Conf-930116--11
BNL-NUREG-48100

RISK-BASED CONFIGURATION CONTROL: APPLICATION OF PSA IN IMPROVING TECHNICAL SPECIFICATIONS AND OPERATIONAL SAFETY*

BNL-NUREG--48100

DE93 002938

P.K. Samanta, I.S. Kim, and W.E. Vesely†
Brookhaven National Laboratory
Upton, New York 11973

†Science Applications International Corporation
Dublin, Ohio 43017

ABSTRACT

Risk-based configuration control is the management of component configurations using a risk perspective to control risk and assure safety. A configuration, as used here, is a set of component operability statuses that define the state of a nuclear power plant. 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, to minimize the risk from components being unavailable, becomes difficult, because the status of a standby safety system component is often not apparent unless it is tested. Controlling plant configuration from a risk-perspective can provide more direct risk control and also more operational flexibility by allowing looser controls in areas unimportant to risk. Risk-based configuration control approaches can be used to replace parts of nuclear power plant Technical Specifications. With the advances in probabilistic safety assessment (PSA) technology, such approaches to improve Technical Specifications and operational safety are feasible. In this paper, we present an analysis of configuration risks, and a framework for risk-based configuration control to achieve the desired control of risk-significant configurations during plant operation.

I. 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 control in areas unimportant to risk.

Currently, in nuclear power plants, individual component outages are controlled (by allowed outage times defined in Technical Specifications) and simultaneous outages of certain redundant equipment are forbidden. With the advances in probabilistic risk assessment (PSA) technology, risk-significant plant configurations resulting from equipment failures or outages due to test or maintenance can be more directly controlled. This is important because all plant risks, all accidents and incidents, and all accident precursors arise because of critical configurations which have occurred. Configuration control becomes difficult because the status of standby equipment is often not apparent unless it is tested.

The use of a PSA to assure control of plant configurations during operation of nuclear power plants will be a significant application of this methodology to assure operational safety. In this paper we present an analysis of configuration risks using a PSA, and then, define a framework for risk-based configuration control. As part of a study of configuration risk and the role of current Technical Specifications in controlling the configuration risk for a nuclear power plant, other aspects for implementation of such an approach were also studied.[1] They include risk-based calculation requirement in implementing the features relating to configuration control, risk modeling requirements, uses of plant-specific data, and criteria consideration for control of configuration risk impact.

With the advances in PSA technologies and success in applying them to improve Technical Specifications (TS), the concept of risk-based configuration control has received wide interest[1-4] in recent years. Using a similar concept, called Essential Systems Status Monitor (ESSM), is in operation at the Heysham Nuclear plant in the United Kingdom.[2] However, the institutional and technical problems associated with the use of such an approach as a "risk monitor" or "risk-meter" have been addressed by others.[5]

II. OBJECTIVES OF RISK-BASED CONFIGURATION CONTROL

The objectives of risk-based configuration control are to manage configurations so that their risk impacts will be properly controlled. Thus, the criteria here involve controlling

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

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 control. 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 control.

2. the core-melt frequency levels associated with the configurations and the expected frequencies of their occurrences.

3. the nature of combinations of the components that give rise to these configurations, and

4. the expected core-melt probability contributions associated with the configurations, and those allowed under present technical specifications.

A systematic methodology was used to identify the core-melt frequency (CMF) significant configurations and to evaluate the above parameters for a specific plant.[1]

In identifying the CMF-significant configurations using a PSA, we are interested in grouping the configurations according to their impacts on core-melt frequency. As such, our interest is not on obtaining a precise CMF, but rather on the level of fluctuation in the CMF. Therefore, the quantification performed does not include any formal methods to

