be suspect, which is chiefly disturbing for quantitative analysis.

---

2 *Ingénieur Sûreté Radioprotection - Shift Technical Advisor (STA): the person who steps in in the event of accident-situation operation.*

2.3 Safety Culture

2.3.1 Description

One of the parts of the risk due to the human factor is represented by the fact that we often have poor perception of risk (refer to this to all the literature on the subject, even if debate is raging ...). This idea can be found in the INSAG 4 report: "... to develop an interrogative attitude, what can go wrong ? How can safety be compromised by errors I might make ? ...".

At the moment, operators are trying to develop this interrogative and preventive attitude by developing a safety analysis method, as described in a guide for nuclear power plants which presents a qualitative method for analysis of the potential consequences of events. This method is based on the event-tree method.

Quantification of event trees with PSA tools and models would enable operators to have and use tools for assessment of risk and identification of the potential consequences of incidents; this would serve as a support for this interrogative attitude.

Even more, INSAG 4 refers to probabilistic studies: "... The results of safety analyses, particularly probabilistic analyses, are consulted regularly to back up the decisions to be taken when special problems arise, and to give the person concerned an idea of the main design and operation characteristics of the power plant in terms of safety ...".

The general idea at the base of the need to develop this type of interrogative attitude can be formulated as follows: the behaviour of operators has important effects on the level of safety of a plant, and is highly affected by the perception operators have of risk, this perception of risk itself being linked to an interrogative attitude towards the potential dangers involved in operating situations. The purpose of probabilistic methods is to reduce the subjective character of the frequency of expected or undesirable events. They are therefore capable of modifying the perception of risk by operators and consequently having an effect on the safety of the plant.

Risk loses its character of inevitability; it can be measured and one can thus reduce the usual phenomena of distortion (one tends to exaggerate the probability of an expected event, to cancel that of an undesirable event, to reduce the probability of an undesirable event if one is directly involved, to accept the risk more easily if it is not due to the behaviour of others or if the expected benefit is great, etc.). One could refer here to a study by D.R. Kouhabenan (1985): "one allocates the causes of an incident in different fashions, depending on one's degree of involvement in the incident".

This sort of supposedly objective modelization can be particularly useful for assessing the risk due to high-frequency harmless incidents. Experience tends to show that serious accidents are often caused by multitudes of harmless incidents, and it is for this reason that fault trees often leave causal incident analysis short of a satisfying conclusion (this can be assimilated to V. Bernhardt, 1984: "most accidents are the result of a combination of factors which can appear harmless in terms of safety if considered separately" (see also § 3.2.). It is with probabilistic methods that the precursor nature of events deemed to be minor could be brought to light, since it is often accepted that the most serious accidents have been described in literature before they actually occur.

2.3.2 Problems posed

Like all changes of this kind, this evolution of "safety culture" cannot take place without some difficulty. It should involve all operational levels in power stations, which requires substantial resources and time before measurable results will be observed.

It is stated above that these analyses require multidisciplinary expertise (PSA, reliability, operation, accident-scenario operation, etc.), which consequently requires a substantial investment by those interested in pursuing the matter. It is therefore probable that probabilistic analyses will remain the business of some specialists with central or on-site services, and the dissemination of this safety culture is likely to be very limited. Nevertheless, we have seen that analyses carried out by specialists were generally legible by the operators of nuclear power station sites.

Moreover, it is not certain that the effects are always positive: one might ask just how much the increased knowledge of risk generates a stress situation incompatible with operating activities. One never insists sufficiently on the difficulty (and danger) of constantly reminding staff of the risks run. Fear could emerge and be a major hindrance to common sense, reflex, experience, etc. In addition, one does not know how "formal" safety based on expertise and "non-formal" safety based on the practical experience of operators can interfere with each other.

Finally, this is where the consequences of an error can be the most important, and it has been seen that it is very easy to make a mistake in this field since there is practically no means of verification. Reliabilistic reasoning has to be integrated into the usual deterministic approach and this reasoning must be properly controlled, even if its scope must be restricted to do so. In addition, the safety criterion must be situated amongst other operating criteria (cf. Topic 2 on PSA applications).

2.4 Evolution of PSA

2.4.1 Description

Probabilistic analysis of incidents compares PSA with reality. It validates or invalidates the PSA assumptions, models, and data by integrating the feedback from unit operation. This is one of the major lessons of exploratory studies performed until now. Probabilistic incident analysis is thus a preferential means of making PSA evolve, which is a prerequisite for achieving what is called "living PSA".

2.4.2 Problems posed

In general terms, as we have seen above, real incidents reveal differences from modelized events. Our experience shows that it is often difficult to interpret these differences, even for the designers of the models. This requires the participation of those in charge of designing PSAs and making "living PSAs". This objective is therefore difficult to obtain, but it is not conceivable to not use the information in these analyses in order to enhance PSA models.

3. EXAMPLES OF STUDIES, LESSONS, AND POSSIBLE CHANNEL FOR RESEARCH

3.1 Introduction

The purpose of this chapter is to propose a channel for research into PSA based on some lessons from Incident Analysis. It is based on the interpretations that can be made of classical experience (analysis of incident causes), and on the interpretation of accident scenarios. These scenarios have been revealed by PSA models in the probabilistic analysis of the consequences of real incidents; some of them are briefly described in the next paragraph.

3.2 Examples of Studies

Details of four examples of incident analysis are given in the appendix. The examples are considered to be representative of the diversity of the types of analysis that can be made and of the lessons that can be drawn from them.

The first case (incident due to frost) demonstrates the interest of linking several incidents whose origin seems to be a single cause when making a probabilistic analysis. Here, the cold weather caused several failures in very different parts of the installation: in particular, a voltage drop on the network and the freezing up of the level sensor in the PTR* tank. Independently these two failures can be considered to be minor. But together they made the incident serious: there was an initiating event (LOCA) and unavailability of the associated engineered safety feature (Safety Injection).

The significance of the incident can only be appreciated if one has a global representation of the installation (a PSA type representation). The first difficulty consists in building the event tree (i.e. identifying the important sequence(s)). The second difficulty is that of quantifying them: here this involves assessing the probability of there being a LOCA and unavailability of IS* simultaneously, i.e. calculating a common mode between these equipment items which, on the face of it, are linked in no way.

