Discussion of the concept of safety indicators from the point of view of TfUX2 accident sequence for Forsmark-3

Bujor, Adrian

Publication date:
1991

Document Version
Publisher's PDF, also known as Version of record

RISØ

Risø-M-2926

Discussion of the Concept of Safety Indicators from the Point of View of TfUX2 Accident Sequence for Forsmark 3

Adrian Bujor

Risø National Laboratory, Roskilde, Denmark
January 1991

Discussion of the Concept of Safety Indicators from the Point of View of TfUX2 Accident Sequence for Forsmark 3

Risø-M-2926

Adrian Bujor

Risø National Laboratory, Roskilde, Denmark
January 1991

Abstract. This paper contains general considerations on the safety indicators, with details at the system level and for the operator actions.

For the system analysis, a modular analysis at a low detailed level is proposed (Module System Approach) in order to emphasize the safety related aspects at the subsystem (module) level.

The operator actions are divided in "active actions" (actions in the control room during incident/accident situations) and "passive actions" (actions during tests, maintenance, repairs, etc.) and are analyzed separately.

In the second part, a discussion of a possible way to apply some SI to the TfUX2 accident sequence for FORSMARK-3, is done. For the analysis of the Auxiliary Feedwater Systems (AFWS) an equation is proposed to derive target values for the failure probability on demand at the train level, given the target value at the system level, including the common cause failures between the redundant trains.

ISBN 87-550-1726-6
ISSN 0418-6435

Grafisk Service, Risø 1991

CONTENTS

1. INTRODUCTION

The operation of a nuclear plant and the authorizing process require a continuous evaluation of the risk and safety related aspects. Useful and comprehensive information is contained in the existing PSA-reports but this is difficult to be used unless an appropriate organization of this data is made. It must also be noted that the conditions in the plant during normal operation are different from those considered in PSA (components unavailable during repairs or T&M, systems in alternate configurations or operation modes etc.) and all these aspects must be considered in the decision process with safety significance.

Therefore a post-analysis of the PSA results is necessary with development of tools as "Living PSA" package (pre-processed information, updatable reliability data bases, simplified risk model for the plant etc.) and a set of Safety Indicators (SI) which should allow a continuous evaluation of the risk and safety in the quantitative and qualitative terms, to cope with the specific demands and concerns at different levels (regulatory, management, operation, etc.).

The objective of this report is to clarify some aspects on SIs with emphasis on the indicators related to the operator and to the (safety) systems.

Based on the available information, an application for the TfUX2 accident sequence for FORSMARK-3 reactor is done. However, the lack of data on:

- operating modes, process parameters, alternate configurations, structure and boundary links of the Auxiliary Feedwater System (AFWS) with other systems
- test and maintenance
- operating experience

- safety philosophy and the quantitative and qualitative criteria already accepted for FORSMARK-3

have a negative effect on the results.

2. CATEGORIES OF SAFETY INDICATORS

Before establishing a set of Safety Indicators, the identification of the users and their demands is a first problem to be solved. This is obvious because of the different ways in which the safety is perceived at different levels. The appropriate parameters "seen" as defining the safety and acceptable quantitative and qualitative evaluation should then be stated.

On the other hand, safety indicators are often included in the more general class of Performance Indicators (PI) as it should be seen from a list with NRC Performance Indicators, /9/, Table 1, and WANO Indicators /9/, Table 2. These indicators reflects different approaches to express the performance and the safety of the plants. The limits for the areas nonaction-warning-action to improve safety, at the plant level, could be established versus the value of such indicators, because their ability to describe in a simplified form, from the safety standpoint, long periods of operation (ex: (Number of) Unplanned Automatic Scrams While Critical). However, the degree of generality is so high (ex: "Collective radiation exposure") that these indicators does not offer information on the events which might cause an eventual increase of the risk or on the ways to improve the safety.

Therefore, at the utility level, and for authorization activities during operation, different indicators should be used.

Table 1. NRC Performance Indicators, /9/ (partial list).

Automatic Scrams While Critical
Safety System Actuations
Significant Events
Safety System Failures
Forced Outage Rate
Equipment Forced Outage per 1000 Critical Hours
Collective Radiation Exposure

Table 2. WANO Performance Indicators, /9/.

Unit Capability Factor
Unplanned Capability Loss Factor
Unplanned Automatic Scrams per 7000 Hours Critical
Safety System Performance
Thermal Performance
Fuel Reliability
Collective Radiation Exposure
Volume of Low-level Solid Radioactive Waste
Chemistry Index
Industrial Safety Loss Time Accident Rate

They are mainly related to the risk evaluation using the information and knowledge included in the PSA analysis.

As results from /13/, many Safety Quantitative Guidelines are derived from PSA and are calculated for different levels (system level, level 1, level 2 or level 3) according to the PSA level used to express the probability of the consequences. Many pro-

babilistic SI's, expressing the availability requirements for the safety systems or safety functions or the core melt probability are implemented as authorization criteria /9/, /13/.

Details on the methodology to derive SI at different levels are given in /7/ and /10/, including the aspects related to the test and maintenance (T & M) activities, /11/, /12/. Important requirements which the SI must satisfy, as formulated in /10/, are related to the necessity of showing, as accurate as possible, the permanent changes in the performance of the plant, from a safety point of view.

2.1. Indicators for Safety Systems

During operation, for a specific state of the plant, the overall risk and consequences expected at the occurance of an Initiating Event depend on the answer of the facility-operator complex system. The effectiveness of this answer represents the measure in which the Safety Functions (SF) at the plant level, are performed.