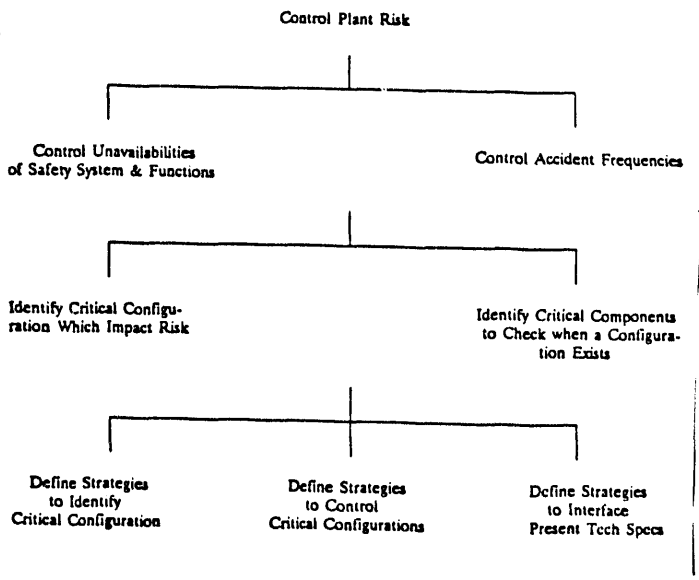

Figure 1. Basic objectives of risk-based configuration control

III. ANALYSIS OF CONFIGURATION RISK CHARACTERISTICS

Using a plant-specific PSA, the characteristics of configuration contributions to core-melt frequency and core-melt probability were analyzed. The aspects of configuration contributions analyzed are:

1. the identification of core-melt frequency significant configurations that may occur during power operation.

assess statistical data and/or model uncertainties. As will be evident later, the results are used as "indicators" to identify the fluctuations so that corrective actions can be undertaken to improve the operational safety of the plant.

The CMF-significant configurations identified in the plant are classified as single, double, triple, and quadruple configurations depending upon the number of components involved. For each of these configurations, the CMF level and the expected frequency of occurrence, and the yearly risk,

which addresses the time period core-melt probability contribution, were determined.

Figure 2 shows how the important characteristics of a configuration, i.e., the CMF level, the expected frequency of occurrence, and the yearly risk, change as the number of outage components increase. The trend of change is illustrated using typical configurations; e.g., the outage of emergency service water pump A is used as a representative single configuration.

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

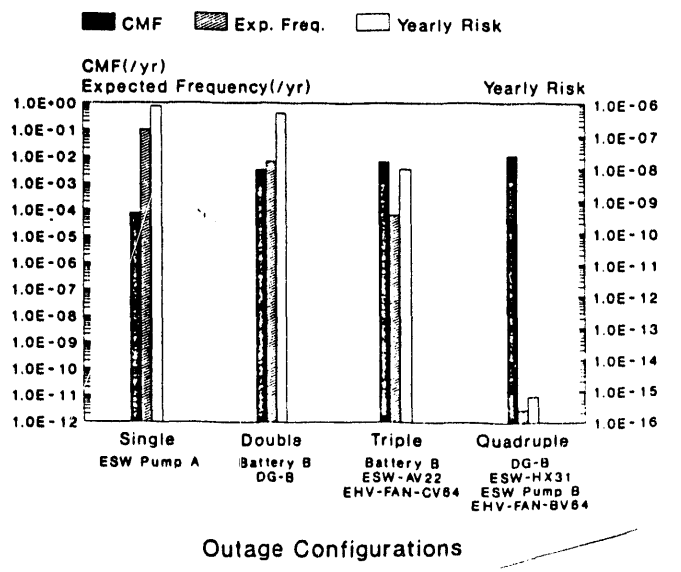

Figure 2. Characteristics of configuration risks

As more components go down, the CMF level, i.e., the pointwise risk level, increases. On the other hand, the expected frequency of configuration occurrences sharply drops as the number of outage components increases.

However, the yearly risk, i.e., the risk expected to be incurred due to the expected occurrences of the configuration over a year, also decreases despite the increase in the pointwise risk level. The decrease in the yearly risk as the configuration involves more components is due to the fact that the expected frequency of configuration occurrences sharply decreases as the number of outage components increases.

In summary, 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,

determines the accumulated risk impact which occurs from the configuration over a period.

IV. 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 and high core-melt frequency. 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 3). These basic focal points parallel the four factors identified above. Each of these focal points is discussed in detail below.

