Conf-910931--1
BNL-NUREG-46565

STRATEGIES AND CRITERIA FOR RISK-BASED CONFIGURATION CONTROL*

P.K. Samanta, W.E. Vesely†, and I.S. Kim

Risk and Reliability Analysis Group
Department of Nuclear Energy
Brookhaven National Laboratory
Upton, New York 11973

†Science Applications International Corporation

BNL-NUREG--46565

DE92 000480

ABSTRACT

A configuration, as used here, is a set of component operability or statuses that define the state of a nuclear power plant. Risk-based configuration control is the management of component configurations using a risk perspective to control risk and assure safety. If the component configurations that have high risk implications do not occur then the risk from the operation of nuclear power plants would be minimal. The control of component configurations, i.e., the management of component statuses, so that the risk from components being unavailable is minimized, becomes difficult because the status of a standby safety system component is often not apparent unless it is tested. In this paper, we discuss the strategies and criteria for risk-based configuration control in nuclear power plants. In developing these strategies and criteria, the primary objective is to obtain more direct risk control but the added benefit is the effective use of plant resources. Implementation of such approaches can result in replacement/modification of parts of Technical Specifications.

In defining the overall framework for risk-based configuration control, we define the factors that determine the risk-impact of a configuration. Probabilistic safety assessment (PSA) evaluations show that critical, high-risk configurations involve critical, safety-important components which are simultaneously down because of either failure, maintenance, or testing. Specifically, the risk impact or safety impact of a configuration depends upon four factors:

1. the configuration components which are simultaneously down (i.e., inoperable),
2. the backup components which are known to be up (i.e., operable),
3. the duration of time the configuration exists (the outage time), and
4. the frequency at which the configuration occurs.

Risk-based configuration control involves managing these factors using risk analyses and risk insights. In this paper, we discuss each of the factors and illustrate how they can be controlled. The information and the tools needed in implementing configuration control are also discussed. The risk-based calculation requirements in achieving the control are also delineated.

*Work performed under the auspices of the U.S. Nuclear Regulatory Commission.

1. INTRODUCTION

The objective of risk-based configuration control is to detect and control plant configurations from a risk perspective. The configurations of particular interest involve components which are down (i.e., inoperable) during power operation. Controlling plant configurations from a risk perspective can provide more direct risk control and also more operational flexibility by allowing looser controls in areas unimportant to risk. Implementation of such a control system will result in a safer plant. Strategies for configuration control can be included in planning and reviewing test and maintenance strategies to avoid having configurations that increase risk. These control strategies also can be implemented using on-line computer systems. A properly functioning configuration control system could replace parts of technical specifications.

Configuration control is important because all plant risks, all accidents and incidents, and all accident precursors arise because of critical configurations which have occurred. If configurations were managed so that critical, high-risk configurations did not occur, then risks would be small and no accidents or incidents would occur. In risk-based configuration control, the focus is on safety systems which generally involve standby components. Configuration control objectives become difficult because the status of a standby component is often not apparent unless it is tested.

Realizing the importance of configuration control in safe operation of nuclear power plants and the advances in probabilistic safety assessment (PSA) technologies, the concept of risk-based configuration control has received wide interest[1-4]. In the United States, the Nuclear Regulatory Commission (NRC) and the nuclear industry are currently studying the feasibility of such a system. A similar system, called Essential Systems Status Monitor (ESSM), is in operation at the Heysham Nuclear Plant in Great Britain[2].

A study of configuration risk and the role of current Technical Specifications in controlling the configuration risk for a U.S. nuclear power plant[1] identified the factors that determine the safety or risk impact of configuration occurrence. In this paper, we discuss the strategies and criteria for risk-based configuration control. The information and the tools needed in implementing configuration control are also discussed. We also discuss the risk-based calculation requirements in implementing the features relating to configuration control. Risk modeling requirements and uses of plant-specific data in configuration control approaches are not discussed here, but are presented in Reference 1. Also discussed in Reference 1 are alternative criteria for determination of allowed durations (similar to allowed outage times in current Technical Specifications) for different configurations.

2. OBJECTIVES OF RISK-BASED CONFIGURATION CONTROL

The objectives of risk-based configuration control are to manage configurations in such a way that the configuration risk is properly controlled. Thus, the criteria here involve controlling some measure of risk. Risk-based configuration control can take many forms. Component configurations can be managed to control component unavailabilities. System configurations can be managed to control system unavailabilities. Safety function configurations can be managed to control safety function unavailabilities. Finally, plant configurations can be managed to control accident-sequence frequencies, core-damage frequencies, or public-health risks.