The state of the plant is appropriate from the safety standpoint if the SF's are properly covered. Further, an SF is properly covered when the systems involved (and also the operator) are in an appropriate state. At system level, the SI's must show the ability of the system to answer the SF's demands. These indications may have different forms upon the way in which the systems are called. Useful information could be obtained form the existing PSA updated with the operating experience. However, it is possible that the operating modes, operating parameters, configurations, etc. for the systems during plant operation are different from the assumptions used in PSA. It is also possible that a system have components, trains, or other modules unavailable because they are under Test and Maintenance (T & M) or Repairs (R) activities, or generally, the system is in a degraded state. So, it is important to define the representative parameters for these states and to have a continuous indication on

these. Obviously, these parameters will not be necessary the same for all the systems.

The information at the system level in PSA is, generally, included in the Fault trees (FT). The level of detail is, however, very deep (we may have as basic events failure modes of the components, including components in the support systems, failures in the instrumentation and control chains, different human errors, etc.) and therefore it is difficult to obtain the essential data which have to be easy for use in operational safety evaluations.

For these analysis, the level of detail must be chosen very carefully using engineering judgements following the functions and tasks of the system. At this level we shall find the new Basic Events related to failures in components, trains/subsystems/modules etc. Based on a functional analysis on the ability of the system to answer at the SF demands, it is possible to establish a modular structure of the system and to analyze the system at this particular level with e.g. fault tree method. We shall call this method - the Module-System Approach (MSA).

For instance, a pump line can be considered a module, and also, redundant lines or set of overpressure valves, etc. and failure of these modules will be the intermediate or basic events in the new FT. The ability of a module to perform its function can be established not only in probabilistic terms (availability, reliability), but also by process parameters (e.g.: flow and pressure at the exit of a pump line module give good indications on the state of the module). It will not be a surprise to find such parameters as those monitored in the control room but now their safety meaning will be emphasized.

Obviously, different approaches should be used for standby (safety) systems whose main object is to act on demand, and for the systems with continuous operation whose main task is to continuously accomplish their function for a long period of time. If for the latter the process parameters in the system during operation could provide useful information related to the safety

aspects, not the same thing can always be said if we consider the systems in the first category.

However, the relations between the modules, both qualitative and quantitative and their importance in the system could provide useful criteria.

From the quantitative (numerical) point of view, we may find the numerical criteria acceptable for these modules as function of the target values imposed for the whole system (e.g. criteria for series-modules, evaluation of the redundancy level required).

Table 3. Maintenance Indicators, /11/.

1. Annunciator Alarms Continuously on:
   - Lifted leads
   - Maintenance Work Request (MWR) on Safety Related Equipment
   - # of Components Tagged out for Maintenance more than 3 months
   - # of Missed Surveillance on Equipment
   - # of MWRs Written by Maintenance Personnel
   - # of Repeat Maintenance Items
   - # of Temporary Modifications over 3 months Delay (%)
   - Realignment Errors During Maintenance
   - Temporary Modifications
   - Wrong Unit/Wrong Train Events
2. % Corrective MWRs Older than 3 months
3. % LERs due to Maintenance
4. % Preventive MWRs Completed on Safety Equipment
5. Accumulated Duration of Limited Conditions of Operation (LCO) Conditions
6. Backlog of Engineering Change Notices (ECN) Related to Equipment Performance
7. Backlog of Maintenance Procedure Revisions
8. Component in LCO Condition
9. Corrective Maintenance Backlog > 3 months

Table 3 (Continued)

10. ESF Actuations due to Maintenance and Testing
11. Fraction Labor Hours on Surveillance
12. Fraction of MWRs Reviewed by Quality Control (QC)
13. Fraction of Components under Condition Monitoring
14. Gross Heat Rate (Thermal Performance
15. Industrial Safety Loss-Time Accident Rate
16. Maintenance Backlog
17. Maintenance Overtime
18. Maintenance Rework
19. Maintenance Staff Radiation Exposure
20. Maintenance Staff Size
21. Mean Age of Maintenance Procedure Revisions
22. Mean Repair Time
23. Mean Time Between Forced Outages from Equipment Failures
24. Mean Time Between Repairs (Most Frequently Repaired Items)
25. Mean Time to Return to Service
26. Number & Duration of BOP Equipment Out of Service
27. Part 21 Reports
28. Preventive Maintenance Items Overdue
29. Rate of Adoption of Industry Upgrades
30. Rate of Calibration Errors
31. Rate of Deferred Periodic Tests
32. Rate of Downtime due to Failures
33. Rate of Faults Detected by Actual Demands
34. Rate of Faults Detected by Periodic Testing
35. Rate of LCOs
36. Rate of Maintenance Errors
37. Rate of Maintenance Requested Training Programs
38. Rate of Maintenance Staff on Vendor Courses
39. Rate of Maintenance Staff Retraining
40. Rate of Manhours in Maintenance
41. Rate of Misalignments
42. Rate of MWRs
43. Rate of Out-of-Service Tags
44. Rate of Pending Modification Requests
45. Rate of Root Cause Evaluations due to Maintenance
46. Rate of Time Spare Parts Unavailable

Table 3. (Continued)

47. Ratio QC/Maintenance Staff
48. Ratio, # Hours to Repair Degraded Components/Total Maintenance Hours
49. Ratio, # of Repairs while Degraded/# of Repairs Failed + Degraded
50. Ratio, # of Deficiencies Discovered in Surveillance/Total Discovered
51. Ratio, # of Failures During Post Maintenance Test/# of P.M. Test
52. Ratio, # of Highest Priority MWRs/Total MWRs
53. Ratio, Mean Repair Time/Time to Failure or Degrade
54. Ratio, Preventive Maintenance/Total Maintenance
55. Ratio, Utility/Contractor Staff
56. Repair Duration w.r.t. Allowed Outrage Times (AOT) by Technical Specifications
57. Safety System Function Trend
58. Scrams due to Maintenance & Testing
59. Turnover Rate/Vacancies
60. Wall Thinning/Pitting
61. Wrong Parts Events

In the evaluation of the system availability as SI, the technical specifications related aspects (test and maintenance, repairments) should be accounted for. Extensive works to include these in the formulation of Performance Indicators and Safety Indicators are reported in /11/ and /6/.