Another type of common mode is illustrated by Case 2. This concerns a fire which made an emergency 6.6 kV switchboard (LHB*) unavailable. The most probable mode of aggravation is easy to identify (it is H3*, black out); in addition, this situation is similar to standard situations described in PSAs. The only difficulty lies in the calculation of the probability of initiating event H3. Several types of calculation have been proposed. The one that seems to be most robust relies on a model with a non-constant lambda value applied to a component part of the 6.6 kV contactors. The importance of the incident depends on the probability of loss of the LHA switchboard when the LHB switchboard is unavailable (this probability is the probabability of initiating event H3 and the value of the common mode between the two switchboards). The final risk is about 1E-2, and if automatic calculation had been done with a PSA model, a value of about 1E-6 would have been found. This is because standard PSA models do not take account of common modes between switchboards and use constant failure rates. This example demonstrates the interest there might be in undertaking a close study of the causes of failures. Here, automatic application of a standard PSA gives a result that is completely irrelevant.

The third case illustrates what a preliminary risk analysis using PSA models could contribute. It concerns the programmed unavailability of an SEC* train. The train was locked out for rehabilitation works. Before the works, specialists made a risk analysis and concluded that the undesirable event was loss of the redundant train (H1* type risk). A study made with the global EPS 1300 PSA model detected a sequence 70 times more significant that no-one had thought of.

This study shows the interest of analyzing the potential consequences of incidents using quantified event trees. It makes it possible to envisage scenarios that take account of the entire installation, including the human factor. This is very difficult to do, even for safety specialists.

Finally, the fourth case illustrates a problem of incident analysis which is detailed in Chapter 4. During uncontrolled cooling of the reactor the operator locked out an engineered safety feature. Probabilistic analysis of the transient shows that the risk is moderate, that the incident is not very important (contrary to the other three cases, probabilistic analysis has a moderating effect). But was the total risk measured ? What would the consequences of this unwarranted action have been under other circumstances where the risks were higher ? The study is complex, but it is considered important to not restrict things to the initiating event that actually took place during the incident, for the effect of this action should also be assessed for all cases where the engineered safety feature function would have been necessary. This question is re-examined in §4.1.3.: initiating events other than the one that actually took place should be envisaged.

In conclusion to these examples, it can be seen that automation of incident analysis cannot be envisaged. Incident analysis requires information and logical data, but also the knowhow, intuition, imagination, and experience of specialists.

3.3 A Special Lesson from Incident Analysis

3.3.1 An Indirect Lesson from Causal Analysis

A henceforth classic significant lesson of analysis of the causes of incidents can be expressed as follows: serious incidents are often the result of the aggregation of several harmless failures (see "Safety Culture" § 2.3.). This aggregation can involve a large number of failures. The important thing here is that they are small, routine, and apparently independent failures. If a method such as the "fault tree" is used, at the "roots of the tree" one finds a string of small failures which, taken separately, are deemed to be innocuous and are generally considered acceptable by the operator. For this reason fault trees, even if acceptably constructed and rigorously logical, often fail to live up to expectations. Probabilistic analysis does not solve this problem: if the failures are independent, the aggregation is given a very low probability. It may nevertheless be of help in finding dependencies between the failures.

3.3.2 Interpretation of Some Accident Scenarios

The examples given above are re-examined here, together with the Three Mile Island accident.

TMI

The causes of the TMI accident can be summed up simply by the aggregation of:
- a concealed unavailability of the ASG* (isolating valves closed),
- a concealed failure (pressurizer relief valve jammed open),
- unwarranted action by the operator (who had trouble understanding what was going on).

Two simple, independent failures were enough to make the situation sufficiently complex to explain human error (given the procedures and organization at the time).

The probability of this sequence occurring is very low in the EPS 1300 PSA.

Train B RRI* + LBA*

This example of incident aggregation is taken from a calculation made for Operating Technical Specification application. It corresponds to the incident described above (Case 3 in the appendix).

This scenario, which is due to the aggregation of two apparently independent failures, is also difficult to imagine without using computerized PSA. "Experts" generally think that it is the loss of the redundant train (Train A RRI*) which represents the highest risk (H1* initiator).

As for TMI, this type of scenario is initiated by two supposedly independent equipment failures.

Scenarios based on two types of common-mode failures

In the chapters above we have seen two examples of incidents distinguishing two different concepts of common-mode failures: the climatic Big Common Mode (Case 1) and the classic Small Common Mode (switchboard fire, Case 2). In both cases a single cause resulted in several failures which had previously been considered to be independent.

3.3.3 Lessons

All these incidents show that one can finish up with unacceptable consequences from a very limited number of failures (never more than two) or of causes of failure (just one in the case of the climatic common mode).

These failures concern identical equipment with a high common-mode factor (Case 2) or different and independent equipment (TMI and Case 3).

In all cases, a "classic" PSA approach (i.e. based on a sensitivity study using existing models) does not furnish a realistic assessment of the seriousness of the incident.

3.3.4 Conclusion: A Qualitative Approach to Small Cutsets

The common factor in these incidents is that they are initiated by **small cutsets** (2nd order) whose probability in the models is very low, either because the failures are supposed to be independent, or because the common-mode failure is deemed to be of negligible probability. The order of the cutsets is linked to the level of detail of the failures considered: it corresponds here to the level of detail of generic events or initiators described in PSA event trees.

One could try to survey all the incidents of this type, i.e. to start with all the second-order cutsets whose conditional probability of unacceptable consequences is high (> 1 E-2) **without taking account of their probability of occurrence**.

One could also build a large matrix involving all the main second-order aggregations.

For the highest results, one could then imagine the scenarios at the origin of the aggregations, which would make it possible to find the appropriate beta factor.

The interest of this method lies in using sequences described in PSAs "backwards" in order to find accident scenarios: a second-order cutset is identified, and a scenario that might lead up to it is then built.

One application of this could be to build more realistic rules of aggregation of unavailability (Table III 6.9 of the French General Operating Rules) than those currently used.

Higher-order cutsets could then be investigated.

