Comparison exercise of probabilistic precursor analysis

V. Fauchille, S. Babst***

* IRSN BP N°17, 92262 Fontenay aux Roses Cedex, France
** GRS, Kurfürstendamm 200, 10719 Berlin, Germany

Abstract:
From 2000 up to 2003, a comparison exercise concerning accident precursor programs was performed by IRSN, GRS, and NUPEC (Japan). The objective of this exercise was to compare the methodologies used to quantify conditional core damage probability related to incidents which can be considered as accident precursors. This exercise provided interesting results concerning the interpretation of such events. Generally, the participants identified similar scenarios of potential degradation. However, for several dominant sequences, differences in the results were noticed. The differences can be attributed to variations in the plant design, the strategy of management and in the methodological approach. For many reasons, comparison of human reliability analysis was difficult and perhaps another exercise in the future could provide more information about this subject. On the other hand, interesting outcomes have been obtained from the quantification of both common cause failures and potential common cause failures.

INTRODUCTION

An official program for probabilistic evaluation of accident sequence precursors exists in a number of countries which operate nuclear reactors, but the comparison of numerical results of precursor analyses, meaning the calculated Conditional Core Damage Probabilities (CCDP), is difficult due to several differences in the methodological approach which are not clearly identified.
From 2000 up to 2003, a comparison exercise concerning accident precursor programs was performed by IRSN, GRS and NUPEC (Japan). The objectives of this exercise were:
- to compare in detail the different methodologies used to quantify incidents which can be considered as accident precursors,
- to understand the methodological approach and the practice of precursor analysis of the other participants,
- to define what could be learnt for future precursor analysis.

The conditions of the exercise were as follows: the same incidents were analyzed and quantified by each participating country; the chosen incidents were derived from real events but were adapted for the exercise; each participant country received a summary of the facts and interpreted them either on their own power stations (IRSN, NUPEC) with their own procedures or on a fictional plant defined on the basis of the event description (GRS).
It has to be noted that this exercise is not a real benchmark of the treatment of an identical problem with identical boundary conditions. The aim was to compare some similar problems in order to identify important methodological issues. For several reasons due to specific practices of each participant, the numerical results have to be considered only as indications.
In the framework of the exercise three analyses of incidents were compared:
- case 1: leak on valves of both trains of the residual heat removal system (RHRS) in cold shut-down state,
- case 2: unavailability of the safety injection system due to a human error,

- case 3: potential common cause failure affecting safety switchboards at full power operation.

The three cases are presented in the following section. General outcomes and conclusions from the exercise are presented at the end of this paper. The comparison exercise is described in detail in report /1/.

CASE 1: LEAK ON VALVES OF BOTH TRAINS OF THE RHRS

The unit was in the cold shut-down state (pressure: 27 b, temperature: 80°C). Both trains of the Residual Heat Removal System (RHRS) were in operation. The operating team noticed numerous boron makeups to the primary system. They took an operating procedure to locate the leak which was discovered on the RHRS train A, on a heat exchanger bypass valve. The operating team isolated RHRS train A and stopped the leak. Chemical and Volume Control System (CVCS) could always compensate the leak. Maximum observed leak rate: 4800 l/h. The reactor was cooled to mid-loop operational state (atmospheric pressure, temperature: 36 °C) and it took 3.5 days to repair the valve.
The day after the requalification and the reconnection of RHRS train A, a small leak (800 l/h) appeared on the symmetric valve (located on the heat exchanger bypass) on train B. Train B of the RHRS was isolated. Two days later, both trains of the RHRS were available.

Interpretation of the event
All participants considered a potential Common Cause Failure (CCF) on the symmetric valves of the RHRS, and assumed that two ways of degradation had to be considered: the loss of the coolant inventory and the loss of the heat removal.