In /11/, a comprehensive list of PI is proposed, Table 3, and between them, a large number of safety-related indicators can be found.

In /6/ is described a systematic approach for defining outage-time criteria ("control values") at different levels (component, system, function, sequence, core melt, overall risk), for different risks (operating accident risk, shutdown accident risk, etc.) and other hypothesis (e.g. possible regulatory approaches,

strategies for addressing different risks). The numerical quantifications are based on combining the down time (planned or unplanned) related parameters (frequency of down time occurrence, down time period, accumulated down time, etc.) with the accident frequency where the component is down, but no information is given on the acceptable values for the control criteria.

Considering that the outage times constitute deviations from the standard state of the systems, specific numerical criteria could be proposed, /8/.

As it can be seen, for the (standby) safety systems the most discussions are taken on the way in which different events affect the availability of the system. This is confirmed by the formulation on this basis of the "Safety System Function Trend" (SSFT) as a performance indicator, /10/, and other similar indicators ("Safety System Performance Indicator", /17/, "Safety Grade Equipment out of Service", /18/).

A possibility for assessing the impact of the changes in the T&M related aspects, is to implement the appropriate new numerical values (as the new human error probability, test interval, etc.) in the risk model of the plant, using the facilities of the Living PSA (LPSA), and to compare the results with the previous ones or with the accepted SI at different levels.

The use of LPSA, if maintained updated with the operating data, would also allow to obtain information on the actual unavailabilities (for components, trains, systems), and to support measures for avoiding unacceptable situations, from the risk standpoint.A special attention should be paid to those factors which have large values resulted from importance calculations.

2.2. Indicators Associated with the Human Factor

The impact of the human factor on the safety of the plant is large enough to require a special attention. The operator affects the risk state of the plant by the actions and the decisions in

the control room, as well as by the Technical-Specifications related activities (test, maintenance, repairments, etc.).

From the safety standpoint it is useful to separe these actions. We shall call "active actions" (A.A.) those decisions and actions in the control room in order to mitigate the accident. The A.A. can be of different types as:

- manual actuation of stand-by equipments following operation procedures or accident procedures
- manual actuation when the automatics fails
- specific commands/actions in situations which are not included in procedures
- other activities related to the management of the accident situations.

These actions have a direct influence on the evolution and the consequences of the accident. Therefore, an obvious analogy appears between the answer of the operator, concertized in A.A.s and the answer of a safety system/mitigation system.

In this approach, it would be suggestive to place the A.A.s at the Event-Tree level. A similar approach is used in the out-dated "Safety Design Matrix" methodology, where these actions are included, as decision nodes, in the Event Sequence Diagrams. So, the target values for the numerical criteria for A.A.s (e.g. human error probability) could be derived from the similar criteria which are imposed for the safety systems/mitigation systems, etc. (An explanation seems to be necessary: the terms used for different types of systems may by unclear. This is because in different approaches, different terms are used: safety systems, process systems, mitigation systems, systems important for the safety, systems with safety functions, support systems, service systems, etc. - which have specific meanings for specific safety philosophies. The lack of information on the specific safety approaches for FORSMARK-3 prevents the use of a precise language).

On the other hand, the answer of the operator is influenced by a number of factors like:

- the training level
- the quality and the quantity of the information available in the control room
- the stress level during the accident
- the presence of the recovery factors
- the time window available

By an appropriate control of these factors the safety indicators related to the operator's A.A. could be maintained inside the accepted limits.

In the second category, the Technical Specifications related activities are included. These activities are continuously performed during the operation of the plant. In the accident situations, these activities are important by their outcome, but only the A.A. can change the evolution of the accident. Therefore, we shall call the activities of this second category "Passive actions" (P.A.).

During the accident situations, their outcome is very important but it can no more be modified: it is "as good (as bad) as done".

These actions cannot be equivalated with the actions of the safety systems/mitigation systems, and the safety indicators cannot be derived from the criteria for these systems. It is more appropriate to associate the P.A. to the Test and Maintenance related criteria at the system/module/component level, because the P.A. have influence on the time during which the system/module/component is down.

The Allowed Outage Times (AOT) impact on the risk was analyzed in extension in /6/, where the planned and unplanned outage times were considered, but without references to the human factor. However, it is obvious that unplanned outage times can result because of errors in P.A. (ex: misalignments, wrong unit/wrong train events, etc.) which must be included in analysis.

For instance - the error in reconfigurating the components/system after test or maintenance, which makes the component/system unavailable until the next test or surveillance, though there is no hardware failure (e.g.: a key/switcher in a panel which remains in "Manual" position instead of "Remote" position).

The contribution of the human errors related to Technical-Specifications activities, to the component/system down time should be accounted for the evaluation of the outage times and their acceptability.

3. APPLICATION FOR THE TfUX2 SEQUENCE

For the analysis of this sequence, the level of technical information available for the systems involved (especially - the auxiliary feedwater system - AFWS), as well as on the operating experience, the T & M related aspects and the safety requirements for FORSMARK-3 did not permit a deep insight on the specific issues.

More, the fault tree associated with this sequence was available in a reduced form, without access to the assumptions for which it was obtained (e.g.: the basic configuration of the systems for which the fault tree was built, justifications for the very large frequencies associated with the common cause failures, boundary conditions, simplifications used, etc.).

Therefore, a detailed quantitative analysis was not the final object but only a descriptive evaluation at AFWS and operator level is done.

