IAEA-CN-82/09

PERFORMANCE INDICATORS AT EMBALSE NPP: PSA & SAFETY SYSTEM INDICATORS BASED ON PSA MODELS

FORNERO, D. A.
Nucleoelétrica Argentina S.A.
Los Cercis 243 – B
5856 Embalse – Córdoba, Argentina
Fax: +543514244577; Email: dfornero@redlago.com.ar / nasa1r3@itc.com.ar

Abstract

Several indicators have been implemented at Embalse NPP. The objective was selecting some representative parameters to evaluate the performance of both the plant and the personnel activities, important for safety. A first set of indicators was defined in accordance with plant technical staff criteria. A complementary set of them was later added based on WANO guidance.

This report presents the set of indicators used at Embalse NPP, centering the description to those related to safety systems performance indicators (SSPI). Some considerations are done about the calculation methods, the need for aligning and updating their values following Embalse Probabilistic Safety Assessment (PSA) development and some pros and cons of using the PSA model for getting systems indicators.

Owing to the fact that PSA ownership by utilities is also a subject of the meeting, some characteristics of the organization of the PSA Project are described at the beginning of the report. At Embalse NPP a Level 1 PSA has been developed under the responsibility of the own plant and with an important contribution from IAEA. PSA was developed at the site, conducting this to a Study strongly interactive with the station staff.

1. PSA AT EMBALSE NPP

1.1. Characteristics — plant ownership

Embalse NPP is a PHWR 650 MWe station, CANDU design (CANadian Deuterium Uranium) that started commercial operation in 1984.

Particular probabilistic studies had been developed for the plant since the beginning of the operation, such as relatively simplified fault trees and the analysis of some event sequences for a limited group of initiating events, with a probabilistic approach.

A comprehensive and systematic Level 1 PSA began to be developed at Embalse on the ends of 1997. Developing a formal PSA at Embalse had been an objective defined some years before. However, its beginning was delayed because it was a priority to develop first the same study for Atucha I, that is the other NPP in operation in Argentina. It is also a PHWR station (Siemens-KWU) and its design is older than Embalse's. So, in the early 1990s it was thought convenient to develop detailed PSA studies for it first. After a Level 1 PSA for internal events were completed for Atucha, PSA started at Embalse in a systematic way.

A very important characteristic of this PSA is that the own station was responsible of the Project from the beginning and the Study was developed essentially at the plant.

The experience showed that this is a very important issue to reflect the actual Operation of the plant. The day to day information supplied for operators, maintenance and technical support personnel to PSA group, would be impossible to be found in the same way in the best formal documentation that

someone can have available in any place. Despite the fact that PSA was mainly developed at the plant, an heterogeneous group of people participated in the Project conducting to have at its disposal a varied kind of previous experiences. So it is worth to be mentioned that among the participants in the Project there were plant specialists in different fields and also people with experience in Atucha PSA, from both the own plant and the Nuclear Safety Head Office, specialists from the Atomic Energy National Commission and from the Regulatory Body. Also, technical visits from the designer (AECL) and from IAEA experts were carried out in order to support PSA team. In this way, IAEA provided two 'one-week' type expert missions.

Foreign specialists from Romanian and Cuban PSA groups, with previous experience in their respective PSA projects, develop different activities for Embalse PSA during relatively large periods. This was an important contribution to the Project and also allowed them to get a good knowledge on an operating plant. IAEA support was fundamental in this point.

Although PSA general applications is not the main objective of this paper, it is anyway considered important to mention that PSA results are starting to be used in different fields. As examples they can be indicated the following cases:

a) PSA Human Reliability analyst work in conjunction with people who develop Emergency Operating Procedures (EOP) in order to optimize then and make compatible aspects that sometimes can go in an opposite way, as the following:
   - The 'needs' of PSA analysts of assuring that human actions (HA) included in the event sequences are contemplated in EOPs.
   - The need of Operation groups that the information included in EOPs is not complicated enough due to the adding of excessive information.

b) Plant modifications are evaluated with PSA model, but at the present only at a system level impact. Impact at a whole model level will be done in the near future.

c) Plant configuration analysis are expected to be done. At present, system configurations are included in some way through safety systems performance indicators. These indicators had been developed up to now using simplified systems fault trees but were gradually replaced by detailed fault trees developed for PSA Project.

Performance Indicators at Embalse NPP are described next in a general way. Particular attention is paid to Safety Systems Performance Indicators and their relationship with PSA models.