4. OUTSTANDING QUESTIONS

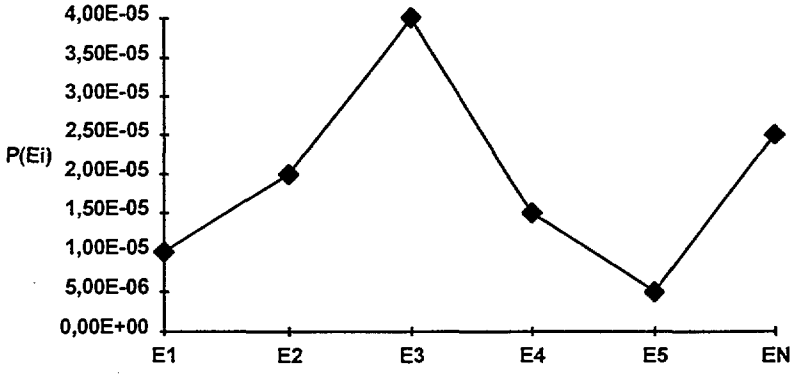
4.1 How is an Analysis Performed ?

4.1.1 Introduction

To guarantee their validity, incident analyses should have the following characteristics: they should be as exhaustive as possible (do not forget any significant fraction of risk), conservative (without being too conservative, in order to remain credible), and reproducible (sufficiently formalized). Our thinking on formalization of these analyses was the main reason for us asking the following questions.

4.1.2 Where Should Analysis Start ?

A complex incident is often a succession of events $\{E_i\}i = 1,n$, some of which aggravate the situation, others improving it. Under these circumstances, $P(E_i)$ is the probability of reaching unacceptable circumstances after occurrence of event E_i. The incident can be represented as shown below:



The risk may not be a function, first increasing, then decreasing in accordance with recovery of equipment or of human errors. This function may have several local extremes.

The question here is to know where to make the break between the determined past and possible futures (cf. Fig. 6). How, at which moment in the incident, and in which unit status should one set the starting point for potential aggravation sequences ?

The break separates the determined past from possible futures. What actually happened after the break has no particular status: all possible evolutions exist side by side. The break is generally made at the place where the risk is supposed to be greatest (most impaired status). Evolution of the situation is then modelized by a series of event trees (Fig. 7). The total risk could thus be represented by a logic sum of all the breaks, of all the variations, and all the elementary risk sequences associated with each sequence calculated.

The starting point of the analysis can therefore be varied (does one analyze the consequences of the first incident to occur, or of that incident plus the events that occurred subsequently ?). These questions can be asked in the case of complex or long-lasting incidents (which are generally the most serious). What method should be adopted ? Should an iterative approach be used ?

4.1.3 What Should be Varied

PSA-model-based incident analysis usually involves modifying the probability of the model's base events or top events which occurred during the incident.

It is usually postulated that:

- P (Ei) = 1 if event Ei occurred during the incident and,
- P (Ei) = nominal value of the model otherwise.

The model's input parameters are thus modified so that:

λ hourly rate of occurrence of an event

γ probability of occurrence of an event

ψ probability of occurrence of human error

I frequency of the initiating event

and sometimes:

β rate of common-mode failure

μ hourly rate of equipment repair

On the other hand, the following are not varied often enough:

p type of unit

η initial reactor status

χ chronology of events that occurred during the incident.

A harmless incident for a unit in a given status may become much more serious if it occurs on another type of plant, in another reactor status, or if the chronology of events is changed.

But how do you estimate the probability of the incident occurring on another type of plant, in another reactor status, or of the chronology of events being changed ? Similarly, how do you take account of the actual behaviour of operators, such as for example the fact that they recover the situation in a time t ?

What should be changed in a precursor type analysis ? All parameters can affect the risk. Shouldn't the risk associated with an accident precursor be written as follows:

$$R = \sum_{i \in \{units\}} \sum_{j \in \{status\}} P_i P_{ij} P(c_{ij})$$

where:

Pi : probability of an incident occurring on unit i,

Pij : probability of an incident occurring in status j of reactor i, knowing that it occurred on reactor i,

P (Cij): probability of core melt, knowing that the incident occurred on reactor i in status j.

The analysis can become complex, for an event is rarely specific to a given unit. It is therefore always necessary to vary parameter p and to duplicate the analysis as many times as there are design types !

There are fewer limits to the domains of parameter variation in the case of analysis aimed at determining information about design or operation. But one might ask if the sole criterion of core meltdown is sufficient to get information efficiently.

4.1.4 Generic, specific, average, or instantaneous data ?

In estimating the risk run by a unit during an incident, one might be tempted to calculate a conditional probability of core melt with representative data on the actual status of the unit at the time of the incident, i.e. using instantaneous specific data (for equipment as well as for operators)[3].

But doesn't that go against the grain of the precursor programme which aims at estimating the safety level of reactors, not the conditional probability of core melt for thirty odd non-reproducible events (an incident can never re-occur in the exact unit status in which it first occurred).

---

3 *"Instantaneous" reliability data is representative data on the actual state of the component (degree of wear, time since the last test, etc.) or of the operating crew (state of fatigue or stress of the various crew members, etc.). Unfortunately it is extremely difficult to estimate data of this kind.*

Furthermore, average generic data is non-representative. The risk calculated with average generic data is not the same as the average of risks calculated on all units with specific instantaneous values. One encounters a more complex version of the problem experienced in unit shut-down PSAs where the possible configurations of units are very numerous (risk cannot be assessed with average unavailabilities and configurations).

4.1.5 Analysis Criterion

Incident analysis is based on a single criterion : core meltdown. This criterion poses a great many problems (cf. § 4.2.3.).

It is not a real safety criterion like the risk of release of radioactive matter or the number of deaths resulting from an accident. These analyses rank the TMI and Chernobyl accidents in the same way, whereas the INES scale makes a distinction between them.

Nor is it a valid economic criterion. Incidents can cause very costly damage without putting the integrity of the fuel in the balance.

Moreover, this criterion is very "distant" from the concerns of operators who tend to reason more in terms of availability, surpassing of operating technical specifications, loss of barriers (protection, in the broadest sense, against initiation of a serious accident, or to limit its consequences), doses to which people are subjected, etc.

Should accident precursor analyses be performed with several criteria : safety, security, availability, potential costs, etc. ? Depending on his position (safety service or safety authority, maintenance service, operator, designer, etc.), each analyst could apply his own criteria.

4.2 Validity and Merit of these Analyses

4.2.1 Validity and Merit of a Safety Indicator

Is risk induced by around thirty precursors, by all declared incidents, or by "near misses" (an operator is on the point of making a mistake but, at the last minute, realizes his error; two independent events occur on the same day, but with the "right chronology") ?

