IMPACT DU RISQUE DANS LES ETATS D'ARRET SUR LE CALCUL DES SPECIFICATIONS TECHNIQUES D'EXPLOITATION

IMPACT OF SHUTDOWN RISK ON RISK-BASED ASSESSMENT OF TECHNICAL SPECIFICATIONS

EDF

Electricité de France

Direction des Etudes et Recherches

SERVICE RÉACTEURS NUCLÉAIRES ET ECHANGEURS
Département Etudes de Sûreté et de Fiabilité

Octobre 1992

DERIOT S.

IMPACT DU RISQUE DANS LES ETATS D'ARRET SUR LE CALCUL DES SPECIFICATIONS TECHNIQUES D'EXPLOITATION

IMPACT OF SHUTDOWN RISK ON RISK-BASED ASSESSMENT OF TECHNICAL SPECIFICATIONS

Pages : 16

93NB00061

Diffusion : J.-M. Lecoeuvre
EDF-DER
Service IPN. Département SID
1, avenue du Général-de-Gaulle
92141 Clamart Cedex

ISSN 1161-0611

SYNTHÈSE :

Cette note décrit le travail actuellement accompli par la Direction des Etudes et Recherches concernant l'utilisation des études probabilistes pour le calcul des Spécifications Techniques d'Exploitation (STE).

On présente l'utilisation faite à EDF des études probabilistes pour le calcul des STE. Puis, on décrit l'étude probabiliste de Sûreté de niveau 1 (appelée EPS 1300) de la tranche 3 de la centrale nucléaire de Paluel. L'EPS 1300 est entièrement informatisée et prend en compte le risque dans les états d'arrêt.

Une étude de cas est présentée. Elle montre que le fait de considérer le risque dans les états d'arrêt implique que les STE actuelles devraient être modifiées.

EXECUTIVE SUMMARY :

This paper describes the current work performed by the Research and Development Division of EDF concerning risk-based assessment of Operating Technical Specifications (OTS).

The current risk-based assessment of OTS at EDF is presented. Then, the level 1 Probabilistic Safety Assessment of unit 3 of the Paluel nuclear power station (called PSA 1300) is described. It is fully computerized and takes into account the risk in shutdown states.

A case study is presented. It shows that the fact of considering shutdown risk suggests that the current OTS should be modified.

1. INTRODUCTION

This paper describes the current work performed by the Research and Development Division of EDF concerning risk-based assessment of Operating Technical Specifications (OTS).

The current risk-based assessment of OTS at EDF is presented. Then, the level 1 Probabilistic Safety Assessment of unit 3 of the Paluel nuclear power station (called PSA 1300) is described. It is fully computerized and takes into account the risk in shutdown states.

A case study is presented. It shows that the fact of considering shutdown risk suggests that the current OTS should be modified.

2. CONTEXT

At EDF, one of the objectives of the OTS is to determine what actions have to be taken when a component or set of components is unavailable. Many Allowed Outage Times (AOTs) have been evaluated a few years ago based on a probabilistic criterion used in agreement with French Safety Authorities: "the additional occurrence probability of a serious accident (leading to core melt) while the nuclear plant is operating at full power during the authorized time period, given the partial unavailability of the safety system, must not exceed 10^{-7}". The AOT is the duration of time that the component or system can remain out of service before the plant has to shut down.

Then, the AOT associated with the unavailability of a component or system can be calculated using the following relationship:

$$\Delta R \cdot T = 10^{-7}$$

where:

ΔR is the increase in plant's core melt hourly risk as result of the unavailability of a component or system

T is the suggested AOT (in hours), which is afterwards debated between EDF and the safety authorities

Figure 1 describes this relationship.

