2009 International Nuclear Atlantic Conference - INAC 2009
Rio de Janeiro,RJ, Brazil, September27 to October 2, 2009
ASSOCIAÇÃO BRASILEIRA DE ENERGIA NUCLEAR - ABEN
ISBN: **978-85-99141-03-8**

APPLICATION OF THE FAILURE MODES AND EFFECTS ANALYSIS TECHNIQUE TO THE EMERGENCY COOLING SYSTEM OF AN EXPERIMENTAL NUCLEAR POWER PLANT

Osmar Conceição Junior[1] and Antonio Teixeira e Silva[2]

[1] Centro Tecnológico da Marinha em São Paulo
Av. Professor Lineu Prestes 2468
05508-900 São Paulo, SP
osmarjr@usp.br

[2] Instituto de Pesquisas Energéticas e Nucleares, IPEN - CNEN/SP
Av. Prof. Lineu Prestes, 2242
05508-000 São Paulo, SP
teixeira@ipen.br

ABSTRACT

This study consists on the application of the Failure Modes and Effects Analysis (FMEA), a hazard identification and a risk assessment technique, to the Emergency Cooling System (ECS), of an experimental nuclear power plant. The choice of this technique was due to its detailed analysis of each component of the system, enabling the identification of all possible ways of failure and its related consequences (in order of importance), allowing the designer to improve the system, maximizing its security and reliability.
Through the application of this methodology, it could be observed that the ECS is an intrinsically safe system, in spite of the modifications proposed.

1. INTRODUCTION

There are a great number and variety of hazard identification and risk assessment techniques, useful and applicable to the project of a nuclear power plant in order to identify possible accident starting events and verify their most important and likely consequences. Among them, the Failure Modes and Effects Analysis (FMEA) is one of the most famous and used one, largely employed in different fields of industry such as aircraft, automobile and nuclear industries.

The purpose of this article is to demonstrate the main results of the utilization of such technique in the Emergency Cooling System (ECS) of an experimental nuclear power plant.

2. MAIN REASONS TO JUSTIFY THE CHOICE OF THE FMEA TECHNIQUE

The identification of vulnerabilities and specific hazards has critical importance to the accidents prevention process.

Once correctly and adequately identified, a major step in the direction of solving the problem of risk assessment has been reached, however this task is not simple (usually, more complex the technology involved much more difficult becomes the process).

According to LEES [1], as time goes by, the accidents prevention activity is supposed to increase its dependency on the management systems and it is not that simple to find weaknesses on these systems. Also the hazards, most of the times, are not so simple and easy to detect that could enable their identification only through a visual inspection. On the other hand, there are, nowadays, a great number of hazard identification and risk assessment techniques which can be used to solve this problem.

Distinct methods are more suitable for the each stage of the design process and there is no specific or ideal procedure, to the hazard identification and risk assessment activities.

The choice of the FMEA technique was due to, as KUMAMOTO [2] assures, it systematically details, for each component, all possible ways of failure, identifying its consequences on the plant, enabling the introduction of improvements and/or the correction of the defects, earlier on design process.

Possible deficiencies in each equipment of the system are analyzed to find its effects in other components related to it.

Another technique that could be employed, as a complement to the FMEA, is the Fault Tree Analysis (FTA), which has a deductive character and is more suitable for the cases in which the failure mechanisms are more complex.

Some difficulties in the utilization of the FTA are: it requires, from the well trained and qualified analysts, a greater spent of effort and time and, although it is one of the best tools to analyze the system as a whole, it does not assure, by itself, the detection of all the possible failures, specially those which have a common cause.

This problem is particularly critical in systems such as those who are part of the nuclear reactor nuclear, where a high level of reliability is demanded (which is the case of the ECS, to be analyzed).

Theoretically, the calculated reliabilities are extremely high but there is some distrust in relation to these numbers due to the dependent failure phenomenon, which may be hided in so many ways.