2. SAFETY INDICATORS AT EMBALSE NPP

Next group of indicators had been defined in a given moment at Embalse NPP in order to analyse some important issues related to plant operation performance:

Fuel Burning	Annual Unavailability of Emergency Core Cooling System
Fuel Failure Rate in the last 12 months	Annual Unavailability of AC Power Stand-by Diesel Generators
Number of Work Orders accumulated and 'Ages'	Annual Unavailability of Containment Dousing System
Number of Modifications to Prev. Mainten. program	Annual Unavailability of Containment Isolation Valves
Number of Modifications to Routine Tests procedures	Annual Unavailab. of Reactor Shutdown System 1 (shutoff rods)
Number of Work Orders related to design changes with pending documentation updating	Annual Unavailability of Reactor Shutdown System # 2 (Liquid poison injection)
Accomplishment of Preventive Maintenance program	Accomplishment of the Equipment Rotation program
Accomplishment of the Routine Tests program (in order to report if any one is pending)	Number of Work Orders accumulated requiring plant in shutdown state for its execution
Number of Audits / Surveillance	Number of Corrective Actions
Training Hours: Executed vs. Programmed	Absenteeism (Personnel Availability)

This set of indicators implemented at Embalse NPP was completed with those defined by WANO, i.e.:

Fuel reliability – Steady State Reactor Coolant Activity	Safety Systems Performance (for HPECI, ABF and EACP).
Thermal Performance	Generation Data (Unit Capability, Unplanned Automatic Scrams)
Radiation Protection (Collective Radiation Exposure, Volume of Solid Radioactive Waste)	Chemical (S/G Blowdown Sodium, Chloride & Sulfate Concentration, etc.)
Personnel Safety (Industrial Safety Accident Rate)	

2.1. Safety systems indicators

2.1.1. Background

At Embalse NPP there are four 'Special Safety Systems' defined: the two reactor shutdown systems, the emergency core cooling system and the containment safety functions. During the plant commissioning stage, the designer left the concept of calculating the so-called 'Annual Actual Past Unavailability' for these systems in order to verify that each individual value was kept lower than 10^{-3} year/year.

Some relevant aspects of the calculation methodology for these values were the following:

- If a system had kept at least one redundancy path available during one year, the Actual Past Unavailability for the system was assumed as 0 (zero), because it was considered that system never had lost its minimal capability to operate properly in case of being demanded.
- If the system was completely unavailable for any reason, for a given period (for instance 8 hours) the system unavailability was defined as the number of hours unavailable divided the total number of hours that the system was required in the year (for instance 8000 hs.). Using as an example the values indicated in brackets, Actual Past Unavailability would be 10^{-3}.

In case that one redundant train of a system had been available during all the period, this method did not allow to distinguish — because it was indistinct for the indicator result — if other redundant paths were 100 % available or it had experienced any problems instead. This has been considered at Embalse NPP as a rigid methodology with the shortcoming of potential masking of important failures and unavailabilities.

2.1.2. WANO Safety Systems Performance Indicators

WANO Guideline establishes that Safety Performance Indicators are calculated for three systems (HPECI, EACP, ABF). According to the definition the way to obtain them is dividing the hours that any component of the system is unavailable by total time in the period considered. Redundancies are simply taken into account dividing the result by the number of trains. This has the advantage that the value is easy to be calculated and understood but the disadvantage that they do not give a good representation of systems characteristics, mainly from the point of view of the redundancies.

2.1.3. Safety Systems Performance Indicators (SSPI) defined at Embalse NPP

In order to solve the disadvantages of not taking into account the redundancies in a proper way, a different way to develop these indicators was implemented at Embalse. This method is a hybrid one and it mixes probabilistic approaches with actual past facts. Although this is not strictly correct from the point of view of the methodology, it has the important advantage that every cause of unavailability of the different components is reflected in the result. These indicators, generically called 'X System Unavailability during the year Y' are obtained, in the following way:

- Taking a simplified but normal fault tree of the system, a basic system unreliability (Qs) is calculated taking into account the normal parameters considered in a fault tree, i.e. system configuration, failure rates, tests frequencies, etc. If no problem occurred in the system during the considered year, it is defined that the *system annual past unavailability* is Qs (not '0'). This intends to indicate that system configuration was kept during the whole year and the probability

of not being available, in case it had been demanded, was the calculated through the 'normal' fault tree.