Cf. the communication "PSA Applications", paragraph on the complementarity of the ESSM and the Safety Index (Topic 2).

How should the very large year-to-year variations of the NRC Safety Index be interpreted : American reactors are not "very safe" one year and "not very safe" the next ?

4.2.2 Using these Analyses for Design and Operation

What sort of organization should be set up to ensure that the results of these analyses are channelled back to designers and operators ? Incident analyses require a large number of skills : knowledge of the plant, operation, reliability, human and organizational factors. Using these studies to enhance design or operation is even more demanding from this point of view. Collective thinking around this application has to be organized.

Can these analyses be used not only to find "chinks" in the "armour" of design and operation but also to find defences to these chinks ?

4.2.3 Safety Culture

Isn't accident precursor analysis a dangerous tool for an operator ?

- it is a complex tool : it is therefore likely to be used incorrectly;
- it is couched solely in terms of risk : it might therefore induce stress in operators;
- it is based on a single criterion (risk of core melt) and has no equivalent (which could be used for reference or comparison). It can therefore be either rejected or serve as the sole factor in a decision if a safety problem arises.

How can this decision-support tool be associated with other elements based on criteria of different kinds : availability, cost, doses, production or operation requirements, etc.

4.2.4 Validation of PSA

If the incident is merely an equipment failure, the corresponding reliability data is reviewed.

If an incident is a matter of human error, things are often more complicated : the event may not be modelized in the PSAs. Should it be added ?

If the event is a combination of equipment failures and human errors, the effect on PSA models is often very difficult to take into account. Let us look at some examples.

1. After the Chernobyl accident (TÜV Workshop - Hamburg - May 1990), the Soviets claimed they had quantified the probability of this scenario occurring. They found a probability of 10^{-9} ! They deduced from this that a PSA would not have revealed this scenario and would therefore have contributed nothing to the safety of RBMK reactors. If they had had a PSA for this type of reactor, they would probably not have doubted this study after the accident.

2. We have mentioned above the fact that the TMI type scenario is of very low probability in the PSA model for French PWR reactors (if it is assumed that the failures that caused the accident are independent). Does that detract from the quantification of this type of scenario in the PSA ? What exactly can be deduced from it ?

An incident always has a negligible probability of occurring "as is" in PSAs. It should be checked whether there is an "envelope" scenario for the incident in the PSA and whether its probability of occurrence is countered by the occurrence of the incident. But this is subject to interpretation :

Is a given scenario the "envelope" of the incident ?

What is the statistical value of an event ? After TMI, can it be said that the risk of core melt for an American reactor is about 10^{-3} (approximately one accident per 1,000 reactor years) and that PSAs giving probabilities of around 10^{-4} under-estimate the risk ?

5. CONCLUSIONS

"What's the point of giving a report on the previous day's weather ?" : that could be said of this method of analysis. What is the point of producing a method that assesses the risk *post hoc*, "after the horse has bolted" ? It could even be said that the *post hoc* risk of core meltdown is always zero since it has never happened.

In fact this method constitutes another point of view on safety : it is decided to attribute as much importance, from the point of view of information, to "near misses" as to actual incidents. This makes use of the immense quantity of knowledge in PSA.

This method makes it possible to understand "how serious it is" and also, and above all, "why it is serious". Whereas we content ourselves with a risk indicator when we do not how to understand "why it is serious", the probabilistic method should enable us to understand what the risk involves, particularly in the case where "hulls scraped" but the operator was not aware of it, or where the accident was more impending than experts thought.

Another important point not mentioned here in detail (refer to the communication on Topic 1, "Methodology"), but which should be referred to in the conclusion, is that the calculation methods are extremely important. When an incident is studied from the probabilistic point of view, it is often necessary to study combinations of unavailabilities. But it is not unavailability that matters but loss of the mission : if the grid is lost for 20 minutes, as is most frequently the case, the risk is practically zero, apart from the risk due to failure of Trip (there is no H3 or "black-out" sequence lasting less than one hour). What makes the H3 risk is the probability that the 20 minutes become 3 hours or 6 hours. Now finding this probability requires two vital conditions :

- the causes of the incident must be known, "in as far as possible", which works in favour of the conventional analysis of causes and the probabilistic analysis of consequences being performed by the same people, and the incident being analyzed "as close as possible" to the point where it occurred;

- you have to have mathematical models capable of satisfactorily modelizing the time dependencies that might exist in the accident sequences.

Furthermore, it must be stressed that :

- this work is still in the exploratory stages, and a lot of thinking and research remains to be done,
- we are a far cry from systematic, automatic methods, for, as we have seen, the analysis of incidents raises a whole host of questions that cannot easily be answered.

Lastly, to conclude, it can be said that risk analysis could perfectly well take place without incidents : what is the point of incidents occurring before they have been analyzed ? The best answer : "the fact that an incident has occurred contributes nothing other than to give us new ideas for enhancing the safety of our plants".

APPENDIX 1
EXAMPLES OF STUDIES

Case 1 : The Big Common Mode (climatic incident)

In January 1987, a wave of intense cold put out the electrical grid in the west of France.

On 12th January there were several incidents in succession on the unit (CP2 900 MW unit) :

- loss of the main 400 kV supply,
- turbine trip, emergency shutdown,
- switchover to the 225 kV auxiliary transformer,
- voltage drop on the auxiliary system,
- trip of several 6.6 kV pumps (ASG*, RRI*, SEC*, etc.) caused by the "maximum current" protection on the motors (risk H1* [total loss of the cooling water], break in primary coolant circuit pump seals, etc.),
- alarms on diesel generators (only available power sources), automatic coupling rejection (risk H3* [black out], etc.). Manual coupling of diesel generators.

The pumps were then started up by the operator. The main line was reconnected after 20 minutes.

On 13th January, in another incident declaration, the operator reported more difficulties due to the cold :

- blocks of ice in the Loire river (risk H1, etc.),
- freezing of the ASG*-degasser connection (unavailability of ASG tank feed in normal mode) (risk H2* [total loss of steam generator feedwater], etc.),
- freezing of VVP sensors (pressure measurement in steam pipes),
- freezing of level sensors in PTR* tank (IS* water supply). Immediate maintenance work; sensors pulled out; the automatic containment recycling system understood the tank to be empty (in the event of Safety Injection startup, the system immediately switches over to the empty containment sumps and the RIS* and EAS* pumps are destroyed).