The HAZOP technique, besides its main utilization in the process analysis, has basically two types of limitations:

- the first one comes from the assumptions concerning to this methodology and constitute an aim limitation. On its original form, the technique assumes that the project was lead according the appropriate regulations; and
- the other is intrinsic to the method. The HAZOP technique is not adequate, for instance, to deal with the special characteristics associated to the layout of the plant and its resulting effects.

3. BRIEF DESCRIPTION OF THE FMEA TECHNIQUE

It is an inductive technique which enables the revision of all the components from a specific system in order to discover its failure modes and their respective possible effects.

All the process of analysis is oriented to the equipments, instead of process parameters, as HAZOP does.

The BS 5760 [3] Reliability of Systems, Equipment and Components, Part 5: 1991 Guide to Failure Modes, Effects and Criticality Analysis treats of the purposes, principles, proceedings and applications of FMEA, as well as its limitations and relation with another risk assessment techniques.

The purpose of the FMEA technique is to identify the failures which lead to unwanted events in the operation of the analyzed system and its goals include:

- identification of each failure mode, of the sequence of events respectively associated to them and the possible effects; and
- the classification of each failure mode according to relevant characteristics, including detection, tests and diagnosis capabilities, possibility of replacement, compensation resources and operational provisions.

The basic information of each one of the analyzed items is: name, function, identification, failure modes, failure causes, effects of the failure on the system, detection methods, compensation resources, severity of the effects and comments.

It is a very efficient methodology of analyzing the components which could be responsible for the failure of the whole (or a great part of the) analyzed system, it is not much recommended when a complex failure logic is necessary to describe the failure of the system.

Steps necessary to the execution of FMEA analysis:

1º) Define the system and its functional and operational requirements:

- include the primary and secondary functions, the expected performance, restrictions of the system and the explicit conditions which constitute a failure. The definition of the system must include each mode of operation definitions, as well as their duration;
- indicate all relevant environmental factors such as: temperature, humidity, radiation and pressure during the period of operation and installation halt; and
- consider failures which can cause the unfulfilment of the minimum requirements demanded by the regulation authority.

2º) Produce the system block diagram, in order to find the relationship among the components and possible interdependencies.

3º) Identify the failure modes, their causes and effects.

4º) List the detection failure methods and isolation and verify if other failure modes would furnish the same indication.

5º) Recognize design characteristics and operational provisions which could prevent or reduce the effects of each specific failure mode.

6º) Identify the specific combinations of multiple failures to be considered;

7º) Revise or repeat the FMEA analysis each time there is a change on the project.

4. THE EMERGENCY COOLING SYSTEM (ECS)

The Emergency Cooling System (ECS) was chosen to be analyzed because it is the main responsible for the mitigation of one of the worst accidents which can occur on a nuclear power plant, the loss of coolant accident.

According to TAKESHI [4], this system is compound by equipments destined to receive, stock and inject the coolant in the reactor, besides removing the residual heat of the reactor core in normal and abnormal conditions, or finally, during the loss of coolant accidents. A schematic diagram of this system is shown on Fig. 1 below:

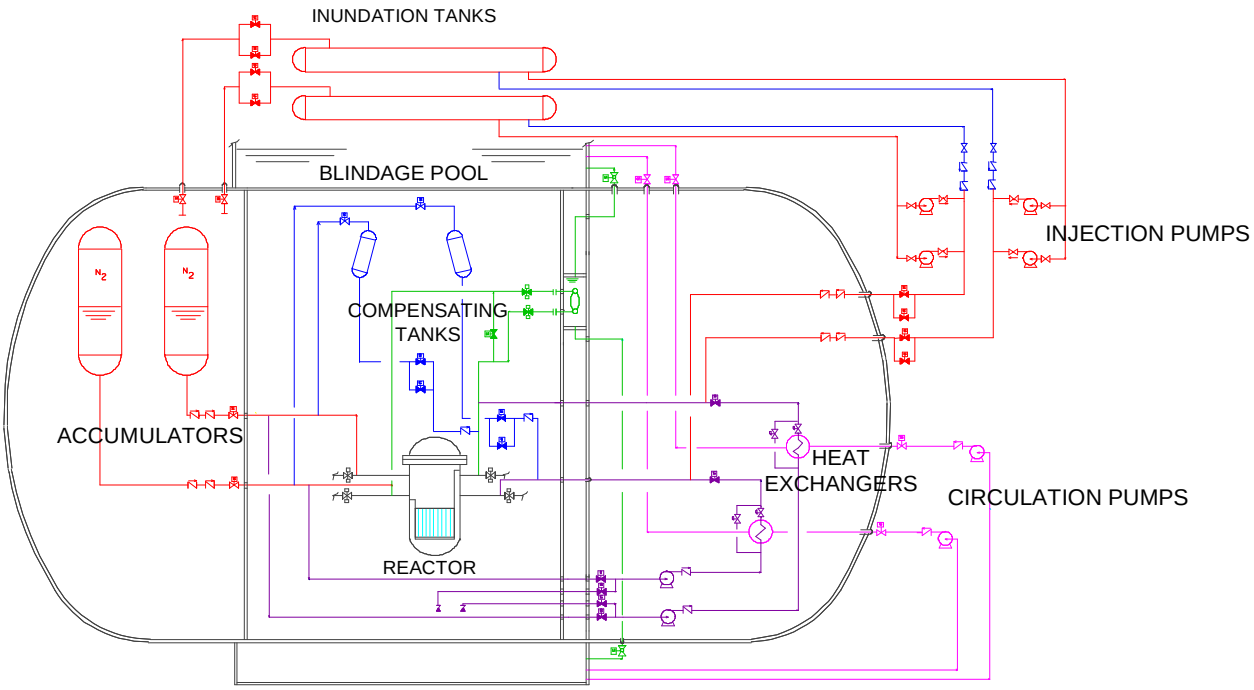

Figure 1. Emergency Cooling System (adapted from Takeshi, 2004).

The ECS can be divided into two subsystems:

a) Emergency Injection Subsystem (EIS), which is responsible for the water replacement on the primary circuit, when there is a leak of more than 1,0 m^3/h, or in such a manner to guarantee the integrity and geometry of the reactor core, through the inundation of the reactor vessel, in case of a loss of coolant accident. A schematic diagram of EIS is shown on Fig. 2:

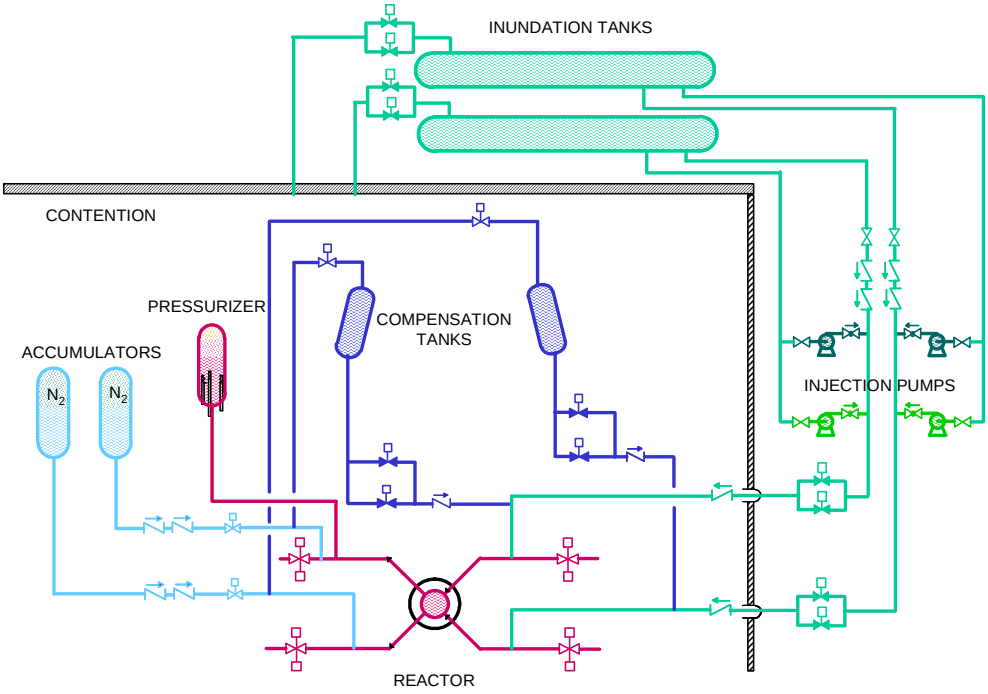

Figure 2. Emergency Injection Subsystem (adapted from Takeshi, 2004).

b) Residual Heat Remotion Subsystem (RHRS), which is responsible for the reactor cooling after its shutdown on the diverse conditions of operation of the plant, including in cases of loss of coolant accident. A schematic diagram of this subsystem is shown on Fig. 3:

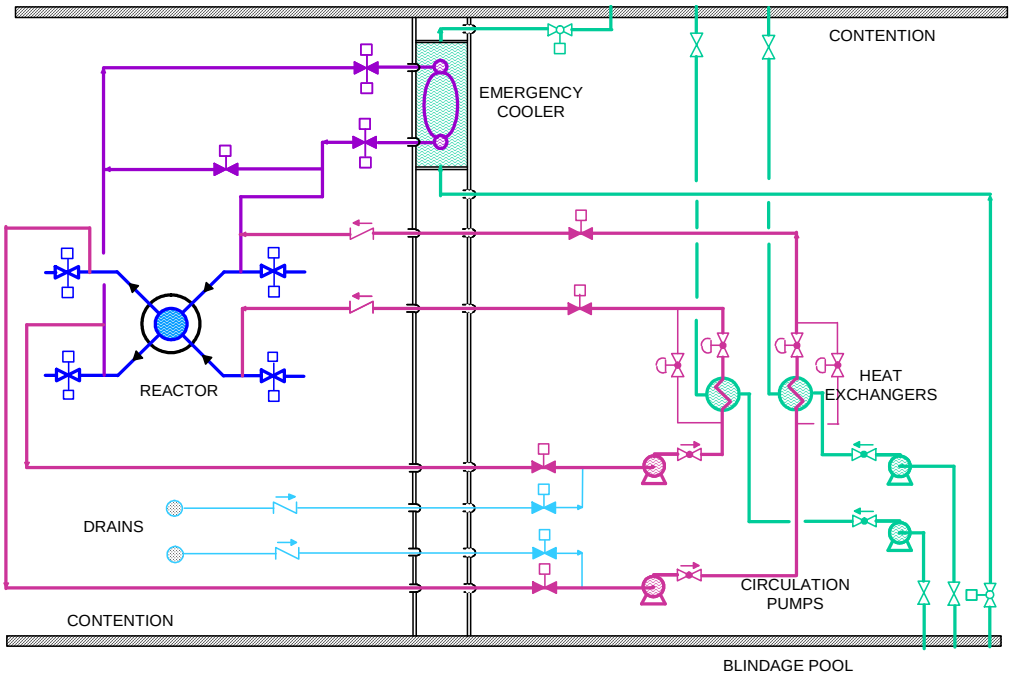

Figure 3. Residual Heat Remotion Subsystem (adapted from Takeshi, 2004).

The exact localization and the interconnection of the equipments of the ECS, as well as all the instrumentation and associated controls, are described in TAKESHI [5] and [6].

The Emergency Cooling System is designed to execute the following basic functions:

- cool the nuclear reactor, after its shutdown, providing the residual heat removal of the core;
- guarantee the integrity of the reactor core, in case of loss of coolant accident;
- assure the reactor cooling, as long as there is a need for it.