- When any component was effectively unavailable for any reason during a given period Ti of the year, value '1' is assigned to its unavailability and a new degraded system unreliability value, Qdi, is calculated for this system configuration. This is repeated the necessary number of times, according to the actual unavailabilities observed.
- In order to obtain the annual unavailability Qy of the system the contributions are weighted with the time period Ti that every configuration actually occurred:

  Qy = SUM over i {Qdi * Ti / 1 year} + Qs * Tr / 1 year

  where Tr is the remaining time in the year (1 year - the sum over i of all Ti.)

This approach has the double advantage of:

- reflecting any kind of component unavailability in the system;
- being essentially conservative: components that actually underwent any unavailability are properly included, while the rest of components, with non observed unavailability during the time period, are nevertheless affected by their normal failure probability.

The present system availability can be measured both *in absolute*, through this definition of Qy, and *in relative* by the ratio (Qy-Qs)/ Qs, which provides a figure of the system degradation in a proportional way. No arbitrary target or reference value is necessary in this approach.

What could be objected, namely the validity of the simple fault tree model, is a point treated later on.

Analysing the trend of Qy and the causes of contributions to systems unavailability, actions are taken endeavouring to minimize these contributions. These indicators were extended also to other systems different from the 'four special safety systems'.

2.1.4. Data collection for obtaining safety systems performance indicators

The data required to obtain the safety systems performance indicators are mainly, the failures recorded in a given period and the unavailabilities due to maintenance. Sources of information are:

a) Test procedures records

In order to get such kind of data, operations test procedures records are daily checked by technical support people. Failures detected for a given system are classified in five types depending on whether they lead to: 1) system becomes completely unavailable, 2) a decreasing in the efficacy of the system, 3) a redundancy is lost, 4) no implication in system availability (except due to the related maintenance) because failure is incipient and 5) evolution to the safe way but affecting normal operation of the plant. When a failure detected in a test is one of the type included in any one of the first three groups, affecting a component availability, the weight of the component in the system is analysed through the corresponding fault tree. Time with the failure present is assumed as half the time between the last successful test and the test that revealed the failure.

b) Work orders

If any doubt is kept about whether a given failure is a catastrophic one or not for a component, work orders open to repair the failure are analysed to pick up more data. If information found there is not clear enough, plant maintenance specialists are consulted. For instance, if an important oil leakage is detected during a test for a stand-by pump, mechanical specialists of the plant are consulted before classifying the failure. They give their judgement about whether or not the pump would be available to work for 24 hours in case of an actual demand (24 hs is the reference components mission time for PSA and safety systems performance analysis).

c) Operation logs

Shift supervisor and operator logs are consulted on a daily basis in order to get information about equipment status, maintenance activities and times in which equipment become unavailable and

re-established after a given maintenance. Maintenance times are counted to obtain safety systems performance indicators if they lead to a decreasing in system reliability.

2.2. PSA models and Safety Systems Indicators

Fault trees developed for Embalse NPP PSA are more detailed than the original and simplified models used for obtaining the indicators. However, some cares have to be taken before replacing the 'old' fault trees by the 'new' ones; mainly when the intention is to compare trends.

Among the PSA results it is frequently observed that two issues appear as important as large contributors to systems unavailabilities:

- Common Cause Failures (CCF)
- Human Actions (HA)

PSA detailed models showed that CCF are important contributors in fault trees results. This is frequent in systems with similar redundant trains. So, if CCF are included in the calculation of the indicators they can largely override and mask contributions to the final unavailability due to particular components. As an example it can be mentioned that at Embalse NPP, for the safety function 'Primary System Loops Isolation after LOCA' the failure probability of the heading appear mul $Q_S = 3.2$ E-3 factor 3 when CCF between redundant valves is included.

Another point to be carefully analysed is the corresponding to Human Actions (HAs). Although the four special safety systems are essentially automatic, HAs associated to some safety related system performance can have an important impact on the results. Under a certain point of view, it may be necessary to consider the indicators without them in order to avoid to loss quantitatively the specific contribution due to individual components.

2.2.1. Indicator 'Increase of Unavailability (F_{IND})'

Simplified fault trees were used to get the indicators up to 1998. More detailed fault trees began to be used since that date and in some systems boundaries were changed. That is why sometimes is not possible to compare the results of different years because the base to calculate are different.