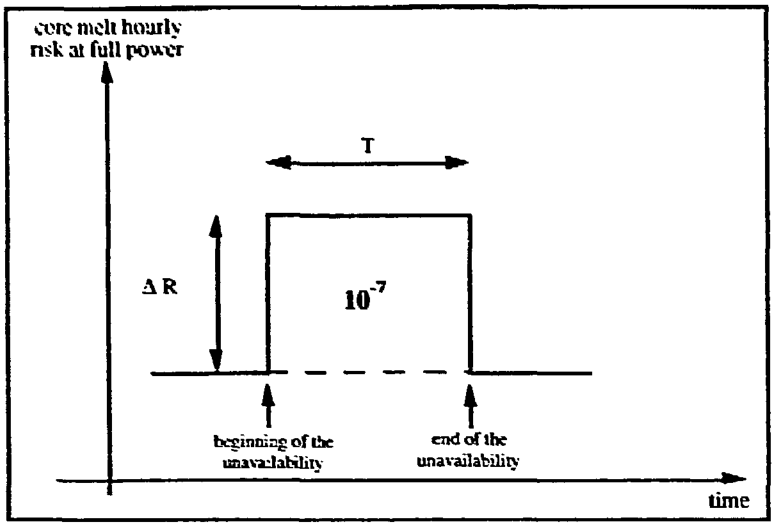


Figure 1

Since we consider the increase of risk as a result of the unavailability of a component or system in a reactor state (in this case, full power), only the accidents relevant to this unavailability and this reactor state require to be studied.

3. PRESENTATION OF THE PSA 1300

EDF conducted the project PSA 1300 from 1986 to the end of 1989 (1) (2).

Two aims have been assigned to the PSA 1300 project:

- evaluation of the probability of damage to the core of reactor unit 3 in the Paluel nuclear power plant, in all reactor states and with a degree of detail as high as possible,
- provision of a computer program for the performance of this evaluation, the LESSEPS software package, in order to produce a PSA with scope for development (3).

3.1 Operating profile

The analysis of the operational feedback made it possible to establish the average time spent in different unit states. The reactor states defined for the PSA and the annual durations associated with them, are as follows:

STATE	SUB-STATE	DESCRIPTION	TIME IN DAYS
state a		Operating point (pressure, temperature) above (P11, P12) (139b, 295°C at Paluel) which corresponds to the standard states:	
	a1	- reactor in power, set coupled	268
	a2crit	- reactor critical, set not coupled	12
	a2sub	- reactor subcritical	15
state b		Operating point (pressure, temperature) between (P11, P12) and Residual Heat Removal System conditions (30b, 177°C)	2 (38 hours)
state c		Shutdown on RHRS, Reactor Coolant System (RCS) full, closed and vented	11
state d		RCS partially drained or open (conservatively, it is the state in which the level of the RCS is in the low work range of the RHRS and where there is minimum reactor coolant mass)	19
state e		Refuelling cavity full with at least one fuel element in the vessel	9

3.2 LESSEPS 1300

A computerized knowledge base called LESSEPS 1300 was developed in the framework of the project PSA 1300. It is a set of reliability models, computation methods and computer tools. It comprises about 200 fault trees, 150 states graphs and 200 event trees (4).

The partial or total unavailabilities of safety systems are generally introduced in the form of a "balloon" (all the components rendered inoperable during maintenance) for which outage rate is calculated on the basis of feedback from operating experience on the Paluel power plant. By performing sensitivity studies on the outage rates associated with each balloon, LESSEPS 1300 allows the evaluation of the "new" annual risk in each reactor state. If we divide by the annual durations spent in different reactor states, we could deduce the measure of the "new" mean hourly risk in each reactor state, given the unavailability.

3.3 Limitation about the use of the PSA 1300 for OTS

Since the PSA 1300 is a level 1 PSA, only systems that take part in preventing core melt have been modelled. This is the reason why the number of single unavailabilities relevant with respect to the use of the PSA 1300 is quite low. The PSA 1300 is not useful at all for components that are only involved in containment or in the operability of the plant (e.g., Containment Atmosphere Monitoring System, primary coolant pumps).

4. CASE STUDY

One of the main lessons of the PSA 1300 is the significant role played by shutdown states (which account for approximately 55% of risks). Then, the following question becomes important: does the shutdown really lead to minimizing the increase of risk due to the unavailability of a safety-related component ?

The study of the long-term unavailability of a Medium-Head Safety Injection (MHSI) pump was carried out.

NB: the results presented below do not include the results of the following accident sequence studies: the total loss of heat sink and the total loss of emergency power supply, which have been updated recently, but which have not yet received approval.

4.1 Description of the study

In the "reference" calculation of the hourly risk in each reactor state, none of components is assumed to be in maintenance. This is the reason why all outages have to be put to zero.