IRSN analysis:
IRSN analyzed the event as a common cause failure that could occur both in the cold shut-down state and during mid-loop operation. The core damage probability was calculated in proportion of the duration of each plant operational state. A maximum 0.41'' LOCA as been assumed on each train. IRSN used International Common cause failure Data Exchange (ICDE) methodology to quantify CCF. An "Impact Vector" of 0.25 was evaluated. It includes the "Component Impairment vector" (evaluated to 0.5) which reflects the state of degradation of the components (with 800 l/h, RHRS train B can fulfill its function but the leakage could increase), the "Time factor" (evaluated to 0.5) which is a measure of the simultaneity of the multiple failures (the second leakage occurred after the repair of the first one, but only 5 days after the first failure), and the "shared cause factor" (evaluated to 1) which indicates whether the multiple failures result from the same cause or different causes (IRSN assumed that the phenomenon which appeared on the valves of the redundant trains was similar). In case of LOCA on both trains of the RHRS, the strategy of management is as follows: operating procedure asks to keep one RHRS train in operation with the leak compensated by CVCS. In the cold shut-down state, the dominant sequence ($1.9\ 10^{-5}$) is the loss of all possibilities of makeup (low and medium safety injection pumps). During mid-loop operation, the dominant sequence is the loss of RHR during repair of one train ($1.8\ 10^{-6}$). The repair of train A and train B was taken into account, thus a 5.5 days duration was considered.

GRS analysis:
GRS situated the event during mid-loop operation. RHRS train A was unavailable for repair (3.5 days) and a potential leak could occur on RHRS train B while the train A was under repair. To calculate the probability of common cause failure, GRS applied ICDE methodology. The degree of damage of the heat exchanger bypass valve on train B was judged "degraded" (the component was capable of performing the major portion of the safety function but part of it was degraded). Therefore an external leakage (probability of 0.5) was assumed. Based on a fault tree calculation, the contribution of the loss of water inventory

was considered as negligible. The failure the RHR train B (the loss of the pumps) gives the major contribution (3.0 10^{-3}).

NUPEC analysis:
NUPEC analyzed the event in the cold shut-down state, which corresponds to the beginning of the first leak. To calculate the common cause failure probability, NUPEC applied NRC methodology /2/ named "Impact Vector Method". In this method three factors characterize a common cause failure: the "Component State Factor (p)" which represents the degree of degradation according to the observed failure, the Timing Factor (q) represents the time delay between failure of components and the Shared Cause Factor (c) indicates whether or not the multiple failures result from the same cause. Since the leak from the valve on train B was lower than 2300 l/h, defined in Tech-Spec for Japanese PWRs, NUPEC considered that the valve on train B was "slightly degraded" and calculated a value of 0.1 with a Timing Factor and Shared Cause Factor of 1,0. The strategy of management consists in isolating both RHRS trains, cooling via steam generators, and in case of failure of secondary cooling, cooling by forced feed and bleed. The failure of these defense lines, combined with the CCF probability, corresponds to a conditional core damage probability of 4.6 10^{-6}.

Outcomes from case 1:
All the participants considered a potential CCF and quantified it using similar methodologies: IRSN and GRS used ICDE methodology and NUPEC applied NUREG methodology. However, they had slightly different interpretations, especially concerning the estimation of the degree of degradation of the valve on train B. Concerning the potential consequences, all the participants also agreed to consider two ways of degradation: the loss of the cooling inventory and the loss of the heat removal. The differences in the results come from two sides. The first one is the plant operational state where the event is situated. GRS analyzed the situation during mid-loop operation; NUPEC situated it in the cold shutdown state. IRSN studied both situations. The second one comes from different strategy of management. In cold shutdown, IRSN considers that RHRS train A will be isolated and train B will remain in operation with a leak compensated by CVCS. NUPEC considers that both trains will be isolated and steam generators will cool the reactor. In case of failure, the defense line is feed and bleed. Considering the event during mid-loop operation, IRSN and GRS both consider that train A is isolated for repair work and the leak on train B is compensated. In case of total loss of RHRS, IRSN considers a cooling possibility by water makeup and boiling, while GRS, according to their methodology principle, does not take this accident management action into account. In case 1, although the main degradation ways are similar, the specific practices of the participants explain the differences in numerical results.