In addition to the options for focusing on components, systems, functions, or plant states, there are other options for risk-based configuration management. The objective can be to control risk or unavailability rather precisely using plant-specific system models or plant models. In controlling these risk measures, a risk-based configuration control system must define risk-significant configurations and forewarn about component statuses which can result in significant risk levels, e.g., core-melt frequency

levels. As such, the system must define strategies to identify and control these critical configurations. Figure 1 illustrates the basic objectives of risk-based configuration management.

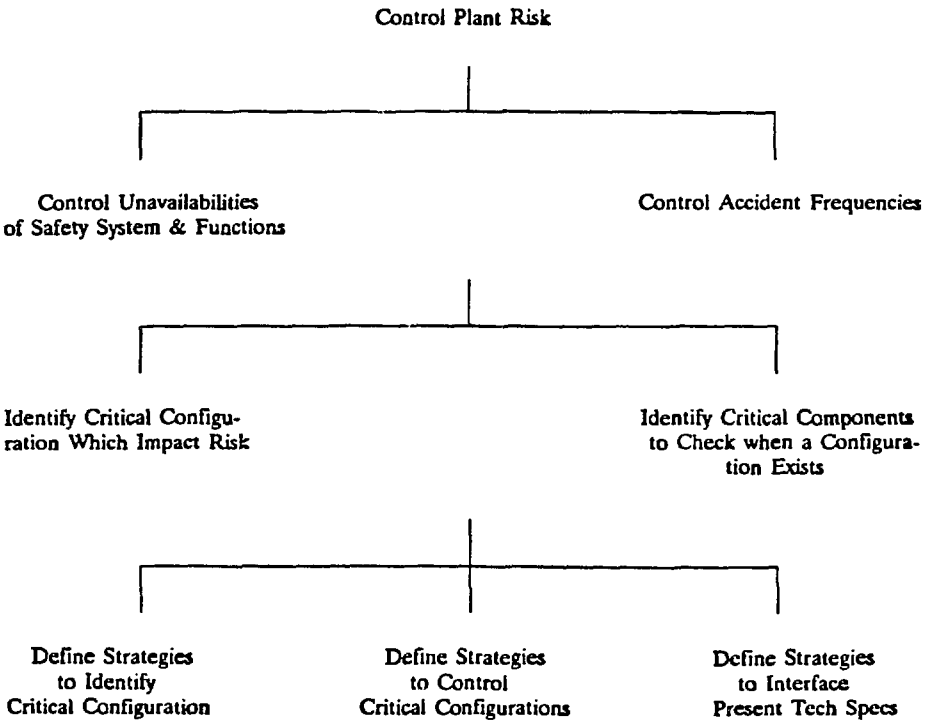

Figure 1. Basic objectives of risk-based configuration management

3. ANALYSIS OF CONFIGURATION RISK CHARACTERISTICS

Probabilistic safety analyses (PSA) have especially shown the importance of configuration management by identifying the critical configurations which cause high system unavailabilities, high core-melt frequency, and high public risks. Critical, high-risk configurations involve critical, safety-important components which are simultaneously down because of either failure, maintenance, or testing[1]. In PSA terminology, the components which are down are critical when they are all in the same minimal cut set. More generally, the components which are simultaneously down are critical because they cause one or more safety functions to be lost or significantly degraded.

PSA evaluations specifically tell us that the risk impact or safety impact of a configuration depends upon four factors:

1. the configuration components which are simultaneously down,
2. the back-up components which are known to be up,
3. the duration of time the configuration exists (the outage time), and
4. the frequency at which the configuration occurs.

The first factor determines the loss of capability. The second factor determines the alternative components which are available to make up the lost capability. The third factor determines the integrated risk impact and the last factor determines the accumulated risk impact which occurs from the configuration over a period.

4. DEVELOPMENT OF RISK-BASED CONFIGURATION CONTROL SYSTEM

The results of configuration risk analyses show the importance of configuration control by identifying the critical configurations which cause high system unavailabilities, high core-melt frequency and consequently, high public risk. As stated, in developing a risk-based configuration control system, the important objective is to control risk and safety. However, the other important objective is to operate efficiently and to make effective use of available resources. With these objectives, the basic focal points of configuration control and the subtopics under each focal point are defined (Figure 2). These basic focal points parallel the four factors identified above. Each of these focal points is discussed in detail below.