However, the impact of outages on the results is almost negligible: for example, the risk at full power with the basic outages of the PSA 1300 is about 5.8E-10 /h, while the same one without any unavailability is about 5.6E-10 /h.

For each event tree, we calculate the hourly risk for all reactor states associated with this event tree.

Particular attention has to be paid to one dilution sequence. For this dilution sequence, the initiating event is the loss of the main electric power supply (leading to the loss of the primary pumps) during dilution related to the criticallity search after a shutdown.

This criticallity search occurs after a refueling shutdown, or after a hot shutdown or after a cold shutdown if it is the beginning of cycle. Its duration depends on the kind of shutdown. Then, the annual risk associated with this sequence depends on both the annual number and the kind of shutdowns. Moreover, the hourly risk due to this sequence is not the division of the annual risk by the annual duration of the state "reactor subcritical".

The hourly result of this sequence is then subtracted from the hourly risk in the state "reactor subcritical" and put aside.

Supposing the unavailability of a MHSI pump, and putting to one the outage rates associated with the balloon of the pump, a sensitivity calculation can be performed. Figure 2 shows the comparison of the results of the "reference" calculation with the results of this sensitivity study.

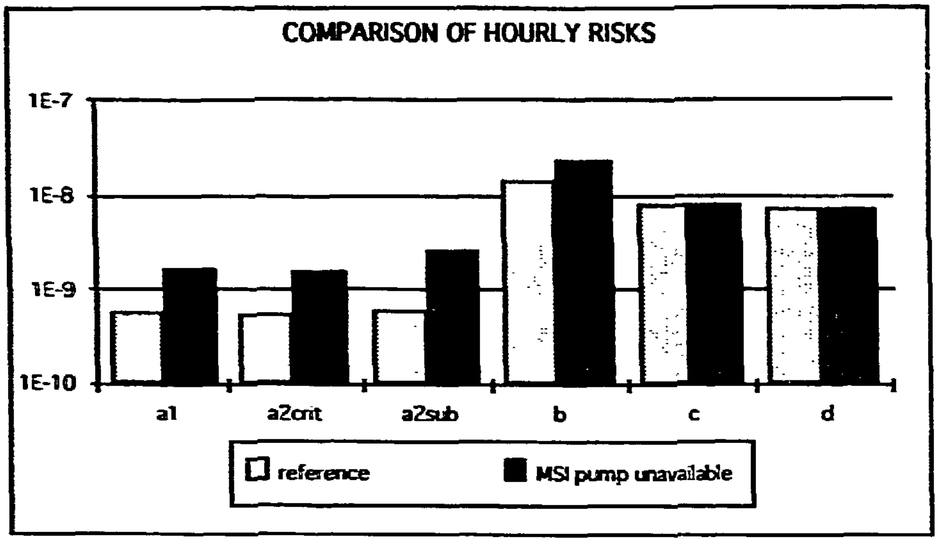


Figure 2

The AOT associated with the unavailability of a MHSI pump can then be calculated using the following relationship:

$$T = 10^{-7} / (R'_{a1} - R_{a1})$$

where:

T is the suggested AOT

$\mathbf{R'_{a1}}$ is the hourly risk at full power, given the unavailability of a MHSI pump

$\mathbf{R_{a1}}$ is the hourly risk at full power without any unavailability

$$T = 10^{-7} / (1.67E\text{-}9 - 5.6E\text{-}10) = 90 \text{ hours}$$

Thus, the AOT associated with the unavailability of a MHSI pump and calculated with the current method seems to be about 4 days.

Suppose that the failure of the MHSI pump requires 5 days to be repaired. The current safe shutdown condition is the intermediate shutdown with the Residual Heat Removal System (RHRS) valved-out (30b, 177°C). Figure 3 shows the distribution of the hourly risks in different reactor states and the evolution of the primary pressure when the current OTS are enforced. The specific sequence occurring during a phase of dilution is included; here, after a hot shutdown, the duration of this phase of dilution is about 2.5 hours.