The importance of the incident went relatively unnoticed because the operator broke it down into two incident reports. The probabilistic study of this incident is complex. Nevertheless, the conditional probability of core melt can be assessed at between 1 E-1 and 2 E-2. This makes it the most serious incident with French reactors that we have studied.

A single sequence represents the entire figure (see tree, Fig. 2) : the simultaneous loss of injection at the seals and of the thermal barrier of the primary coolant circuit pumps causes a LOCA which requires Safety Injection. The pumps then start up, connected to the empty containment sumps since the automatic system interprets the PTR tank as being empty. Safety Injection is thus totally unavailable. The sequence leads to core melt. The intervention by maintenance staff does not seem to have taken this sort of sequence into account. This sort of sequence requires understanding of the overall operation of the plant.

A single cause affects several equipment items of very different design and purpose. The seriousness of the incident is due to the common mode between the LOCA and the only associated line of defence. If the two events are considered as independent, the probability of such aggregation is infinitesimal.

This is a classic example of a large aggregation of failures on supposedly independent and different equipment. There may be other examples of Big Common Modes : other types of external aggression (earthquake, floods), maintenance (the same techniciäns with the same work sheets perform maintenance on the line breaker and the diesel generator couplers), etc.

The existence of such big common modes now makes it difficult to demonstrate that the total risk of core melt is less than 1 E-3.

It has thus been demonstrated that it is possible to lose supposedly unconnected equipment simultaneously and for the same reason.

Case 2 : Small Common Mode (switchboard fire)

A short-circuit on a 6.6 kV contactor caused a fire on the LHB* switchboard (6.6 kV B train with emergency diesel power).

The reactor (CP2 900 MW) was initially operating when a short-circuit in the 6.6 kV cell caused a fire which destroyed the LHB switchboard. The switchboard was out of action for 27 hours. In addition there was only one train A SEC* pump available at the time of the incident (the other SEC pump was under maintenance, and was put back on line again 5 hours after the start of the incident); The failure of the cell was due to the failure of one of its components (an operating mechanism damping washer). Subsequently a large number of damping washers on the LHA* sister board were also found to be in critical condition.

The probability value for the H3* initiator is due entirely to calculation of the common mode between the two switchboards (a result between 1E-1 and 1E-2, IPSN* and DER values). The failure of an H3 situation of this type is of the order of 1 E-1, which puts this incident just behind that described above in terms of seriousness (see tree, Fig. 3). The common mode between the two switchboards was calculated using a model with non-constant failure coefficients (ageing law).

It can be seen that the ASG* is the weak point in the plant : all the preponderant sequences include its failure. On the other hand, the unavailability of an SEC Essential Service Water System pump is of little effect. During control of the incident however, the operator was very concerned by the SEC system, and requalified the pump with a startup test, causing two operations in a cell which was already weakened.

What can be called the "small common mode" corresponds to the traditional definition of the beta factor (common-mode failure on identical equipment).

It should be noted that there is no common mode between the two switchboards in PSA models.

As a result, the analysis of this incident with basic PSA models determines a very low risk (about 1 E-6). Measurement of the seriousness of this incident is therefore very sensitive to the method of calculation of the common mode between the two emergency switchboards under emergency supply.

Case 3 : partial unavailability of the cooling water system

This incident occurred on a 1300 MW unit in September 1993. Apparently the unit had been shut down for about one month for maintenance on the underground pipework of the SEC* circuit.

Works were undertaken on one train, then the other, the fallback state chosen by the operator being intermediate shutdown, RRA valved in, with one primary coolant circuit pump on line. Analysis of the potential consequences of the incident performed by the operator revealed risk H1* (total loss of cooling water).

If studied from the probabilistic point of view, this prolonged unavailability reveals a potential scenario different to that mentioned by experts (the H1 risk due to loss of the redundant train).

Indeed, for unavailability of the train B RRI* (or train B SEC), the EPS 1330 PSA describes a more critical scenario (i.e. more serious and more frequent) than loss of the redundant train.

This scenario is described in the event tree in the appendix (Fig. 4). It consists of envisaging loss of the LBA* switchboard [125 V DC power system bus A]. Loss of the LNG [Continuous 220 V AC Power System] results in similar effects : LBA loss causes total loss of cooling to the bearings of the primary coolant circuit pumps as well as making it impossible to manually or automatically stop the operating primary coolant pump from the Control Room. The pump then continues to operate without cooling and without protection. Studies refer to a 30-minute period after which overheating causes the shaft to seize; the pump stops, causing a LOCA. Failure of LOCA control is certain since Safety Injection is totally unavailable without LBA and without train B RRI.

Without recovery of the initiator (LBA or train B RRI), the only line of defence is to shut down the primary pump locally (impossible to use a pendant-control box) or to open the line breaker. Human reliability studies reveal the weakness of these lines of defence : there is little time available, and the operation is not easy to perform.

Calculation of the sequence gives rise to several comments.

- The risk of core meltdown due to LBA loss (2 E-5) is about 70 times higher than the risk due to Train A RRI loss (3 E-7). That is why it is the former risk that is always referred to by safety experts.

- The study reveals a substantial disproportion between the risk linked to unavailability of RRI/Train A SEC and unavailability of RRI/Train B SEC. This is because this scenario does not exist in the event of unavailability of RRI/Train A SEC.

- There are uncertainties : in the context of the incident (ground movement and works on SEC pipework) the type "H1" hourly risk is certainly higher than the basic data of the EPS 1300 PSA. On the other hand, feedback shows that the probability of failure of the

LBA (5.5 E-3 per reactor year) is essentially due to maintenance works when the unit is shut down. This assumption remains valid even if, as is probably the case, all works on Train A are prohibited during the period during which the SEC/B is locked out.

- Finally, the study shows that it is absolutely necessary to choose a fallback state with primary coolant circuit pumps shut down, or at least to prepare operators for the eventuality of such a sequence. **This is the main lesson learnt from the study.**

Case 4 : mistaken action

Locking out of safety injection by the operator (1300 MW, 1993).

During a low-power test, a valve on the condenser bypass circuit jammed in the open position. The loss of steam from the secondary cooling circuit resulted in uncontrolled cooling of the core.

Thinking he had the situation under control, the operator chose a programmed cooling procedure and locked out the automatic Safety Injection startup system.

What is the risk involved in this incident, i.e. the conditional probability of core melt associated with the mistaken action of the operator ?