CASE 2: UNAVAILABILITY OF THE SAFETY INJECTION SYSTEM DUE TO A HUMAN ERROR

The operators were on the way to cool down the reactor for refueling. The reactor was in intermediate shutdown state (pressure = 27 bar ; temperature = 170°C), cooled by steam generators. RHRS was not yet in operation. In this situation, the interlocking for protection against spurious safety injection was set too early and LPSI pumps were disconnected during the night. In the morning, during his turn-over inspection, the shift supervisor detected the error and the pumps were reconnected. The LPSI pumps were unavailable for 7 hours. During the same period, the boron tank had been isolated erroneously for 1 hour, leading to HPSI pumps unavailability. During this phase, if a LOCA had occurred, safety injection pumps would have started and without shutoff they would have been destructed.

Interpretation of the event:
All participants divided the incident in two phases, phase 1: unavailability of LPSI for 6 hours, phase 2: unavailability of HPSI and LPSI for 1 hour. For each phase the initiating events leading to sequences affected by LPSI and HPSI unavailability were analyzed. A recovery of the human error was introduced where appropriate.

IRSN analysis:
The worse situation is the unavailability of high pressure safety injection pumps. It is necessary that the operators detect it before starting the pumps, otherwise they would be destructed. In this situation, pumps recovery is considered as impossible. On another hand, low pressure safety injection unavailability can be detected: in this operational state, injection pumps are started by an operator in the main control room. Pumps failure to start is indicated by alarms and procedures ask for checking safety injection flow. Probability of human error recovery depends on initiators and accident kinetic. Even if pre-accident human error is corrected, other human errors modeled during accident management still remain. In the model, probability had been calculated taking into account duration before core melting. Durations are shortened by 20 minutes (time necessary to put an end to local lockout). In case of loss of auxiliary feedwater, operators have time before putting into operation feed and bleed, so the recovery of the auxiliary feedwater is modeled.

TABLE 1 – IRSN RESULTS

	Frequency /hour	LPSI unavailable for 6 hours	LPSI and HPSI unavailable for 1 hour
small LOCA	$1.8\ 10^{-7}$	$3.2\ 10^{-8}$	$1.8\ 10^{-7}$
Loss of auxiliary feedwater	$6.0\ 10^{-7}$	$1.1\ 10^{-7}$	$9.3\ 10^{-8}$
Total result		$1.4\ 10^{-7}$	$2.7\ 10^{-7}$

GRS analysis:
GRS considered small LOCA (diameter: 2-12 cm^2 and 12-25 cm^2). In case of unavailability of LPSI pumps and small LOCA 2-12 cm^2, GRS considered a recovery action by operators. In ASEP – Methodology /4/ used by GRS for the quantification, nominal HRA for post-accident tasks is a combination of diagnosis error ($2.7\ 10^{-3}$) and error of commission ($8\ 10^{-2}$). According to most German PSAs, no accident management measures was taken into account for the quantification. Therefore, conditional beyond design probabilities were estimated by GRS. In case 2, this fact has no significant impact on the results.

TABLE 2 – GRS RESULTS

	Frequency /hour	LPSI unavailable for 6 hours	LPSI and HPSI unavailable for 1 hour
small LOCA 12-25 cm^2	$1.6\ 10^{-8}$	$9.8\ 10^{-8}$	$1.6\ 10^{-8}$
small LOCA 2-12 cm^2	$3.2\ 10^{-7}$	$1.6\ 10^{-7}$	$3.2\ 10^{-7}$
Total result		$2.6\ 10^{-7}$	$3.4\ 10^{-7}$

