

Considerations for Adopting Risk Informed Techniques for Electrical Surveillance Testing (Future Revision of IEEE 338)

Glen E. Schinzel

*STP Nuclear Operating Company.
Wadsworth, TX 77483
GESchinzel@stpegs.com*

David A. Horvath

*Advent Engineering Services, Inc.
Ann Arbor, MI 48106-0555
DAH@adventengineering.com*

Theodore J. Riccio

*STP Nuclear Operating Company
Wadsworth, TX 77483
tjriccio@stpegs.com*

George A. Ballassi

*General Dynamics / Electric Boat
Groton, CT 06340
GBALLASS@ebmail.gdeb.com*

Abstract - *As the electrical deregulation saga in the US continues to unfold, economic pressures for nuclear power stations to produce electricity at lower costs will continue to increase. The use of risk informed approaches has been both identified and encouraged as an option to improve management of station resources more effectively and this technique has seen notable successes in the areas of in-service inspection and testing. Because of those successes, IEEE's Nuclear Power Engineering Committee has directed its Working Group 3.1 to evaluate integration of risk informed approaches into its electrical testing standard - IEEE Std 338. This paper will report on considerations for adopting similar risk-based techniques to fine-tune testing intervals for electrical and I&C equipment at nuclear power stations. These approaches will be based on techniques successfully employed by STP Nuclear Operating Company at the South Texas Project Electric Generating Station in Wadsworth, Texas.*

1. INTRODUCTION

IEEE Std 338 "Standard Criteria for Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems" provides design and operational criteria for the performance of periodic testing as part of the surveillance program of nuclear power generating station safety systems. The scope of periodic testing covered in the standard consists of functional tests and checks, calibration verification, and time response measurements, as required, to verify that the safety system performs its defined safety function. The system status, associated system documentation, test intervals, and test procedures during operation are also addressed. Maintenance is not covered by this document. IEEE Std 338 was last revised in 1987.

In June of 2001 the IEEE Standards Board approved the recommendation of the Nuclear Power Engineering Committee (NPEC) of IEEE's Power Engineering Society and directed NPEC to sponsor an update and revision of IEEE Std 338.

NPEC's Working Group 3.1 was assigned to this task. The project authorization directs that the revised standard:

1. Develop and provide guidance on optimizing periodic test intervals based on reliability, availability, and risk-informed approaches,
2. Review and consider "lessons learned" from implementation of risk-informed approaches in other standards and regulatory activities, and
3. Review and consider any other feedback obtained from performers of periodic testing and users of IEEE Std 338-1987 and related documents.

This paper will report on the working group's intended approach for incorporating risk informed considerations into the determination and/or refinement of testing approaches and frequencies and solicit feedback from conference attendees. The working group hopes to use techniques successfully employed by STP Nuclear Operating Company at the South Texas Project Electric Generating Station in Wadsworth, Texas for similar risk-informed ISI Program improvement efforts as well as take advantage of relevant

testing considerations described in related international standards.

Note that because of the multi-disciplinary nature of this paper, the terms component [of a system] and equipment will be used interchangeably and will include electrical equipment, instruments, and controls.

2. PRESENT IEEE STD 338 APPROACH

IEEE Std 338¹ presently requires sufficient functional testing to assure safety systems and equipment will meet performance specifications. Safety (Class 1E) system testing intervals are to be determined from the following considerations as appropriate:

1. Regulatory requirements,
2. Scheduled plant operating cycle,
3. Plant safety considerations,
4. Manpower and ALARA considerations, and
5. Equipment degradation caused by testing.

The testing intervals for components of safety systems are to be determined using the following as appropriate:

1. Manufacturer's recommendations / requirements;
2. Historical experience of similar equipment (for example, failure rate data such as information from reliability data banks, preoperational testing, and related quality information);
3. Equipment qualification reports and analyses; and
4. Failure data (e.g., mean time to repair, mean time to failure, and historical data).

Periodic reevaluation of the testing interval is also required to ensure that the equipment continues to be fully operational. Reevaluations are to consider the following:

1. Equipment performance history, particularly failure rates and failure rate increases,
2. Necessary corrective actions,
3. Comparison to equipment in other plants or similar environments, and
4. Plant design changes.

As can be seen above, functional testing and interval determination are presently based on system design configuration, and empirical equipment performance data determined either from actual use, qualification testing, or similar plant or conditions. All systems and equipment receive equal consideration by the Standard regardless of function or risk.