3.1. Description of the Sequence

The TfUX2 Sequence is described in /14/ and is given by a reduced list of the most important cut sets /1/, and their probabilities, Table 4. In Table 5, /1/, the codification system for the basic events is presented. A general flow-chart of the plant is shown in Fig. 1, /14/.

The initiating event is Loss of Off Site Power (event Tf) with a frequency of 0.25/y, which causes the loss of the Main Feedwater System.

For removing the residual heat and cooling the core (in this sequence it is assumed that the scram occurs), it is automatically actuated the Auxiliary Feedwater System (AFWS), whose electrical power supply is assured by diesel generators and a gas turbine.

If AFWS fails to start (event U with a probability of $1.72 * 10^{-3}$/d) the heat in the core is not removed, the pressure increases and the liquid coolant level decreases. The only possibility to prevent the fuel damage because the decreasing of the level (below 0.5 m) is to use the Emergency Core Cooling System (ECCS) which, however, operates at a lower pressure level. For this, the operator must initiate the depressurization of the core down to the pressure where the ECCS action is possible. If the operator fails to do this (event X2, with a probability of $1.0 * 10^{-2}$/d), the fuel damage occurs.

The frequency of this sequence is $4.3 * 10^{-6}$/y, which represents 91% from the overall contribution of the sequences in Tf category to the total core melt.

In the total core melt probability, which is $7.0 * 10^{-6}$/y for FORSMARK-3, the sequence TfUX2 has the most important contribution (61.4%).

The available fault tree for this sequence, contains the most important 88 cut sets which represents approximately 91% from the

total frequency of the sequence. The most important is the cut set no. 1 (H314BMAN-failure of the operator to initiate the depressurization - and H327XOOCCF - common cause failure which makes all the four trains of AFWS unavailable) with a probability of $1.3 * 10^{-6}$/y and represents 68.4% in the total frequency of TfUX2.

Besides the AFWS (327) and the operator, the following systems are involved:

- secondary cooling system for starting and shutdown (721)
- seawater cooling system for shutdown reactor (712)
- logic channels (516)

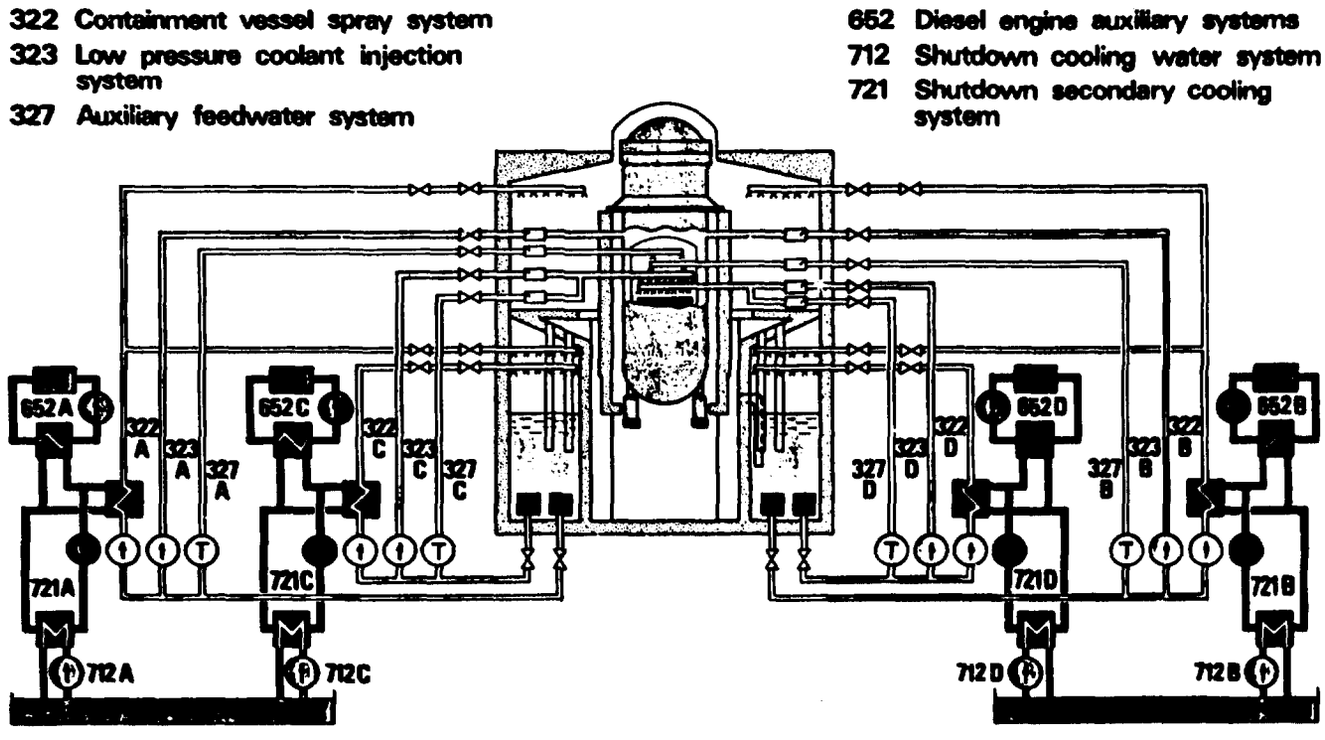
However, their structure, function, operating modes, etc. as well as their interaction with AFWS are nor very clear. Therefore, it was necessary to neglect in the analysis all the aspects in which these systems are involved.