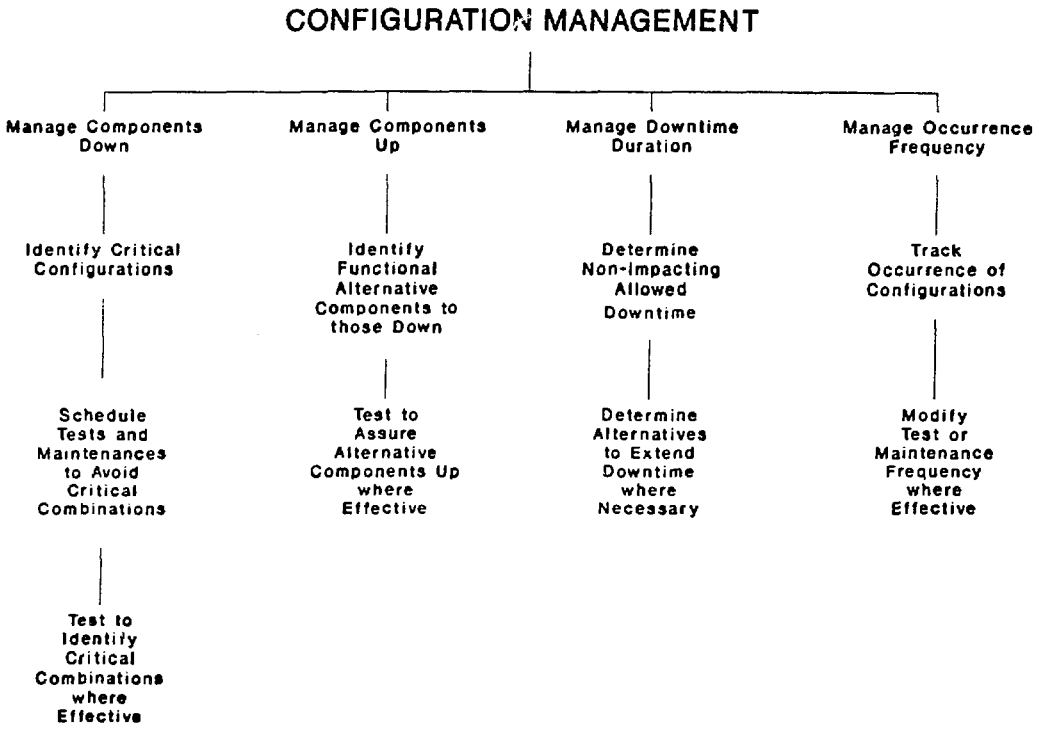

Figure 2. Focal points and subtopics of configuration management

4.1 Managing Downed Components

Managing downed components involves importance considerations, scheduling considerations, and test considerations. With regard to importance considerations, management of the downed components involves knowing which combinations of components cause large risk impacts if they are down simultaneously. The critical component combinations can be determined from the plant PSA or from plant logic schematics using risk considerations. The critical component combinations are, basically, a function of the plant design.

With regard to scheduling considerations, managing downed components involves scheduling maintenances and tests so that critical combinations of components are not down at the same time. In preparing the surveillance schedules, or the master surveillance schedule, operational considerations and resource constraints are important considerations; however, avoiding critical combinations also becomes an important objective.

When components are in standby, it is not always apparent which are down. When failures of components are discovered, then additional components may need to be tested to assure that they are also not down so forming a critical combination of downed components. Thus, management also involves testing after failure to assure that there are no such critical configurations.

These test-after-failure considerations involve knowing which additional components, if also down, constitute a critical configuration. These additional components can be called critical complements, since they complement the already downed components to form critical downed configurations. Furthermore, test-after-failure considerations involve knowing whether tests of these complementing components are feasible and effective in determining their failure status.

In summary, management of downed components involves:

1. Knowledge of critical component combinations,

2. scheduling of maintenances and tests to avoid the critical combinations, and

3. knowledge of critical complementing components and effective tests which can be performed on them.