NUPEC analysis:
NUPEC analyzed 7 of 13 initiators of the Japanese PSA model. The remaining 6 initiators such as large and intermediate LOCA were not considered in this study since RCS pressure was much lower than in full power operation. Among the 7 initiators, the most important CCDPs were obtained for small LOCA and very small LOCA:
In phase 2, NUPEC expected the recovery of one of CHSIPs (Charging/SI Pumps) if its power supply would be turned off before the event in accordance with Japanese T-Spec. For the other two CHSIPs, the time of 10 minutes were considered too short to recover them based on THERP methodology. The outage of LPSI pumps, serving as RHR pumps, is not

allowed in Japanese PWRs. NUPEC considered the erroneous turning off of the switches for power supply to LPSI pumps in the main control room. This would cause the unavailability of LPSI pumps and NUPEC took credit for the recovery of these pumps.

TABLE 3 – NUPEC RESULTS

	Frequency /hour	LPSI unavailable for 6 hours	LPSI and HPSI unavailable for 1 hour
Very Small LOCA	$3,2\ 10^{-7}$	$2,4\ 10^{-10}$	$2,2\ 10^{-10}$
Small LOCA	$1,7\ 10^{-8}$	$3,7\ 10^{-10}$	$8,0\ 10^{-11}$
Loss of CCWS	$8,9\ 10^{-9}$	$5,1\ 10^{-11}$	$8,7\ 10^{-12}$
Total result		$6,6\ 10^{-10}$	$3,1\ 10^{-10}$

Outcomes from case 2:
In principle, GRS, IRSN and NUPEC have the same approach for the analysis of this precursor event. The analysis of the event takes into account the plant operational state where the precursor event originally occurred. Each participant selected small LOCA at least. In addition, NUPEC considered very small LOCA and other transients and IRSN considered loss of feedwater. The results of IRSN and GRS are close. The results of NUPEC are much lower. One reason is the different design of the Japanese plant. NUPEC had to make some special assumptions to transfer the event to a Japanese PWR-plant. In addition NUPEC treated the recovery for both, HPSI and LPSI pumps as possible. It can be concluded that the results are strongly affected by the plant design and operation procedures. Furthermore, the results are influenced by the HRA methodologies applied, which are fairly different among participants.

CASE 3: POTENTIAL CCF AFFECTING SAFETY SWITCHBOARDS

The unit was operating at full power. An arc strike that occurred on one contactor supplying one Essential Service Water System (ESWS) pump resulted in a cell explosion and a fire in the emergency switchboard LHB, leading to its destruction. The deterioration of the damping washers in the contactor, resulting from heating due to aging, provoked the arc strike. The unit was placed in intermediate shutdown conditions, as soon as the operator extinguished the fire and identified the safe state adapted to the situation. The same aging effect was found at the contactors in the redundant switchboard LHA.

Interpretation of the event:
All the participants considered a potential CCF of both safety switchboards LHA and LHB, leading to a station blackout. The potential consequences are a loss of secondary cooling or a primary circuit LOCA without water injection possibility.

IRSN analysis:
Taking into account that the root cause of the incident was aging, IRSN assumed that a beta factor of 0.1 could be taken for the CCF probability of both safety switchboards. The dominant sequences are: the failure of the turbine driven feedwater pump ($2.2\ 10^{-3}$; 44 %) and the failure of the secondary side cooling due to human errors ($2.1\ 10^{-3}$; 42 %). Reactor Coolant Pump (RCP) seal LOCA followed by failure of the injection from the twin unit ($7.5\ 10^{-4}$; 15 %) gives the third contribution. A sensibility study was conducted, regarding the consequences of the loss of LHA and LHB switchboards for all the plant operational states. The result is 10 % higher. The study shows that the event would have been more serious at mid-loop operation.

GRS analysis:
For the loss of LHA switchboard, two possibilities have been considered, the potential CCF (incipient impairment of circuit breakers, ICDE definition, CCF probability 0,1) or the fire spreading from redundancy LHB. A beyond design event probability of 6 10^{-3} due to this precursor event was calculated. The result is dominated by the complete loss of the busbars LHA and LHB due to CCF and the failure of the turbine driven auxiliary feedwater pump. GRS noticed that the result depends strongly on the judgment of the degradation of the circuit breakers in redundancy LHA.