Table 4. Cuts sets for the sequence TfUX2 ordered by probability

1.	1.30E-05	H314TBMAN	H327X00CCF			
2.	2.03E-07	H314TBMAN	H327AB0CCF	H327CMAINT		
3.	1.04E-07	H314TBMAN	H327AB0CCF	H327VC4M1A		
4.	1.04E-07	H314TBMAN	H327AB0CCF	H327VC2M1B		
5.	1.04E-07	H314TBMAN	H327ABCCCF	H327VD4M1A		
6.	1.04E-07	H314TBMAN	H327ABCCCF	H327VD2M1B		
7.	1.04E-07	H314TBMAN	H327BCDCCF	H327VA4M1A		
8.	1.04E-07	H314TBMAN	H327BCDCCF	H327VA2M1B		
9.	1.04E-07	H314TBMAN	H327ACDCCF	H327VB4M1A		
10.	1.04E-07	H314TBMAN	H327ACDCCF	H327VB2M1B		
11.	1.00E-07	H314TBMAN	H327MSG	H516RCCCF		
12.	3.27E-08	H314TBMAN	H327CMAINT	H327VD4M1A	H327VB4M1A	H327VA4M1A
13.	3.27E-08	H314TBMAN	H327CMAINT	H327VD2M1B	H327VB4M1A	H327VA4M1A
14.	3.27E-08	H314TBMAN	H327CMAINT	H327VD4M1A	H327VB2M1B	H327VA4M1A
15.	3.27E-08	H314TBMAN	H327CMAINT	H327VD4M1A	H327VB4M1A	H327VA2M1B
16.	3.27E-08	H314TBMAN	H327CMAINT	H327VD2M1B	H327VB2M1B	H327VA4M1A
17.	3.27E-08	H314TBMAN	H327CMAINT	H327VD2M1B	H327VB4M1A	H327VA2M1B
18.	3.27E-08	H314TBMAN	H327CMAINT	H327VD4M1A	H327VB2M1B	H327VA2M1B
19.	3.27E-08	H314TBMAN	H327CMAINT	H327VD2M1B	H327VB2M1B	H327VA2M1B
20.	2.77E-08	H314TBMAN	H327AB0CCF	H327CMAINT	H327VD4M1A	
21.	2.77E-08	H314TBMAN	H327AB0CCF	H327CMAINT	H327VD2M1B	
22.	2.77E-08	H314TBMAN	H327B00CCF	H327CMAINT	H327VA4M1A	
23.	2.77E-08	H314TBMAN	H327B00CCF	H327CMAINT	H327VA2M1B	
24.	2.77E-08	H314TBMAN	H327AD0CCF	H327CMAINT	H327VB4M1A	
25.	2.77E-08	H314TBMAN	H327AD0CCF	H327CMAINT	H327VB2M1B	
26.	2.30E-08	H314TBMAN	H327ASTDBY	H327CSTDBY	H721X00CCF	
27.	2.20E-08	H314TBMAN	H327ASTDBY	H327CSTDBY	H712X00CCF	
28.	2.18E-08	H314TBMAN	H327ABDCCF	327PC01K1A		
29.	2.18E-08	H314TBMAN	H327ACDCCF	327PB01K1A		
30.	2.18E-08	H314TBMAN	H327ABCCCF	327PD01K1A		
31.	2.18E-08	H314TBMAN	H327BCDCCF	327PA01K1A		
32.	2.03E-08	H314TBMAN	H327CSTDBY	H327ABDCCF	H721CMAINT	
33.	2.03E-08	H314TBMAN	H327CSTDBY	H327ABDCCF	H712CMAINT	
34.	1.68E-08	H314TBMAN	H327VC4M1A	H327VD4M1A	H327VB4M1A	H327VA4M1A
35.	1.68E-08	H314TBMAN	H327VC2M1B	H327VD4M1A	H327VB4M1A	H327VA4M1A
36.	1.68E-08	H314TBMAN	H327VC4M1A	H327VD2M1B	H327VB4M1A	H327VA4M1A
37.	1.68E-08	H314TBMAN	H327VC4M1A	H327VD4M1A	H327VB2M1B	H327VA4M1A
38.	1.68E-08	H314TBMAN	H327VC4M1A	H327VD4M1A	H327VB4M1A	H327VA2M1B
39.	1.68E-08	H314TBMAN	H327VC2M1B	H327VD2M1B	H327VB4M1A	H327VA4M1A

Table 4. (Continued)