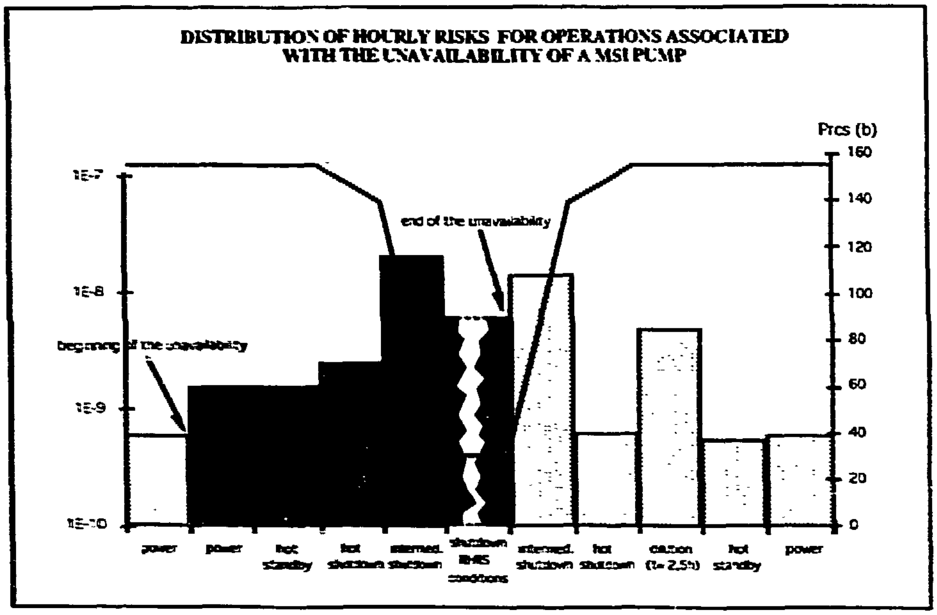


Figure 3

We can easily notice that, whatever the duration of the unavailability of the MHSI pump may be, the increase of risk associated with operating until the "safe" shutdown condition is far higher than that associated with remaining at full power or shutting down until hot standby. As a matter of fact, by operating until the intermediate shutdown:

- one denies oneself the automatic start-up of the Safety Injection System (SIS) for most of LOCAs, even if this system is partially unavailable;
- one increases the frequency of the accident for which the unavailable component is principally designed, because the isolation valves on the relief lines of pressurizer are forced open.

4.2 Discussion about results

The PSA 1300 was conducted in order to evaluate the probability of damage to the core per unit and per year. Thus, some conservative assumptions were kept because they had no impact on the annual probability. Here, for risk-based assessment of OTS, we argue about hourly risks. This is the reason why some of those assumptions have had to be reviewed.

Concerning the case study, the main assumptions are the following ones:

- The rate of primary breaks per hour has been assumed to be equal to that applied at the nominal temperature and pressure. Although this might seem to be a conservative estimate, most breaks are caused by erosion or corrosion, and are more likely to arise under transient conditions than under normal operating conditions. In this respect, there has been no proof that failure rates are substantially lower at low pressure or low temperature than under nominal conditions.

- The success criteria of SIS for a small LOCA are the same during the whole intermediate shutdown; while in the intermediate shutdown state with the RHRS valved-out, one MHSI pump is not absolutely necessary to mitigate a small LOCA: one out of the four safety injection pumps (low-head or medium-head) is adequate to prevent core damage. Therefore, the failure probability of SIS in the safe shutdown condition is lower than in the rest of the intermediate shutdown state.

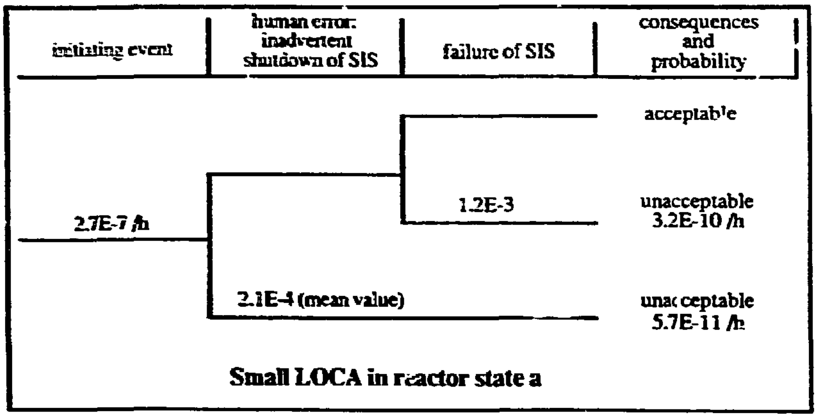
- The time t after which the operators have to start-up the safety injection system in response to a break in a steam line of the pressurizer was assumed to be unique in the whole intermediate shutdown state (i.e., the minimal time corresponding to the upper part of the intermediate shutdown state). Therefore, the probability p of this operator error is lower in the intermediate shutdown state with the RHRS valved-out (30b, 177°C: t=2h and p=1.4E-3) than at the upper part of the intermediate shutdown state (139b, 295°C: t=1h and p=4.2E-3).