There are two ways of analyzing the situation :

- one can start from the "secondary coolant steam boost" transient that is studied in the EPS 1300 PSA, or
- extend the mistaken action to all the initiating events requiring startup of Safety Injection.

The first analysis can be deduced from one of the EPS 1300 PSA event trees (see tree 1, Fig. 4). The second analysis is more complicated : what is the probability of such action occurring under circumstances different to the actual circumstances (Tree 2) ? In other words, the operator could have disactivated the SI system in a situation where it was in fact required, as with small LOCAs for example. There is time for such manual disactivation to occur, but misinterpretation of events is less likely than in the incident under study. Quantification of human error is more difficult in this case.

It is relatively easy to quantify the risk consecutive to this initiating event (the risk is low; see Tree 1). On the other hand, this value is not all-encompassing. The unwarranted action could have occurred under other circumstances where the risks would have been greater (see Tree 2). This is what is called variation around the "initial status of the plant" (cf. below, § 4.1.3.). It is then very difficult to assess the probability of operator error. Nevertheless, from human reliability data, we know that the probability is greater than 1E-3. The risk is therefore greater than 2E-6.

To appreciate the total risk, all the scenarios where SI is required and there is enough time for it to be disactivated must be taken into account.

GLOSSARY

AGR :	Advanced Gas Reactor
ASG :	Auxiliary Feedwater System
AU :	Trip
DSIN :	French safety authorities
EAS :	Containment Spray System
ESSM :	Essential System Status Monitor
GMPP :	Reactor Coolant Pump
GV :	Steam Generator
H1 :	Total loss of Service Water or Component Cooling System
H2 :	Total loss of Steam Generator Feedwater
H3 :	Total loss of emergency supplied power system (Black out)
INES :	International Nuclear Event Scale
IPSN :	Technical support of DSIN (French safety authorities)
IS :	Safety Injection System
LBA :	125 V DC power system train A
LCA :	Relaying 48 V DC power system train A
LHA, LHB :	6.6 kV AC Emergency Supplied Power System trains A and B
LNG :	Continuous 220 V AC Power System
LOCA :	Loss of Coolant Accident
PTR :	Boric acid tank for SIS and CSS (Reactor Water Storage Tank)
RCV :	Charging pump
RIS :	Safety Injection System
RTGV :	Steam Generator Tube Rupture (SGTR)
RRI :	Component Cooling System
SEC :	Essential Service Water System
VVP :	Main Steam System

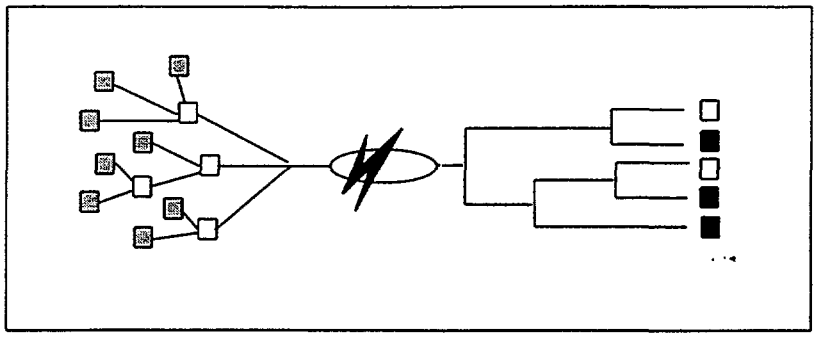


FIGURE 1 : the link between causes and consequences

This figure features on the cover of the "Guide to Incident Analysis" that the management of EDF nuclear reactors has issued to all EDF nuclear power plants. It symbolizes the complementarity of conventional analysis of the causes of an incident (fault tree for faults upstream of the incident) and analysis of potential consequences (fault tree downstream).

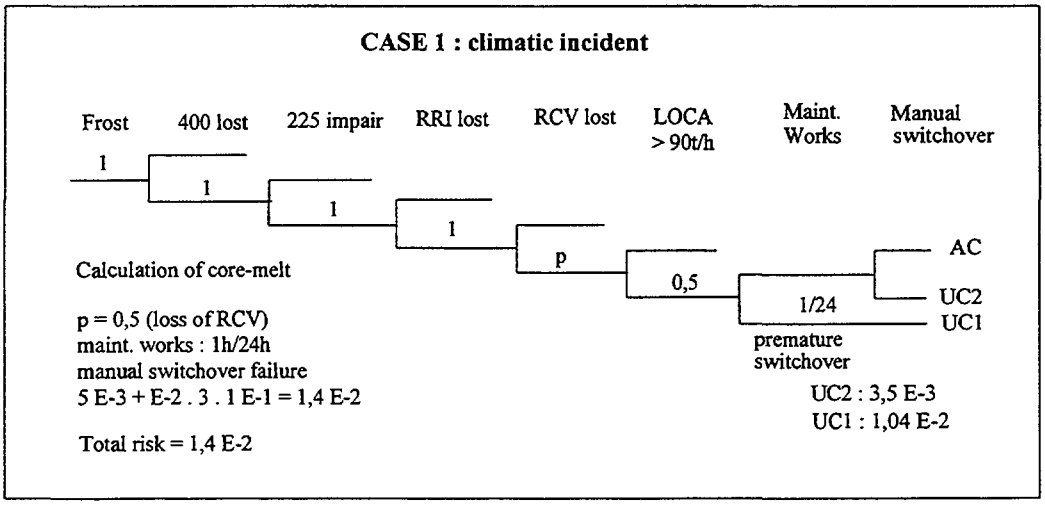


FIGURE 2

This event tree presents one of the scenarios that could have led to unacceptable consequences during a brutal cold snap in the west of France in 1987. The seriousness of the incident is entirely due to the common mode between the initiating event (LOCA on primary coolant pump seals) and the defence designed to counter it (safety injection). The LOCA could have been caused by simultaneous loss of seal injection (RCV) and of the thermal barrier (RRI) : some pump motors tripped when the system voltage dropped.

Safety Injection could have been lost in two ways :
- unwarranted switchover of SI pump suction to empty sumps due to pulling out of level sensors in the PTR tank (UC1),
- failure of manual switchover to sumps, the automatic system being out of action due to freezing of level sensors (UC2).