3. IN-SERVICE INSPECTION RISK INFORMED APPLICATION

The IEEE Std 338 revision effort is required to consider "lessons learned" from implementation of risk-informed approaches in other standards and regulatory activities. One example for consideration is its application to the in-service inspections required by Section XI of the ASME Boiler and

Pressure and Vessel Code. In this area, risk informed approaches have resulted in both substantial savings in time and money as well as improvements in focus on overall safety.

The first five steps of an approach developed for Westinghouse plants² are summarized below:

1. The piping system scope and segments are defined. A full scope program considers all fluid systems within the scope of the plant's PRA/PSA. The systems are divided into piping segments for which a failure results in the same consequence.
2. Piping failure consequences are evaluated. Each segment is evaluated for direct and indirect effects both with and without operator action to mitigate a piping failure at that segment. The postulated consequences of the failure are used to calculate the pressure boundary failure risk. Groupings of segments help to reduce the number of PRA runs needed.
3. Piping failure probability is assessed. For each segment grouping, an engineering team reviews industry experience, plant layout, materials, operating conditions, and plant experience, and identifies potential failure modes and causes. The team then uses ISI-specific PRA software to calculate probabilities for leaks (through wall cracks), disabling leaks, and/or full breaks.
4. Risk is evaluated. The effect on core damage frequency (CDF) and large early release frequency (LERF) is determined by using conventional approaches such as by calculating Risk Achievement Worth.
5. Expert Panel finalizes categorization. Expert panel reviews and completes categorizations as to level of safety significance by considering deterministic as well as risk based factors.

All of these steps have analogous counterparts for electrical and I&C systems.

4. INTERNATIONAL STANDARDS APPROACH

A second consideration is the approach offered to countries under the auspices of the IAEA (primarily European Union countries) and the set of standards developed by the International Electrotechnical Commission (IEC). IEC 1226-1993 "Nuclear Power Plants – Instrumentation and Control Systems Important for Safety – Classification"³ states that the IAEA recommends that I&C systems be placed in categories according to importance to safety. One of the considerations given for making this determination is the probability and potential severity of consequences of postulated initiating events if the I&C system fails.

The purpose of IEC 1226 is to establish a method for classification of certain I&C and equipment (those providing an information and command function) into categories that designate importance to safety. Four categories are defined.

Category A is for those equipment items that play a principal role in achieving and maintaining safety. The role includes both automatic and manual actions. A Category A function is essential to preventing a postulated initiating event [basic event] from leading to a serious sequence of events. Examples are reactor protection systems, safety actuation systems and their support features, and key instruments and displays to permit preplanned operator actions that are defined in the nuclear power plant's operating instructions and that are required to ensure plant safety.

Category B equipment items play a complementary role to Category A. A Category B function may help avoid the need for a Category A function or may help improve the mitigative action of Category A. Also a Category B function failure may initiate or worsen a postulated initiating event. Examples are accident prevention interlocks, fire suppression systems, control room data processing, fuel handling system interlocks, and instruments monitoring the performance of individual safety systems.

Category C equipment items play an auxiliary or indirect role in achieving or maintaining nuclear power plant safety.

They are part of the total response but not directly involved in mitigating the physical consequences of an accident sequence. Examples are alarm systems, radwaste system monitoring, access control systems, and emergency communication systems.

The final category is "unclassified" and represents everything else.

Although these four categories do not entirely result from a risk assessment evaluation, some of the risk and consequence based considerations applied to Categories A & B may be useful to fine tuning or validating approaches to be offered for consideration in the future revision of IEEE Std 338.

IEC 671 "Periodic Tests and Monitoring of the Protection System of Nuclear Reactors"⁴ states that periodic testing should contribute, by means of detection of failures, to the achievement of the desired system availability where availability is defined as the probability that a system or assembly will be operational at a randomly selected future instant in time. It also states that test intervals should be chosen as a function of the availability goal for the system. The availability goals and test intervals are to be based on mathematical relations involving type of logic, failure-rate data, test duration, and permissible system unavailability. Such considerations may be applied to US electrical and I&C equipment determined to be of high safety significance as described below.

5. USEFUL PRA/PSA DETERMINED CHARACTERIZATIONS

Although the considerations described above will still apply to the determination of testing intervals, it is desired that some quantitative risk-based criterion or criteria be available to allow refinement based on safety significance of component. Two useful characterizations readily calculated from PRA/PSA modeling are Fussell-Vesely (FV) and Risk Achievement Worth (RAW).