40.	1.68E-08	H314TBMAN	H327VC2M1B	H327VD4M1A	H327VB2M1B	H327VA4M1A
41.	1.68E-08	H314TBMAN	H327VC2M1B	H327VD4M1A	H327VB4M1A	H327VA2M1B
42.	1.68E-08	H314TBMAN	H327VC4M1A	H327VD2M1B	H327VB2M1B	H327VA4M1A
43.	1.68E-08	H314TBMAN	H327VC4M1A	H327VD2M1B	H327VB4M1A	H327VA2M1B
44.	1.68E-08	H314TBMAN	H327VC4M1A	H327VD4M1A	H327VB2M1B	H327VA2M1B
45.	1.68E-08	H314TBMAN	H327VC2M1B	H327VD2M1B	H327VB2M1B	H327VA4M1A
46.	1.68E-08	H314TBMAN	H327VC2M1B	H327VD2M1B	H327VB4M1A	H327VA2M1B
47.	1.68E-08	H314TBMAN	H327VC2M1B	H327VD4M1A	H327VB2M1B	H327VA2M1B
48.	1.68E-08	H314TBMAN	H327VC4M1A	H327VD2M1B	H327VB2M1B	H327VA2M1B
49.	1.68E-08	H314TBMAN	H327VC2M1B	H327VD2M1B	H327VB2M1B	H327VA2M1B
50.	1.60E-08	H314TBMAN	H327ACDCCF	H327VB5B1A		
51.	1.60E-08	H314TBMAN	H327ABCCCF	H327VD5B1A		
52.	1.60E-08	H314TBMAN	H327ABCCCF	H327VD3B1A		
53.	1.60E-08	H314TBMAN	H327ABDCCF	H327VC5B1A		
54.	1.60E-08	H314TBMAN	H327BCDCCF	H327VA3B1A		
55.	1.60E-08	H314TBMAN	H327ABDCCF	H327VC3B1A		
56.	1.60E-08	H314TBMAN	H327BCDCCF	H327VA5B1A		
57.	1.60E-08	H314TBMAN	H327ACDCCF	H327VB3B1A		
58.	1.43E-08	H314TBMAN	H327ADOCCF	H327VC4M1A	H327VB4M1A	
59.	1.43E-08	H314TBMAN	H327ADOCCF	H327VC2M1B	H327VB4M1A	
60.	1.43E-08	H314TBMAN	H327BDOCCF	H327VC4M1A	H327VA4M1A	
61.	1.43E-08	H314TBMAN	H327ADOCCF	H327VC4M1A	H327VB2M1B	
62.	1.43E-08	H314TBMAN	H327ADOCCF	H327VC2M1B	H327VB2M1B	
63.	1.43E-08	H314TBMAN	H327BDOCCF	H327VC2M1B	H327VA4M1A	
64.	1.43E-08	H314TBMAN	H327ABOCCF	H327VC4M1A	H327VD2M1B	
65.	1.43E-08	H314TBMAN	H327ABOCCF	H327VC4M1A	H327VD4M1A	
66.	1.43E-08	H314TBMAN	H327ABOCCF	H327VC2M1B	H327VD2M1B	
67.	1.43E-08	H314TBMAN	H327BCOCCF	H327VD4M1A	H327VA4M1A	
68.	1.43E-08	H314TBMAN	H327BCOCCF	H327VD2M1B	H327VA4M1A	
69.	1.43E-08	H314TBMAN	H327BCOCCF	H327VD4M1A	H327VA2M1B	
70.	1.43E-08	H314TBMAN	H327BCOCCF	H327VD2M1B	H327VA2M1B	
71.	1.43E-08	H314TBMAN	H327ACOCCF	H327VD4M1A	H327VB4M1A	
72.	1.43E-08	H314TBMAN	H327BDOCCF	H327VC4M1A	H327VA2M1B	
73.	1.43E-08	H314TBMAN	H327BDOCCF	H327VC2M1B	H327VA2M1B	
74.	1.43E-08	H314TBMAN	H327ACOCCF	H327VD2M1B	H327VB4M1A	
75.	1.43E-08	H314TBMAN	H327ACOCCF	H327VD4M1A	H327VB2M1B	
76.	1.43E-08	H314TBMAN	H327ACOCCF	H327VD2M1B	H327VB2M1B	
77.	1.43E-08	H314TBMAN	H327CDOCCF	H327VB4M1A	H327VA4M1A	
78.	1.43E-08	H314TBMAN	H327CDOCCF	H327VB2M1B	H327VA4M1A	
79.	1.43E-08	H314TBMAN	H327CDOCCF	H327VB4M1A	H327VA2M1B	
80.	1.43E-08	H314TBMAN	H327CDOCCF	H327VB2M1B	H327VA2M1B	
81.	1.43E-08	H314TBMAN	H327ABOCCF	H327VC2M1B	H327VD4M1A	
82.	1.21E-08	H314TBMAN	H327ADOCCF	H327BCOCCF		
83.	1.21E-08	H314TBMAN	H327CDOCCF	H327ABOCCF		
84.	1.21E-08	H314TBMAN	H327ACOCCF	H327BDOCCF		
85.	1.19E-08	H314TBMAN	H327ASTDBY	H327BCDCCF	721PA01C2A	
86.	1.19E-08	H314TBMAN	H327ASTDBY	H327BCDCCF	712PA01C2A	
87.	1.19E-08	H314TBMAN	H327ACDCCF	H327ASTDBY	712PB01C2A	
88.	1.19E-08	H314TBMAN	H327ACDCCF	H327ASTDBY	721PB01C2A	



Emergency cooling systems.

Fig. 1. Main flow sheet of FORSMARK-3 plant.

Table 5. Codification system for the basic events, /1/,

Code	Codification system for the basic events, /1/
H314TBMAN	Failing manual depressurization
H327XOOCCF	Quadruple Common Cause Failure (CCF) in the system 327 (AFWS)
H327XXXCCF	Triple CCF in 327
H327/H721/H712MAINT	Maintenance in 327, 721 or 712
H327VXXMYY	Valve (MOV) in 327 fails to close/ open
H327MSG	Non-appearing/Blocked Actuation Signal in 327
H516RCCF	CCF in 3/4 logic channels
H327XXOCCF	Double CCF in 327
H327ASTDBY	Operation > 0.5 h in standby loop for the train A in 327
H721XOOCCF	Quadruple CCF in 721
H712XOOCCF	Quadruple CCF in 712
327PX01K1A	Reciprocating pump (RP) fails to start
H327VXXBYY	Check valve (CHV) fails to open
712/721PX01C2A	Centrifugal pump (CP) fails to start

3.2. Safety Indicators

In the sequence TfUX2, the AFWS is automatically actuated after the loss of main feedwater system and, after the actuation, it

must be able to operate for a relative short period of time (hours) until the recovery of the Off-Site Power Supply and thus, the recovery of the main feedwater system.

The safety indicators of AFWS level are related to the capacity of the system to operate "on demand". An evaluation of the SI for AFWS (in terms of "System unavailability" on "Failure probability on demand") should be done following the contribution of this system by different sequences to the core melt probability.

A detailed analysis, as described in /6/ and /10/ is relied on the knowledge of the factors which influence the planned and unplanned outage times which affects the availability of the system. They include the T & M related aspects, the history of operation, repairment outcomes, impacts from other systems, etc. As mentioned above, the lack of data makes such analysis beyond the scope of this paper.