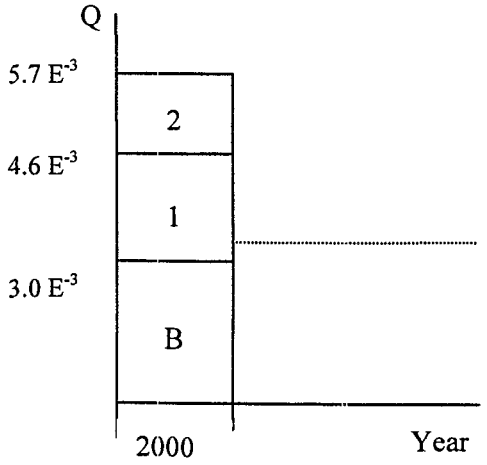
In order to compare trends it was thought useful to define a factor called *Increase of Unavailability (F_{IND})*. This factor represents the increase of the annual unavailability of the system referred to the basic value taken as reference (Qs). $F_{IND} = (Q_y - Q_s) / Q_s$.

2.2.2. Examples

Two examples based on hypothetical configurations postulated are presented to show:

a) the calculation steps to get the annual unavailability for a system in a year, taking into consideration a couple of contributions due to a failure and a maintenance.
b) values of system unavailability as well as the factor F_{IND} for different years resulting from calculate them with the old simplified models, the new models without HA and CCF and the new models with HA and CCF.

Example a) This example shows contributions of components unavailabilities in the whole system unavailability for a given system during a year. It is calculated assuming that two degraded system configurations were presented during the year: 1) One MV fails during a monthly test and 2) One pump under a large maintenance.



1. Contribution of the configuration 1 (CC1)

Degraded condition:	One MV fails during a monthly test
Degraded System Unavailability without unavailability)	$4 * 10^{-2}$. Obtained from the modified fault tree the MV (assigning '1' to MV
Failure duration:	15 days (dormant failure during 15 days assumed)
CC1 = $4 * 10^{-2} * 15$ days / 365 days	$1.6 * 10^{-3}$

2. Contribution of the configuration 2 (CC2)

Degraded condition:	*One pump in a large maintenance.*
Degraded System *Unavailability without unavailability)*	*$8 * 10^{-2}$. Obtained from the modified fault tree the Pump. (assigning '1' to Pump*
Failure duration:	5 days
CC1 = $8 * 10^{-2} * 5$ days / 365 days	$1.1 * 10^{-3}$

B. Contribution of the basic system unavailability (CCB)

Condition:	Normal configuration of the system
Basic system unavailability (Qs): from components.	$3.2 * 10^{-3}$. Assumed in this example and obtained the 'normal' fault tree that includes all the
Duration of this configuration:	345 days (whole year less time any component unavailable).
CCB = $3.2*10^{-3} * 345$ days/365 days	$3 * 10^{-3}$

Annual System Unavailability	Q_y = CC1 + CC2 + CCB =	**$5.7 * 10^{-3}$**
Increase of Unavailability Factor:	F_{IND} = (Qyear – Qs)/Qs =	**0.78**

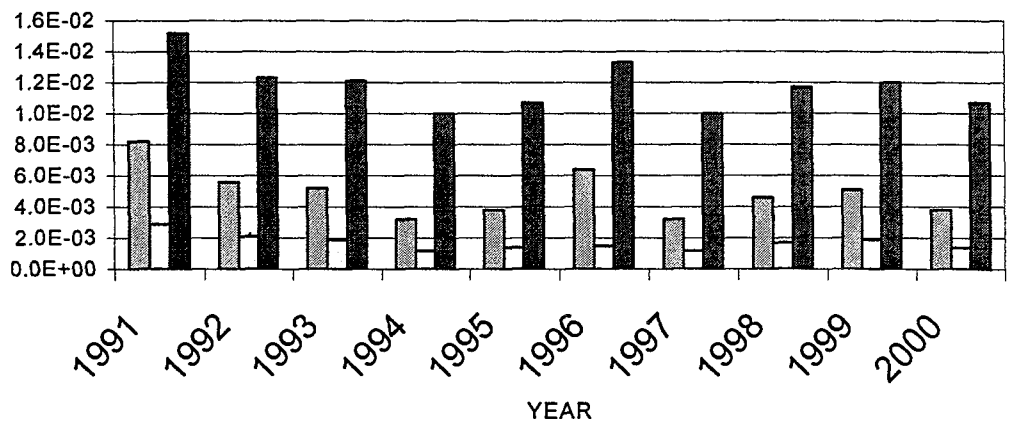
Example b) This example shows the differences in unavailability and increase of unavailability factor results by obtaining them from different basic fault trees for ECCS and assuming hypothetical failures.

1: Obtained from 'old' simplified fault trees that consider High, Medium and Low Pressure stages (HP, MP, LP) of the system but not including Human Actions (HA) nor Common Cause Failures (CCF).