4.2 Managing Back-Up Components

Managing back-up components involves knowledge and testing considerations. To counter the loss of capability from components being down, other components can be checked to assure they are up. Management of back-up components involves knowing which components can carry out the same functions as those components which are down. For a given configuration of downed components, the back-up components are determined from a PSA model or from a plant schematic using risk considerations.

Management also involves knowing whether tests or inspections can be effectively performed on the back-up components to assure they are operational. This knowledge is obtained from plant operational and test considerations, as well as reliability and risk considerations.

Thus, management of back-up components involves:

1. Knowledge of the back-up components for given configurations of downed components, and

2. knowledge of effective tests which can assure the operation of the back-up components.

4.3 Managing Outage Time

Configuration management involves knowing how long a configuration can exist before the risk incurred becomes significant. Sometimes configurations cannot be avoided because of failures or

corrective maintenances which must be performed. Configuration management involves knowing how much time exists to complete the repairs or maintenances before the risk impact becomes significant.

The allowable outage time for a given configuration is an extension of the allowable outage times for individual components as defined by tech specs. Configuration management involves determining allowed outage times for individual and for configurations of downed components. Allowable outage times for multiple downed components can be quite different from those for single components because of their different impacts on risk. The allowable outage time for single and for multiple downed components should have a sound risk basis which not only controls risk but can also reduce burden by allowing larger outage times for those unimportant configurations. All of these outage times can be determined from the plant PSA (or equivalent), with operational and resource considerations.

Management of outage times also involves knowing the alternatives that can extend the allowed outage time without increasing risk significantly. These alternatives can reduce burden when necessary and basically involve testing back-up components to assure they are up, where tests are effective. The knowledge of the back-up components and the effective tests to carry out is part of the management of the back-up components.

Thus, the management of configuration time duration involves:

1. Knowledge of the allowed outage time for a configuration so that there is insignificant impact on risk, and

2. knowledge of the alternatives for extending the allowed outage time.

4.4 Managing Frequency

Finally, configuration management involves controlling the frequency at which configurations, especially risk significant configurations, occur. Controlling the frequency, in turn, involves tracking the frequency of occurrence of configurations and modifying procedures and testing where necessary.

Tracking the frequency of occurrence can be carried out through data collection and data analyses, including the construction of appropriate indicators. Readjusting procedures and testing to modify the frequency involves having criteria, and identifying the relationships between the frequency and testing and maintenance procedures. Modifying the procedures can involve either tightening or loosening the schedules. Operation considerations and the plant PSA can be used for these applications.

In summary, management of configuration frequencies involves:

1. Tracking the frequency, and
2. controlling the frequency through appropriate procedure changes.

4.5 Information and Tools Requirements

Information and tools requirements for configuration management are presented pictionally in Figures 3 and 4. Figure 3 illustrates the information requirements for configuration management which involve plant operational information and PSA information. Finally, Figure 4 presents the techniques for configuration managements where each horizontal line presents one alternative for configuration management. The first alternative will be to develop lists of critical configurations to and, using PSA/plant information as a tool to manage downed components; lists of functional alternate components

for downed component configurations; lists of allowed downtime durations to manage impact from configuration occurrences, and finally, providing surveillance frequencies for components as a function of configuration occurrence frequency. Another alternative will be to develop criteria for each of the factors that require actions by plant operational staff; and finally, on-line computer programs can be developed which can provide the needed advice and options for plant operating staff.