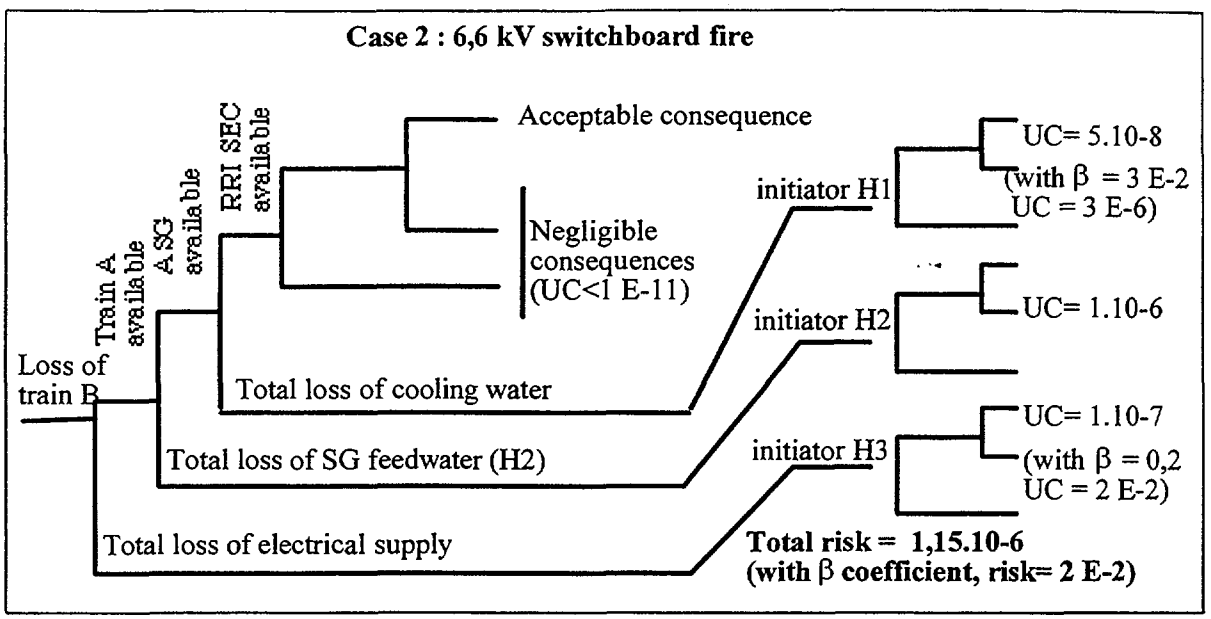


FIGURE 3

This event tree shows the three main modes for potential degradation into an accident with unacceptable consequences which could have developed following a fire on a 6.6 kV electrical switchboard. The loss of the ASG is the preponderant sequence of trees H1, H2, and H3. It is therefore important to monitor the proper operation of the SGs during the entire duration of the incident. Measurement of the seriousness of the incident depends much on the value of the β common mode between the two emergency switchboards. This value can be calculated in several ways. In our opinion, the most robust calculation involves very detailed analysis of the cause of the fire (failure of a contactor component) and uses a reliability model with non-constant coefficients (Weilbull law).

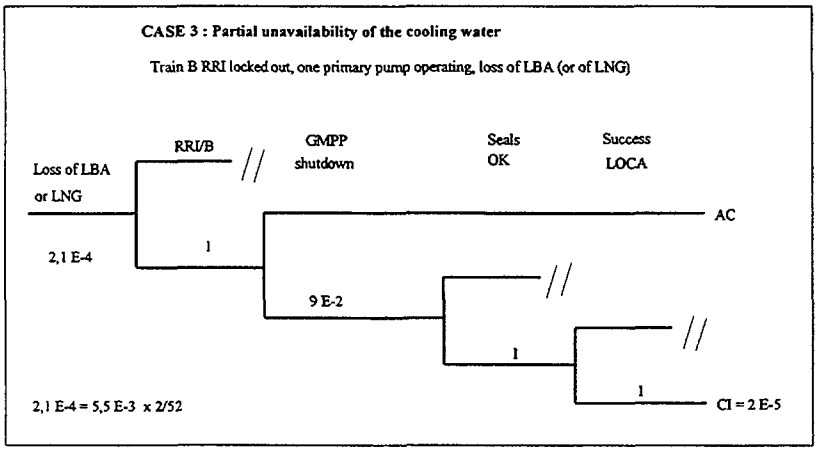


FIGURE 4

The unit (1300 MW PWR) was shut down for a month in September 1993 for rehabilitation works on the underground pipework of the SEC Essential Service Water System circuit. For 15 days, each SEC train was therefore locked out. The risk envisaged by the operator at the time was simultaneous loss of the two SEC trains (H1 situation).

The tree shows another sequence which is far more critical. In the event of loss of a 125 V switchboard, cooling of the seals of the primary coolant circuit pumps is lost, and the pumps can only be stopped locally. In the event of failure, Safety Injection is then unobtainable, and the LOCA at the seals leads to unacceptable consequences. Simultaneous loss of the Train B SEC and the Train A 125 V results in a LOCA and failure of the only associated defence.