The previous distribution of hourly risks takes into account the modifications concerning the last two assumptions, which are related to the construction of reliability models.

4.3 Towards a new management of operations ?

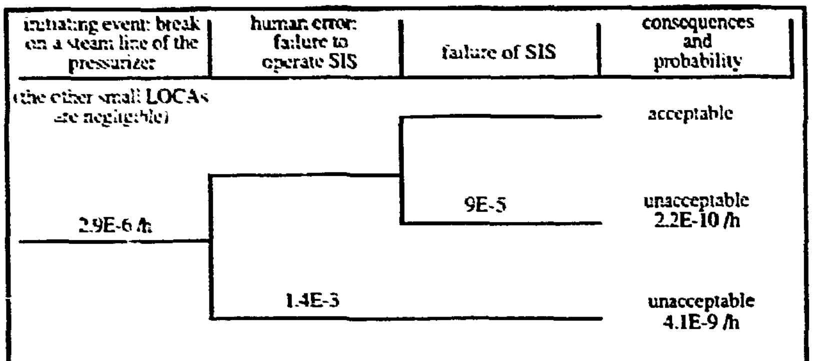
For the long-term unavailability considered (5 days), and whatever the current managements of the operations may be (i.e., remaining at full power or shutting down until 30b), the probabilistic criterion of 10^{-7} cannot be respected. The solution could be a change in the way of shutting down.

Using very simplified event trees, let us compare the accident "small LOCA" in the "safe" shutdown condition and in reactor state a, given the unavailability of a MHSI pump:



Small LOCA in reactor state a

Adding breaks on a steam line of the pressurizer, the overall risk related to a small LOCA in reactor state a is about 4.2E-10 /h.


initiating event: break on a steam line of the pressurizer
human error: failure to operate SIS
failure of SIS
consequences and probability
(the other small LOCAs are negligible)
2.9E-6 /h
1.4E-3
9E-5
acceptable
unacceptable 2.2E-10 /h
unacceptable 4.1E-9 /h

Small LOCA in the safe shutdown condition (30b, 177°C)

The overall risk related to a small LOCA in the intermediate shutdown state with the RHRS valved-out is about 4.3E-9 /h. It is higher than at full power, although the reliability of SIS is better.

Supposing that a Low-Head Safety Injection (LHSI) pump was manually started-up as soon as the reactor is in state b. The risk in the "safe" shutdown condition due to the accident "small LOCA" would be approximately of the order 10^{-10} /h. This new management of operations would permit:

- to avoid the non-automatic start-up of SIS,
- to profit by the redundancy of the four safety injection pumps.

Thus, the intermediate shutdown state with the RHRS valved-out would be the "real" safe shutdown condition.

4.4 Comparison between the different managements of operations

The duration of the unavailability of the MHSI pump is supposed to be 5 days.

The increase of risk associated with remaining at full power is:

$$S_1 = (R'_{a1} - R_{a1}) \, 120$$

where:

R'_{a1} is the hourly risk at full power, given the unavailability of a MHSI pump
R_{a1} is the hourly risk at full power, MHSI pump available
120 is the duration of the unavailability in hours

$$S_1 = 1.3E\text{-}7$$

The increase of risk associated with operating until the return to the initial state (and through the current "safe" shutdown condition) is:

$$S_2 = \Sigma_i R'_i t_i + \Sigma_j R_j t_j - R_{a1} (120 + \Sigma_j t_j)$$

where:

i is the reactor state from power until the safe shutdown condition

R'_i is the hourly risk in state i, given the unavailability of the MHSI pump

t_i is the duration of time in state i

j is the state from the safe shutdown condition (not included) to return to power

R_j is the hourly risk in state j, MHSI pump repaired

t_j is the duration of time in state j

The calculation gives: $S_2 = 8.5E-7$

As was planned in figure 3, the current management is not the best one.