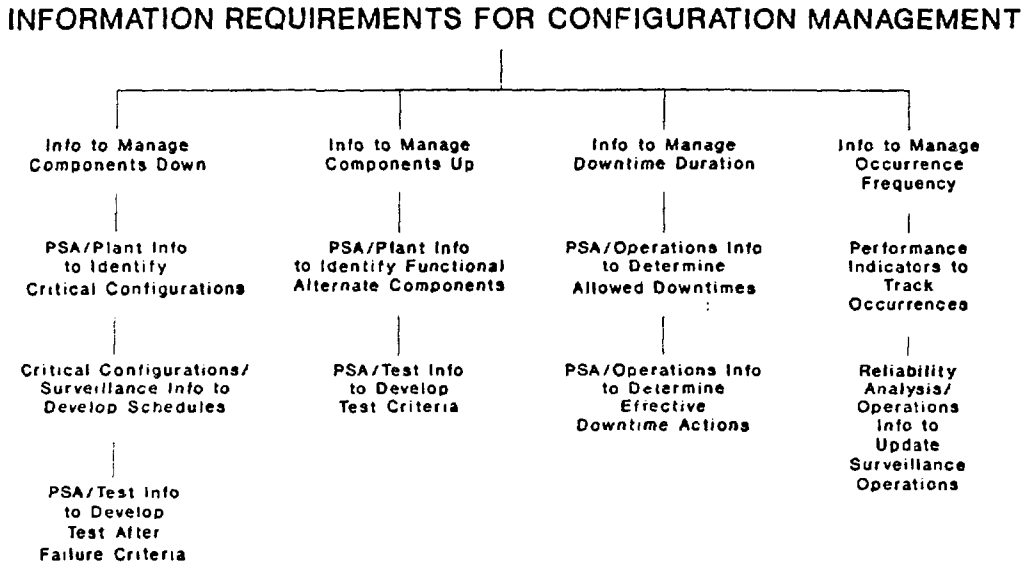

Figure 3. Information requirements for configuration management

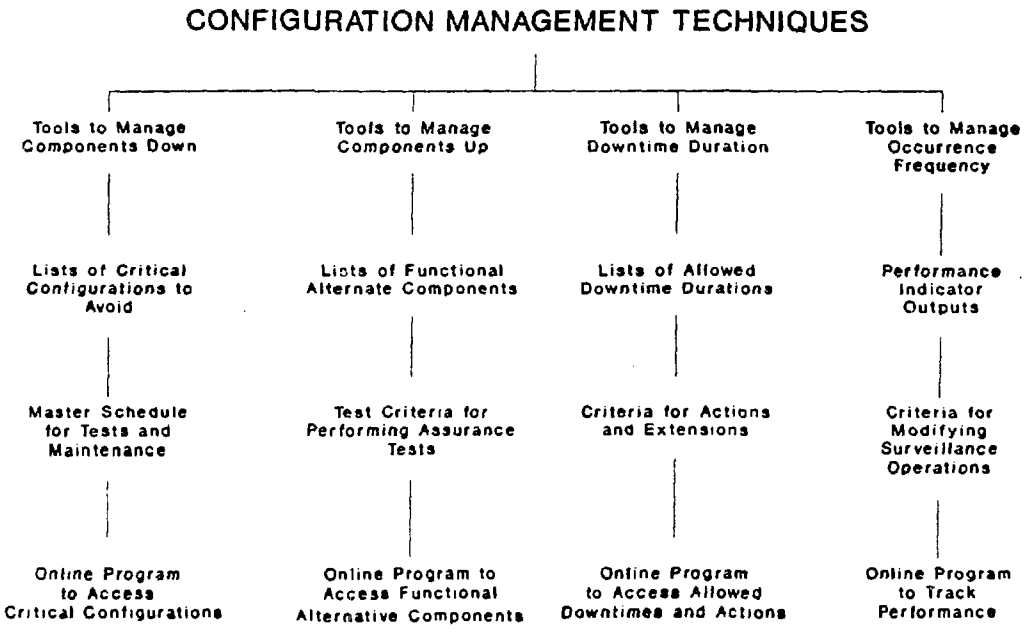

Figure 4. Techniques for configuration management

5. RISK-BASED CONFIGURATION CALCULATION REQUIREMENTS

To achieve the potential benefits of a risk-based configuration control system, the system to be built should be able to perform the necessary risk calculations that represent the risk level at the plant caused by component outages. The primary requirement for the model is the ability to calculate the increased level of risk resulting from various configuration changes. During plant operation, various configurations result because some components are down for testing while others are down for maintenance. Also, when certain components are down, other components can be reconfigured to compensate or to allow for testing and maintenance. Here, we define the requirements for risk-based calculation for quantifying the risk impact of configurations.

Risk-based configuration calculations refer to the evaluations to calculate the core-melt frequency (and other risk measures) for given plant configurations. By calculating the core-melt frequency (CMF) for given configurations and tracking it with time, the configuration risk can be more effectively controlled. As discussed, the duration for which the configuration can exist can then be limited, or the CMF level associated with the configuration can be reduced. Furthermore, maintenances and tests can be scheduled to avoid configurations which cause large increases in CMF. To calculate the core-melt frequency and probability contributions for given configurations, the risk calculations, including the associated software, must have certain capabilities. Table 1 lists the capabilities that would be useful for risk-based configuration calculations, with the potential criteria grouped according to specific capability areas. What, in the authors' opinion, represent sufficient, minimal capabilities are indicated with an asterisk (*).