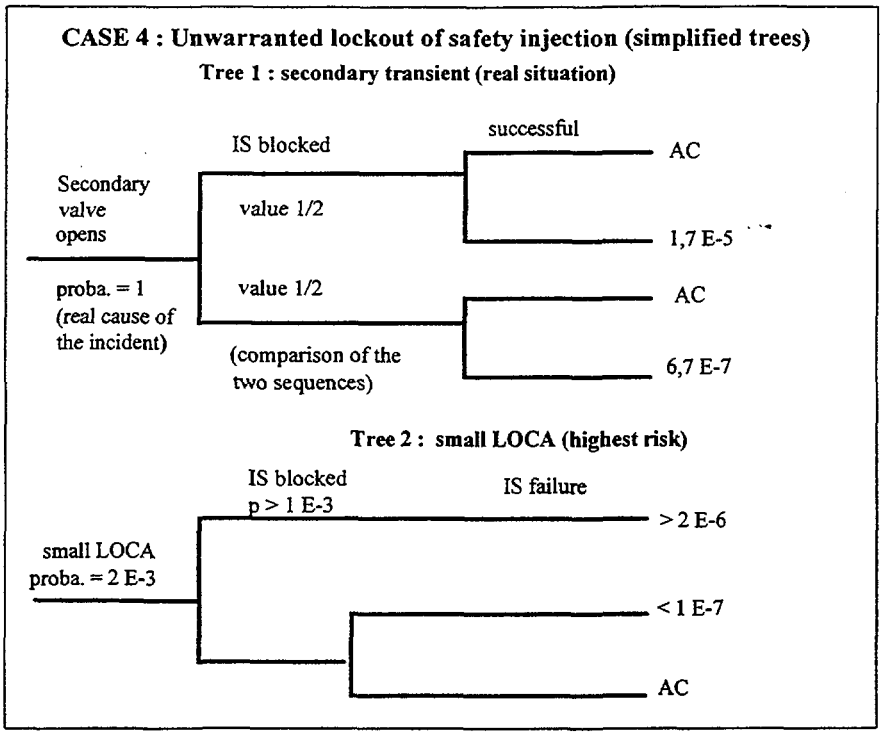


FIGURE 5

During a low-power test on on a 1300 MW PWR power plant, a valve on the secondary coolant circuit jammed in the open position. This caused uncontrolled cooling of the core. Thinking that cooling was a normal result of startup of the ASG, the operator chose a normal cooling procedure and locked out the automatic system for startup of safety injection.
What is the risk associated with this incident ?
Two analyses are possible : consider only the transient that actually occurred ("secondary coolant steam boost"), or extend the erroneous operation to all initiating events that require IS startup.
The first analysis can be deduced from an event tree of the EPS 1300 PSA (tree 1). The second one is more difficult : what value can be given to the probability of such action in a context other than the real context (tree 2), for the operator could indeed have locked out IS in another situation where it was in fact required : this is the case, for example, with small LOCAs. The times available make this lock-out possible, but an error in diagnosis is less probable than in the incident studied.
It is therefore relatively easy to assess the risk due to the real initiating event of January 20th (tree 1). Nevertheless, one knows that this value is not an envelope value. The erroneous action could have been performed under circumstances where the potential risk is greater (tree 2). To determine the total risk, it is necessary to take account of all the initiating events where safety injection is required and where the time available allows it to be locked out.

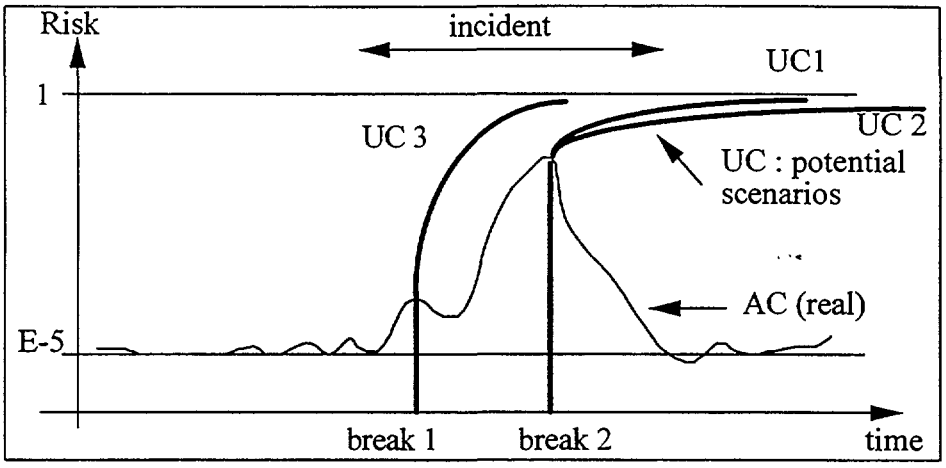


FIGURE 6 : the problem of the break

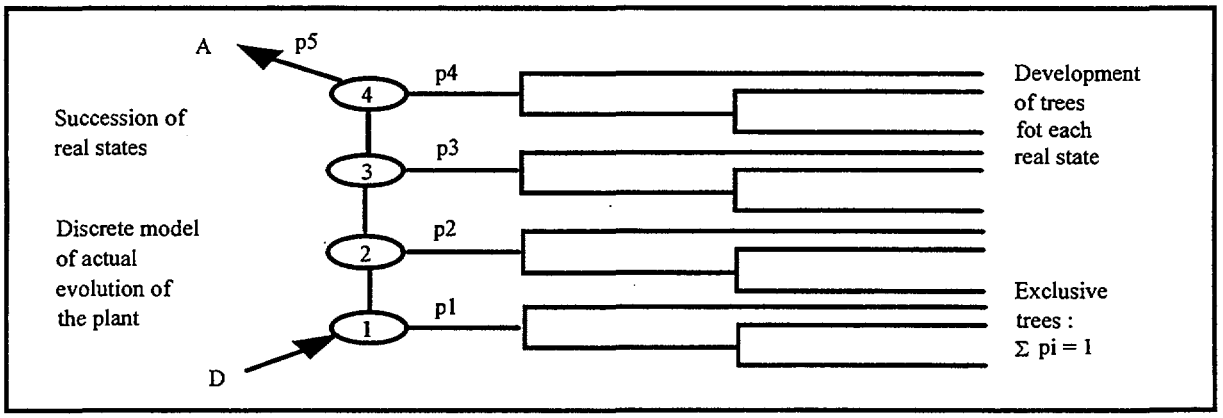


FIGURE 7 : example of a solution

In the case of complex incidents or incidents which last any length of time, specific questions must be asked : how, and when during the incident should one determine the starting point for potential aggravation sequences ? In other words, what moments in the incidents should be chosen to initiate the potential aggravation scenarios ?

Figure 6 illustrates this problem. A nuclear power plant is an installation that is continually evolving within a "risk space" limited by a lower boundary (everything is available, optimum safety) and an upper boundary (probability of unacceptable accident = 1). The value of the risk fluctuates above the lower boundary and can deviate substantially from it during an incident. An incident is therefore a moment in the history of the plant when this function reaches extremes. Probabilistic analysis consists in trying to identify some of these extremes and to make a break between what actually happened afterwards and the potential aggravation scenarios. In Figure 6 three possible scenarios (aggravation sequences) are started at two moments in the incident (breaks). A break separates the determined past from possible futures. Since one cannot know the risk-function beforehand, the break is made at the point where the risk is assumed to be highest.

Figure 7 represents the modelization that can then be made of the incident : a succession of plant states defines a succession of initiating events. Each initiating event is associated with one or more event trees.

This type of modelization is still wholly experimental. It should concern a very restricted number of incidents. But it seems that they are the most important ones.