Supposing that one LHSI pump was manually started-up as soon as the reactor is in state b. Another calculation gives the increase of risk associated with this arrangement: it is about 1E-7. We can notice that the gain (with regard to remaining at full power) is not very important for this duration of the unavailability of a MHSI pump. This is due to the risk during the transient states. The gain would be higher for a longer duration of the unavailability.

5. CONCLUSION

This paper is aimed at demonstrating that the PSA 1300, which is fully computerized and which takes into account risk in shutdown states, is a powerful tool for risk-based assessment of Operating Technical Specifications (OTS).

The PSA 1300 emphasized the importance of risk in shutdown states. The current design of reactor units is, in fact, based on the premise that there will be little risk arising in shutdown states. Consequently, the majority of analyses carried out and design considerations adopted for systems and automatic equipment have been based on reactors under operating conditions. It is therefore essential to consider the increase of risk associated with operating from the occurrence of the unavailability of a component until the return to initial condition. People involved in PSA area become more and more aware of this necessity (5) (6).

The computerized PSA represents an overall view of safety of the plant, and not a "system view" of safety. When we consider the increase of risk at full power, only the accidents at full power impacted by the partial or total unavailability of a safety system require to be studied. But it becomes essential to take into account all the accidents when we consider a change of reactor state. For example, considering the unavailability of a diesel generator and the accidents impacted by this component, i.e., essentially station blackout, the "safe" shutdown condition seems to be the intermediate shutdown. Thus, we "forget" that the unit is, in this reactor state, quite vulnerable towards primary breaks. The computerized PSA does not "forget"...

Thus, it appears that a risk-based assessment of OTS has the potential to better control plant operational risk compared to a deterministic assessment. Nevertheless, it is necessary to remain modest: there are many factors, physical and operating, that a purely probabilistic approach cannot take into account. Moreover, the use of this tool is confined to a limited number of safety components.

In this paper, a new method, developing at Electricité de France, for risk-based assessment of OTS has been presented through a case study. The main outlines of this method are an evaluation of the core melt hourly risk (due to all types of accidents) in different reactor states and an interpretation of results. It can help to determine not only the Allowed Outage Time, but also the "real" safe shutdown condition and in some cases the way of shutting down. However, some improvements in the reliabilistic models in shutdown states have to be made.

REFERENCES

(1) Villemeur, A., Berger, J.P., Dubreuil-Chambardel, A., Moroni, J.M., "Living Probabilistic Safety Assessment of a French 1300 PWR NPP Unit: Methodology, Results and Teachings", 2nd TÜV-Workshop on Living PSA Application, Hamburg, 7th-8th May, 1990.

(2) Berger, J.P., Villemeur, A., De Guio, J.M., "PSA 1300; Results and Future Prospects", International Symposium on the Use of Probabilistic Safety Assessment for Operational Safety, PSA'91, Vienna, Austria (3-7 June 1991).

(3) Ancelin, C., Lucas, J.Y., Magne, L., Bouissou, M., Molinero, J., "LESSEPS or a Computerized Management of Reliability Studies", 7th International Conference Reliability & Maintenability, Brest, France (June 1990).

(4) Ancelin, C., Dubreuil-Chambardel, A., "From LESSEPS 1300 to the Application of Computerized PSAs to Operational Safety", International Symposium on the Use of Probabilistic Safety Assessment for Operational Safety, PSA'91, Vienna, Austria (3-7 June 1991).

(5) Sandstedt, J., Berg, U., "Living-PSA Applications for a Swedish BWR with the Aid of RISK SPECTRUM", 3rd TÜV-Workshop on Living PSA Application, Hamburg, 11th-12th May, 1992.

(6) Nakai, R., "Application of a Living PSA system to LMFBR", 3rd TÜV-Workshop on Living PSA Application, Hamburg, 11th-12th May, 1992.