A loss of coolant accident is detected by the Plant Protection System (PPS), through the simultaneous occurrence of pressure fall on the primary circuit associated with the pressure and/or radioactivity rise inside the contention; another possibility is a water level fall inside the pressurizer, below the minimum value of reactor shutdown.

Once the accident has been detected, the PPS commands the reactor shutdown and the turn off the primary circulation pumps generating the Security Injection Signal (SIS) to start the operation of the ECS.

In case of high losses of coolant on the primary circuit, the ECS will provide (besides the actuation of the compensation tanks and the high pressure injection pumps) the passive injection, assured mainly by the two accumulators, which contribute for the cooling of the core, in the very beginning of the accident.

After the performance of the accumulators, when its level reaches the minimum, the obstruction valves are closed, automatically isolating and interrupting the injection through them.

At the same time, a signal is sent to allow the turning off of the high pressure injection pumps, allowing a higher outflow in the injection lines.

On this stage, the low pressure injection pumps start their operation, automatically commanded by the SIS when the pressure on the primary circuit reaches 14 bar, injecting borated water, which comes from the inundation tanks, in the reactor hot and cold legs.

In case of failure on the low pressure injection pumps, it is possible to inject borated water directly from the inundation tanks, through gravity force, using the discharge tabulation of the injection pumps.

Part of the injected water passes through the reactor core and leaves the Reactor Cooling System, by the leak on the pipe, remaining restrained at the bottom of the reactor compartment.

After the inundation tanks are empty, the RHRS can be commanded by PPS to collect the water, existing on the bottom of the reactor compartment, and return it to the reactor vessel, after it has been cooled on the heat exchangers.

5. AIM OF THE ANALYSIS

Due to the employment a redundance of four on the instrumentation of PPS, for the effects of this paper, the analysis of such components will not be executed.

In relation specifically to the human failures, due to the operation of the EIS be entirely remote and, in the case of RHRS, observing the fact that the critical performance consists on the repositioning the subsystem to the water recirculation mode, it is considered that this operation was successfully made and thus that kind of failure does not occur.

Another ways of human failure such as project mistakes, inadequacy on the specification of the components and/or errors on installation procedures and maintenance also will not be object of this study.

6. RESULTS

Through the analysis of the system, it can be observed that eventual failures on the compensation tanks, in the accumulators and in the components connected to them do not present major risk, due to their small stored volume of coolant and/or of their small time of actuation during a LOCA.

The unique exceptions are due to leaks on the valves which communicate these components to the reactor vessel, that in normal operation could cause the shutdown of the reactor due to pressure fall in the primary circuit, causing unforeseen maintenance periods and unexpected financial costs.

It can also be observed that one of the worst ways of failure on the ECS is the loss of inventory in one of the inundation tanks (due to leakage on the tank, on the pipe lines or in their components) but, even in this case, this kind of accident would not bring major problems because besides the existence of the redundant line, there is the RHRS, which is responsible for the recirculation of the water through the reactor core until the temperature for the safe SCRAM of the plant is reached.

Once this is known, it can be observed that a great leak on the valve, which enables the injection by gravity (or in one of the two retention valves in series to it) would have the same effect of the loss of na inundation tank, as seen above.

A great leakage on any of the items of the high and/or low pressure injection lines can also produce the same effect of the loss of an inundation tank.

A great leakage on the pipes also present the same effects that a failure of this type on the inundation tanks, with the exception that in some points of the line there are ways of isolation.

Continuing the analysis, next item is a parallel association between two valves, normally closed, which objective is to shut the contention, during the normal operation of the system, and allow the emergency an by gravity injection, in case of accident.

In this situation, they could also leak, causing the loss of inventory of one of the tanks with no possible compensating measures (because all the liquid injected in the contention, in case of accident, necessarily pass through one of these two valves).