NUPEC analysis:
Using Impact Vector Method like for case 1, NUPEC assigned the probability of 0,1 to the initiator "loss of LHA and LHB switchboards". The dominant sequence for this event (7,3 10^{-2}: 96 %) is the RCP seal LOCA. Based on /3/, NUPEC assessed that the probability of RCP leak greater than 21gpm/RCP is about 0.73. Such high CCDP is caused by the followings reasons. First, Japanese 3-Loop PWR has no alternative seal injection measure for RCP seal LOCA like French 900 MWe PWR. Batteries are not charged in case of loss of total emergency buses in Japanese 3-Loop PWR since no power supply to batteries such as that from twin unit exists in Japanese PWRs.

Outcomes from case 3:
All participants considered potential CCF for total loss of electric power. They used similar methodologies as seen for case 1 and they all agree on the probability of 0.1 for the CCF of the redundant busbars LHA and LHB. The result of IRSN and GRS are pretty close while that of NUPEC is more than 10 times higher due to the contribution of RCP seal LOCA. Differences concerning the design of the reactors impact the ways of degradation leading to core damage. GRS does not consider the sequences relevant to RCP seal LOCA, while on another hand, IRSN considers the credit of alternative seal injection and several means of mitigation. NUPEC, based on the design of Japanese 3-Loop PWR, does not consider such mitigation or prevention measures but takes into account that the auxiliary feedwater system is backed up by main feedwater system.

GENERAL CONCLUSIONS

A great advantage of probabilistic analysis of events is that the analysis is not limited to the study of causes of the event (as generally done by classical event analysis), but is also an evaluation of potential consequences and of the remaining lines of defense. In that way, this exercise shows that IRSN, GRS and NUPEC have a similar approach. In the comparison of 3 cases, it appears that the interpretation has been very similar (same potential ways of degradation). Concerning quantification, this exercise provided a lot of feedback concerning numerical results and methodology. In several cases, numerical results were not very different. When they are different, an explanation can be found in the design, the strategies of management or the plant operational state chosen for the quantification. Some important differences in specific practices are for example:

- The risk measure which is Conditional Core Damage Frequency (CCDF) for IRSN and NUPEC, while GRS uses the conditional probability of beyond design situations. That means, accident management measures are not taken into account by GRS in the precursor analysis.
- The state of the plant in which the event has been analyzed: generally, GRS and NUPEC analyze the event in the plant operational state where the event has really occurred, while IRSN considers all the possible plant states and performs either an average or a sensitivity study.

– The recovery possibilities: especially concerning recovery actions carried out by operators, the possibilities depend strongly on design and operation specificities of the plant.

Interesting comparisons have been obtained from the quantification of the potential common cause failures. GRS and IRSN used the ICDE methodology and NUPEC used the NRC methodology that is very similar. In this way, the different factors that qualify the common cause failures can be compared.

The comparison underlined the importance of recoveries which strongly depends on the plant design and operation. It could be interesting to have a further investigation in this field with a comparison of a problem specifically defined for that purpose.

Furthermore, this comparison exercise can be used as a basis for deriving suggestions or recommendations for harmonization of precursor analysis methods.

REFERENCES

1. IRSN, GRS, NUPEC:
   Comparison exercise of probabilistic precursor analysis
   Final Report, October 2003
2. K. J. Kvarfordt, M. J.Cebull, S. T. Wood, A. Mosleh:
   Common Cause Failure database and Analysis System,
   NUREG/CR-6268, June 1998
3. U.S. Nuclear Regulatory Commission:
   Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants
   NUREG-1150, December 1990 (Vol. 1), December 1990 (Vol. 2), January 1991 (Vol. 3)
4. A. D. Swain:
   Accident Sequence Evaluation Program,
   Human Reliability Analysis Procedure
   NUREG/CR-4772, February 1987