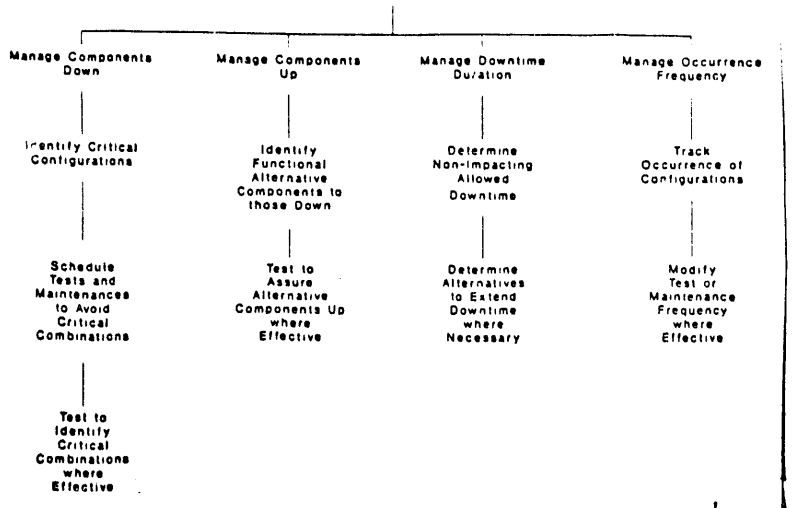

Figure 3. Focal points and subtopics of configuration control

A. Managing Down 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 complementary 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 complementary components and effective tests which can be performed on them.

B. Managing Back-Up Components

Managing back-up components involves knowledge of available components 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.

C. Managing Outage Time

Configuration control 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 control 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 control 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 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 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 duration involves:

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

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

D. 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.

E. Tools Requirements

Figure 4 presents the techniques for configuration control where each horizontal line presents one alternative for configuration control. The first alternative will be to develop lists of critical configurations to avoid 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.

V. DIFFERENCES AND INTERFACES WITH EXISTING TECH SPEC REQUIREMENTS

There are significant differences in achieving operational safety, using a risk-based configuration control approach, compared to that of existing Technical Specification (TS) requirements. These major differences are summarized below.

1. Control of multiple component outages - existing TS focuses on individual component outages, which does not necessarily provide the appropriate risk control and may be resulting in unnecessary control of risk-unimportant components. Focussing on control of risk-critical configurations will enhance risk control due to equipment failures and outages. This is also expected to result in relaxation of a number of existing requirements which may be considered unnecessarily burdensome.

2. Assuring alternate success path - existing TS typically requires change of plant modes (i.e., shutdown from power operation). However, such actions do not necessarily assure safe operation and in some situations may be undesirable. Assuring alternate success paths through testing can define an alternative, appropriate operator role in such situations, and will reduce unnecessary change of plant modes.

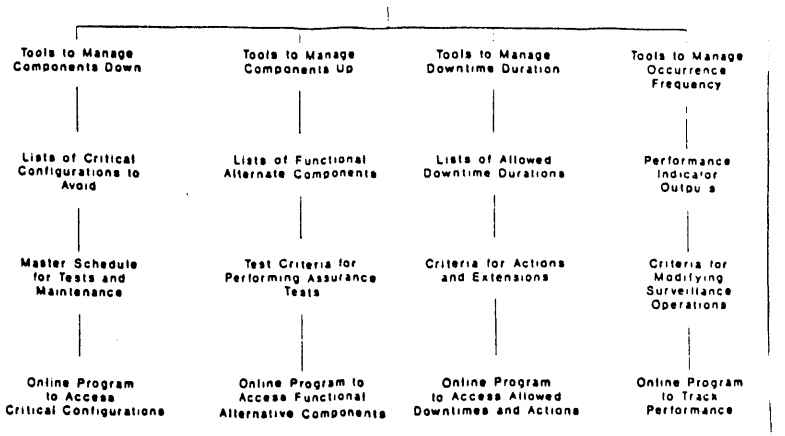

Figure 4. Techniques for configuration management

3. Surveillance directed to detect and control configuration risk - existing TS requires fixed frequency surveillances. In such an approach, risk-significant configurations may remain undetected. Surveillance requirements can be modified to detect risk-significant configurations, and at the same time, to decrease the total number of surveillances required.

VI. SUMMARY

This paper presents considerations in outlining a risk-based configuration control approach 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. The application of PSA in such a manner will improve the risk-effectiveness of Technical Specifications and the operational safety.

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, August 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 Probabilistic Methods - a Nordic Perspective," 1985-1989, Ed. by K. Laakso, NKA/RAS-450, November 1989.

4. Report of a Consultants' Meeting, Use of reliability methods and probabilistic safety assessment to improve operational limits and conditions, Vienna, Austria, published in IAEA-TECDOC-599, Report of a Technical Committee Meeting held in Vienna, 18-22 June 1990, published April 1991.

5. J.P. Sursock and D. True, EPRI Perspectives on the Use of Risk-Based Technical Specifications in Controlling Plant Operations, IAEA-TECDOC-599, Report of a Technical Committee Meeting held in Vienna, 18-22 June 1990, published April 1991.

END

DATE FILMED

2 / 26 / 93