Table 1. Criteria for the Capabilities of Risk-Based Configuration Calculation

Capabilities to Calculate Risk Levels

1.* General system models (e.g., fault trees or GO system models) or general plant models (e.g., event trees) can be used to determine the risk level.

2.* There is negligible error in determining the risk level due to truncation of minimal cut sets.

3.* In determining the risk level for a given configuration of components being down, other components being up or being reconfigured are accounted for.

4.* In determining the risk level for a given configuration, the tests that can cause transients including balance of plant (BOP) tests are taken into account.

5. In determining the risk level for a given configuration, the times at which other components were last tested or were last known to be up are incorporated.

6. In determining the risk level for a given configuration, the uncertainties in the evaluations are accounted for or bounded.

Table 1. Criteria for the Capabilities of Risk-Based Configuration Calculation (Cont'd)

Capabilities to Calculate Accumulated Risks

1.* The accumulated risk for a given duration of a configuration is determined.

2. The uncertainty in the accumulated risk for a given configuration duration is accounted for or bounded.

Capabilities to Calculate an Allowed Duration Time for a Given Configuration

1.* The allowed duration for any given configuration is determined using given criteria.

2. The uncertainty in the allowed duration for a given configuration is accounted for or bounded.

Capabilities to Calculate Risk Contributors

1.* The components that are important contributors to risk for a given configuration are determined.

Capabilities to Identify Other Components to Check

1.* For a given configuration, priorities are shown for checking alternative success paths (by checking other components to assure they are operable).

2. For a given configuration, the new allowed duration time for the configuration is determined when given components are checked to assure they are up.

Capabilities to Compare with Present Technical Specifications

1. For a given configuration, present technical specification requirements are given as a basis for comparison.

Capabilities to Incorporate Plant-Specific History

1. Past plant history, including failures, downtimes, and human errors which have occurred are input to update the evaluation.

2. The past occurrences of given configurations are retained to provide the frequencies at which given configurations have occurred.

3. The past accumulations for given configurations and their duration which have occurred are retained to provide input for allowed duration times based on accumulated risks.

Capabilities to Perform Real-Time Evaluations

1. For real-time evaluations, the risk levels and other information are calculated for each configuration in a timely fashion, e.g., less than several minutes.

Table 1. Criteria for the Capabilities of Risk-Based Configuration Calculation (Cont'd)

Capabilities to Perform Auditing Evaluations

1. For auditing evaluations, the risk levels and other information are calculated in an effective manner using plant history and accounting for recorded overlaps of component downtimes.

Capabilities to Provide Meaningful Information to the User

1.* Meaningful information is provided to different types of users. For the operating personnel, information is provided on when to take actions. For the engineering personnel, information is provided on the calculated risks and the risk contributors.

---

*Indicates the authors' opinion of minimal calculation capabilities for initial use.

6. SUMMARY

This paper presents considerations in outlining a risk-based configuration control system as applicable to nuclear power plants to control component outages caused by testing, maintenance, or failure. A PSA-based evaluation was performed to analyze the configuration risk contributions and was directed at defining approaches for such a system. Using the results and insights obtained, guidance for developing an effective risk-based configuration control system is presented.

7. REFERENCES

1. Samanta, P.K., Vesely, W.E., and Kim, I.S., "Study of Operational Risk-Based Configuration Control," NUREG/CR-5641, BNL-NUREG-52261, Brookhaven National Laboratory, to be published, 1991.

2. Horne, B.E., "The Introduction of Probabilistic Evaluation into the Operation of CEGB NPP Using the ESSM Facility," ANS/ENS International Topical Meeting on Probabilistic Safety Assessment and Risk Management, Zurich, Switzerland, September 1987.

3. Nordic Liaison Committee for Atomic Energy, "Optimization of Technical Specifications by Use of Probabilisitic Methods - a Nordic Perspective," 1985-1989, Ed. by K. Laakso, NKA/RAS-450, November 1989.

4. IAEA Consultants' Report, Use of reliability methods and probabilisitic safety assessment to improve NPPs operational limits and conditions, Vienna, Austria, Draft Report, December 1989.

DISCLAIMER