For the simplicity of the analysis, we may suppose that the AFWS in FORSMARK-3 is regarded as a mitigation system for which a good requirement for the failure probability per demand is 10^{-2}. As it is known, AFWS is made by four identical trains in parallel which assure a 4 x 100% redundancy level. Despite that, the overall availability of the system is strongly reduced because of the common cause failures which could make two, three, or even all the four trains unavailable.

Using MSA (se cap. 2.1) - it can be demonstrated that, given the target criteria for the system failure probability per demand (q_{ST}) and the frequency of the common cause failures of different order (q_{CCFi}), the target value for a single train (q_{TT}) is solution of the equation:

$$q_{TT}^{n} + \sum_{i} C_n^i \, q_{CCFi} \, q_{TT}^{n-i} = q_{ST} \qquad (1)$$

n = degree of redundancy
i = order of the common cause failure,
i = 2, ---, n

For our case, n = 4, and, from /1/,

$q_{CCF4} = 1.3 * 10^{-3}/d$

$q_{CCF3} = 2.9 * 10^{-4}/d$

$q_{CCF2} = 1.1 * 10^{-3}/d$

We obtain, for $q_{ST} = 10^{-2}/d$

$q_{TT} = 0.296/d$

The value seems to be very high, but this is because of the very high redundancy level and because of the low value assumed for q_{ST}.

However, during operation, one train may be unavailable (during T & M activities, for instance). In this situation, the level of redundancies is reduced to 3 * 100% (n=3 in eq. 1) and the target values at the train level is now

$q_{TT} = 0.1979/d$ for $q_{ST} = 10^{-2}/d$

and this value should be assured. Obviously, other calculations could be done. If we impose that the target for AFWS failure probability on demand should be the value used in PSA ($1.72 * 10^{-3}/d$), then, for n=3 we obtain $q_{TT} = 3.06 * 10^{-2}/d$.

Establishing such criteria at a lower level (train level, e.g.) has the advantage that, for assessing from the risk point of view the various deviations from the standard state of the system (as considered in PSA), the level of complexity for the risk model required to calculate these indicators is much reduced.

In terms of "unavailability", the performance of AFWS is influenced by the maintenance performed in AFWS (event H327CMAINT and, in a lower measure, by the events H327AMAINT, H327BMAINT and H327DMAINT) as well as by the maintenance in the support systems (events H712CMAINT and H721CMAINT).

H327CMAINT with a probability of $7 * 10^{-2}$ has a large contribution in the frequence of TfUX2. It can be seen (Tab. 4) that, during this event, at least one of the other trains of AFWS (A,

B, or D) must be available. Similar conclusions are obtained if the minimal cut sets containing H721CMAINT and H712CMAINT are analysed.

The use of a LPSA in this problem, requires special demands as:

- the plant risk model must be detailed enough to allow an appropriate modelling of the T&M factors included in these events in order to evaluate the impact on the risk for possible changes

- the pre processed information must allow the identification of the minimal cut sets containing a component/train which can be down during T&M and the realignments required in this case (if any), including the interface with the support systems

- the updated risk models must allow the identification of the momentan unavailablilities at lower levels (e.g. at train level for AFWS).

Another component of the TfUX2 sequence is the event X2: the failure of the operator to depressurize the reactor. The probability of this event, as it is used in /14/, is $1.0 * 10^{-2}$/d.

The depressurization is supposed to be done manually in order to avoid economical losses in the case of a spurious actuation of an would-be automatic actuation.

Therefore, this operator action (an active action, as stated in 2.2) can be equivalated with the action of a safety system or of a mitigation (process) system, and the operator (team) in the control room-regarded as such a system.

A detailed analysis was done in /4/ and the results obtained with different methods are summarized in Table 6.

If we compare these values with a general accepted value for the failure probability on demand for a safety system (10^{-3}/d) /9/,

we observe that the performance of the operator must be improved (e.g.: by special training for this sequence, better access to the key and, especially, by assuring the presence of the recovery factors). If, however, the manual depressurization is equivalated with the action of a mitigation system, with the target value for the failure probability on demand of 10^{-2}/d, the assurance of the effectiveness of the recovery factors in the control room is enough to cope with this criteria.

Another solution is to replace the manual depressurization with an automatic system for actuation for which the safety criteria for reliability and availability should be assured. In this case, an analysis of the economical risk due to the possibility of a spurious actuation have to be done.

Table 6. Failure probabilities for the manual depressurization, /9/.

	Method	
	THERP	HCR
Case A	$7.4 * 10^{-3}$	$4.5 * 10^{-3}$
Case B	$2.6 * 10^{-1}$	$5.5 * 10^{-1}$

Case A: with recovery factors
Case B: no recovery factors

4. CONCLUSION

The continuous evaluation from the safety point of view of different situations which appear during the operation (deviation from the conditions assumed in PSA, including unavailabilities at different levels, alternative operating regimes, etc.) require the implementation of a system of safety indicators which should provide reliable information on the impact of these situations on the safety and risk.

This problem is very complex and systematic studies should be done.

From the risk point of view, most of the works must be focussed on the safety systems as well as on the operator actions, both those in the control room during the accidents and those related to test and maintenance.

The analysis and calculations performed for the TfUX2 accident sequence for FORSMARK-3 have shown that the criteria for failure probability per demand for a single train in AFWS are restrictive because of the very high values for the common cause failure probabilities. Any improvement of AFWS performance is strongly conditioned by the reduction of the common cause failure probabilities or by diminishing their importance.

Regarding the manual depressurization (event X2 in the sequence) - the failure probability used in PSA (10^{-2}) is under the level of a safety system requirement and, also under the probability of the other event in the sequence ($1.72 * 10^{-3}$ for the event U).