2: Obtained from detailed fault trees from PSA for HP and MP stages taking away CCF. This fault tree without LP stage was chosen because it does not include HA that mask the rest of the contributions.

3: Obtained from detailed fault trees from PSA including all the stages and HA and CCF.

FIG. 1. COMPARISON BETWEEN SYSTEM ANNUAL UNAVAILABILITIES OBTAINED BY DIFFERENT WAYS

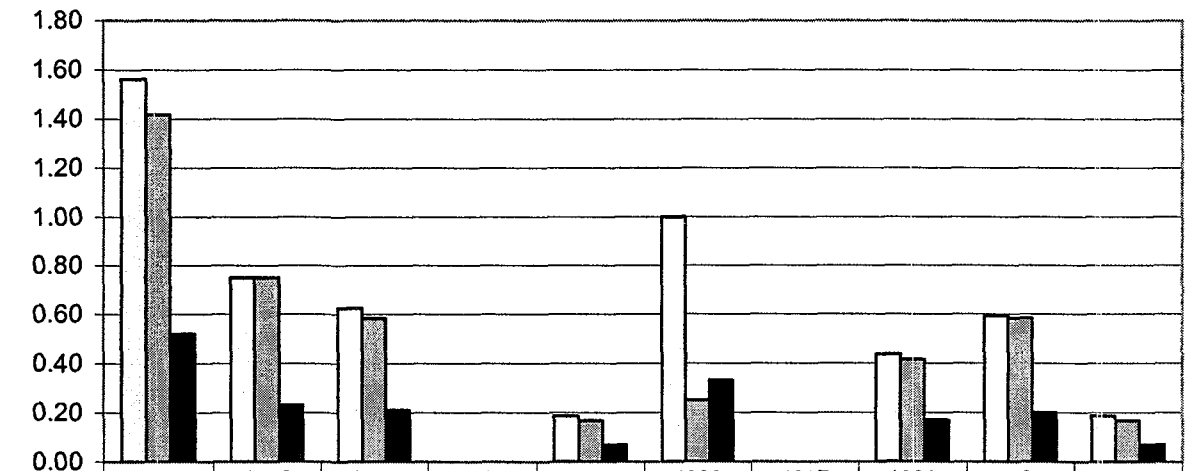


It can be seen that Qy from 1 and 2 are quite different. This occurs due to the fact that the system boundaries taken as reference are different. For case 1 the HP, MP and LP stages have been taken while for case 2 LP was not considered. However as can be seen in Figure 2 the proportional factor F_{IND} from 1 and 2 are quite similar. This shows the advantage of this factor in order to compare trends.

For year 96 F_{IND} 1 and 2 are well different because of a failure was assumed in a LP Stage and it cannot be distinguished using model 2 because LP is not included in the fault tree selected as reference.

For case 3 even F_{IND} are well different and that is due to the fact that HA and CCF have been included in the basic fault tree. So when a failure or a maintenance occur their contribution are usually masked for the large contribution of HA and CCF being the indicator less sensible to the degraded configurations that took place during the year.

FIG. 2. COMPARISON BETWEEN FIND FACTORS OBTAINED BY DIFFERENT WAYS



	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000
FIND1	1.56	0.75	0.63	0.00	0.19	1.00	0.00	0.44	0.59	0.19
FIND2	1.42	0.75	0.58	0.00	0.17	0.25	0.00	0.42	0.58	0.17
FIND3	0.52	0.23	0.21	0.00	0.07	0.33	0.00	0.17	0.20	0.07

YEAR

3. CONCLUSIONS

A set of indicators have been developed at Embalse NPP in order to evaluate plant and personnel performance. For safety systems, indicators measure system past availability. A method was developed to calculate them and it has the advantage that allows to distinguish differences in the performance of a system, although when in a strict way it was available the whole time. This method takes into account the loss of redundancies and the impact of the components unavailabilities in the system from a probabilistic point of view.

Originally this method was developed using simplified fault trees. Afterwards a comprehensive Level 1 PSA, with the main characteristic of being strongly interactive with plant operational staff, has been carried out in last years. As a product of such a PSA Study new and more complex fault trees have been obtained. Detailed fault trees developed in the framework of Level 1 PSA are in principle fully applicable to continue getting safety performance indicators in a similar way.

In order to compare trends a proportional factor was defined and it indicates that the relationship of system annual unavailability in relation to basic value are kept similar using simplified or detailed fault trees. However, it is not the same if CCF and HA are included in the models to get the Safety Systems Indicators, because their high relative weights usually mask particular component unavailabilities contributions.