The next item is a retention valve, which function is the same as the parallel association previously described and which, in case of leakage during an accident, could cause the loss of the coolant in one of the inundation tanks, with no compensating provisions.

Finally, on the emergency injection line, there are two valves in series associated in parallel with another set of identical valves disposed the same way, which objective is to shut the reactor compartment, during normal operation, and permit the emergency and by gravity injection, on accidental conditions.

In case of accident, the failure on the first valve can occur by leakage, allowing the liquid to exit the line and counting with no compensating resources on this circuit, which could occasion the loss of inventory in one of the tanks.

The second valve (a retention one), in normal operation, can fail by leakage, allowing the passage of the borated water outside of the line, causing loss of coolant on the primary circuit and consequently the reactor shutdown.

In case of accident, it could fail by leakage, causing a loss of coolant inside the reactor compartment, obliging the liquid derived from one of the tanks does not pass through the reactor core before it is flooded but, unless there is a simultaneous failure on the RHRS, the water will be cooled and circulated in the reactor core.

The other line, in parallel to this, presents the same failure modes and the same consequences described on the tree previous paragraphs.

Failures on the pressure equalization line (to enable the injection by gravity), does not present a major problem, once the injection through the high and low pressure injection pumps is sufficient to flood the reactor vessel and in case of failure of one circuit, there is another in parallel (besides the RHRS).

On the other hand, failures on the RHRS will only present major gravity since the EIS has previously failed.

If the reactor core is, at least, partially flooded its integrity is preserved, not depending on the performance of RHRS.

Then, it can be deducted that failures on the RHRS have less severity than those on the EIS and among the most important ones can be mentioned: the clogging of the drains or the failure in two main items (one in each line), for instance a heat exchanger and a circulation pump, a leakage or a unwanted closure of two valves, which are on the critical path, and so on.

For additional information, the table containing all data and results obtained, through the appliance of the FMEA technique, can be found in [7].

7. CONCLUSIONS

Through this analysis, it can be observed that the ECS is intrinsically safe, once as long as there is an event capable of preventing the performance of one line of the ECS (a very rare event, as shown in OLIVEIRA ET AL. [8]), there is possibility of using the other line and also there is the RHRS.

Some recommendations for improvements on the system are:

- think about redundant lines with different project philosophies;
- separate the two inundation tanks (physically);
- connect the lines and install valves at the exit of the inundation tanks;
- utilize redundant components of a different nature from that used on the main line;
- install a leakage detection system in all extension of the lines; and
- realize adequate maintenance and regular tests and inspections.

REFERENCES

[1] LEES, F. P. *Loss prevention in the process industries: hazard identification, assessment and control***.** 2.ed. Oxford, R.U..: Butterworth-Heinemann, 1996.

[2] KUMAMOTO, H.; HENLEY, E.J. *Probabilistic risk assessment and management for engineers and scientists*. 2.ed. Nova York, N.Y.: IEEE Press, 1996.

[3] BRITISH STANDARDS INSTITUTION. *Reliability of Systems, Equipment and Components, BS 5760*, BSI, Londres, R.U., 1991.

[4] TAKESHI, R.V.R. *Descrição do sistema de resfriamento de emergência*. São Paulo: CTMSP, 2004a.

[5] TAKESHI, R.V.R. *Sistema de resfriamento de emergência – fluxograma de engenharia*. São Paulo: CTMSP, 2004b.

[6] TAKESHI, R.V.R. *Sistema de resfriamento de emergência – fluxograma de processo* São Paulo: CTMSP, 2004c.

[7] CONCEIÇÃO JR., O. *Aplicação da técnica de análise de modos de falha e efeitos ao sistema de resfriamento de emergência de uma instalação nuclear experimental* São Paulo: IPEN, 2009

[8] OLIVEIRA, P.S.P.; JAQUES SAUER, M.E.L.; VIEIRA NETO, A.S.. *Análise de confiabilidade do sistema de resfriamento de emergência da INAP* São Paulo: IPEN, 2000.