5. REFERENCES

1. PÖRN, K., FAHLEN, R. (1988). "Reference Study on Uncertainty and Sensitivity Analysis". Studsvik/NP-88/53, NKA/RAS-470(88)/7.

2. BENGTZ, M., BJÖRE, S., HIRSCHBERG, S. (1985). "Identification of Common Cause Failures Events for Motor Operated Valves in Swedish Boiling Water Reactor Plants". ASEA-ATOM, RAS-470(86)4.

3. BENGTZ, M., HIRSCHBERG, S. (1985). "Benchmark Exercise, Phase 2; Quantification of Common Cause Failure Contributions. Final Report". ASEA-ATOM, RAS-470(86)8.

4. PETERSEN, K.E. (1988). "Reference Study on Human Interactions". Risø, RAS-470(87)16.

5. KIRCHNER, J.R., CAMPBELL, D.J. (1987). "An Overview of the Plant Risk Status Information Management System". NUREG/CP-0082, Vol. 1.

6. VESELY, W.E. (1989). "Evaluation of Allowed Outage Times (AOT's) from a Risk and Reliability Standpoint", NUREG/CR-5425.

7. VESELY, W.E., DAVIES, T.C., DENNING, R.S., SALTOS, N. (1983). "Measures of Risk Importance and their Application". NUREG/CR-3385.

8. LAASKO, K., MAUKAMO, T. (1990). "Notes from the IAEA Technical Committee Meeting on the Use of Probabilistic Safety Analysis to Evaluate Nuclear Power Plant's Technical Specifications - 18.-22.06.1990, Wien", Work Report, NKS/SIK-1(90)14.

9. LEHTINEN, E. (1990). "International Survey of Safety Indicators", NKS/SIK-1 Seminarium, Arlandia, Sweden, 23.08.1990.

10. BOCCIO, J.L., VESELY, W.E. et al. (1989). "Validation of Risk Based Performance Indicators: Safety System Function Trends", NUREG/CR-5323.

11. WREATHALL, J., FRAGOLA, J. (1990). "The Development and Evaluation of Programmatic Performance Indicators Associated with Maintenance at Nuclear Power Plants", NUREG/CR-5436.

12. CONNELLY, E.M., VAN HEMMEL, S.B., HAAPS, P.M. (1990). "Industry Based Performance Indicators for Nuclear Power Plants", NUREG/CR-5568.

13. CHAKRABORTY, S., GONEN, Y.G., VESTEEG, M.F. (1990). "Considerations of Quantitative Safety Guidelines in Member Countries". CSNI-R-117.

14. ***"FORSMAARK-3, Säkerhetsstudie", ASEA-ATOM, R-KPA-85-43.

15. MARCUS, A.A., NICHOLS, M.L., et al. (1990). "Organisation and Safety in Nuclear Power Plants". NUREG/CR-5437.

16. LEHTINEN, E., SAARELAINEN, P. (1990). "Monitoring of System Unavailability and Maintenance Performance Using LOTI Information System and Operational System Indicators. A Trial Study for Diesel Generators of LOVIISA-2 Plant". Technical Committee Meeting on Exchange of Experience in Managing Nuclear Power Plant Safety Using Numerical Indicators, Vienna.

17. DEY, M., TATABAI, A., SCOTT, W. (1988). "Proceedings of the Public Workshop for NRC Rulemaking on Maintenance of Nuclear Power Plants", NUREG/CP-0099.

18. OLSON, J., CHOCKIE, C.L. et al. (1988). "Development of Programmatic Performance Indicators", NUREG/CR-5241.

Riso National Laboratory

Riso - M - 2926

Title and author(s)

DISCUSSION OF THE CONCEPT OF SAFETY INDICATORS FROM THE POINT OF VIEW OF TfUX2 ACCIDENT SEQUENCE FOR FORSMARK-3

Adrian Bujor

Date January 1991

Department or group

Nuclear Safety Research

Groups own registration number(s)

SIK-01-91

Project/contract no.

Pages 29 Tables 6 Illustrations References 18

ISBN 87-550-1726-6

Abstract (Max. 2000 char.)

Abstract. This paper contains general considerations on the safety indicators, with details at the system level and for the operator actions.

For the system analysis, a modular analysis at a low detailed level is proposed (Module System Approach) in order to emphasize the safety related aspects at the subsystem (module) level.

The operator actions are divided in "active actions" (actions in the control room during incident/accident situations) and "passive actions" (actions during tests, maintenance, repairs, etc.) and are analyzed separately.

In the second part, a discussion of a possible way to apply some SI to the TfUX2 accident sequence for FORSMARK-3, is done. For the analysis of the Auxiliary Feedwater Systems (AFWS) an equation is proposed to derive target values for the failure probability on demand at the train level, given the target value at the system level, including the common cause failures between the redundant trains.

Descriptors - INIS

FORSMARK-3 REACTOR; HUMAN FACTORS; PROBABILISTIC ESTIMATION; REACTOR SAFETY; RISK ASSESSMENT; SYSTEM FAILURE ANALYSIS

Available on request from Risø Library, Risø National Laboratory, (Risø Bibliotek, Forskningscenter Risø), P.O. Box 49, DK-4000 Roskilde, Denmark.
Telephone +45 42 37 12 12, ext. 2268/2269. Telex: 43116, Telefax: +45 46 75 56 27

RH9500009/89

Available on exchange from:
Risø Library
Risø National Laboratory,
P.O. Box 49, DK-4000 Roskilde, Denmark
Phone +45 42 37 12 12, ext. 2268/2269
Telex 43116, Telefax +45 46 75 56 27

ISBN 87-550-1726-6
ISSN 0418-6435