FV for a basic event is defined as the fractional change in the core damage frequency (CDF) when the basic event probability is set to zero. The basic event of interest is the failure of an electrical / I&C component. Thus the FV is a measure of how sensitive the degradation or failure of a component is to the CDF. FV depends both on the component's reliability and the effectiveness of the plant's defense in depth for that particular component. Thus FV will be high if the component has low reliability or if the plant has limited defense in depth to mitigate the detrimental effects of the component's failure or poor performance.

RAW for a basic event is defined as the ratio of the CDF when the probability for the component's failure is set to unity to the baseline value of CDF. The value of RAW shows the relative importance of the component when failed or "out of service." RAW depends strongly on the plant's design configuration (defense in depth) but very little on the component's reliability or availability.

FV gives the combined effect of a component being down and the likelihood of this happening. RAW only gives the effect of the component being down.

6. PROPOSED NEW APPROACH FOR TESTING

A risk informed approach to determining surveillance testing approaches and frequencies would require a documented basis for identifying what components are important (safety significant) and what components are not important (not safety significant). Once applied, resources can be appropriately focused on safety significant components. This approach results in reduced burden for the power plant and the regulator and improved overall safety focus

Techniques employed at the South Texas Project for ISI and other activities are being considered for adoption in IEEE Std 338 for electrical and I&C surveillance testing frequency determination.

A summary of how a similar approach would be applied for electrical and I&C component testing is summarized below.

1. All PRA/PSA electrical and I&C components are grouped initially into one of four categories according to risk as follows:
 High Safety Significance (HSS):
 RAW greater or equal to 100.0, or
 FV greater or equal to 0.01, or
 FV greater or equal to 0.005 and RAW greater or equal to 2.0
 Medium Safety Significance (MSS):
 FV greater or equal to 0.005 and RAW less than 2.0, or
 FV less than 0.005 and RAW greater than 2.0
 Low Safety Significance (LSS):
 FV less than 0.005 and RAW less than 2.0
 Not Risk Significant (NRS) is everything else.
2. Risk-informed means that other conventional and deterministic factors remain a part of the categorization decision. The risk based groupings resulting from Step 1 are evaluated with respect to manufacturer recommendations, Environmental Qualification Program requirements, other plant-specific needs, industry lessons learned, and other factors currently in IEEE 338 and described above.
3. Some form of a verification or validation of the resulting groupings is suggested.
4. HSS and MSS are combined and classified as safety significant. LSS and NRS are considered not safety significant.
5. Testing intervals are applied to the safety significant components based on mean time between failures, reasonable margin, and satisfying any established availability goals. It is necessary to assure that the basic event probability as affected by the test interval time (which represents time available for possible hidden failures to occur) does not result in a detrimental increase in CDF or LERF.
6. For components newly classified as not safety significant, limited testing may be imposed to satisfy the minimal design functional requirements of the component. In the absence of other considerations (such as licensing commitments) significantly reduced testing requirements may be justified. In certain cases, a run-to-failure methodology could be adopted if determined to be the best approach from a safety and economic determination. If a component fails when demanded, the impact to safety is negligible.

Note that the above approach may result in some Class 1E components being categorized as not safety significant and some non-Class 1E components now being categorized as safety significant. The result may also support an

analytical basis for an Operating License Technical Specification change or for an exemption from Maintenance Rule commitments... It is also hoped that this new approach will be able to take credit for the self-diagnostics now available in digital systems and the resulting increased reliability and high FV.

Why is it acceptable to categorize components and treat them differently from original Class 1E determinations? Safety-related and nonsafety related component failure rates have been found to be generally the same. Also commercial practices have been demonstrated to be acceptable through improved power plant capability and reliability. Thus, it is expected that the least important components will continue to function when demanded. And even if a low safety significance component were to fail, the result would be little to no impact on safety.

7. CONCLUSION

A promising approach for optimizing surveillance test approaches and intervals for electrical and I&C components based on safety significance of the components is being considered in the form of a revision to IEEE Std 338. It is believed that use of risk informed considerations will allow resources to be optimally applied to where the most value can be obtained. Less important equipment could receive less attention and high safety significance equipment would have a higher level of focus further improving reliability and safety. Implementation of such proposed techniques will likely require changes to the licensee's technical specifications and / or exemptions from various federal requirements such as the Maintenance Rule until such a time in the future that a change to the 10 CFR Part 50 can be obtained.

8. REFERENCES

1. IEEE Std 338-1987 "Standard Criteria for Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems."
2. BALKEY, KENNETH R. AND NANCY B. CLOSKY, "Implementation of Risk-Informed In-Service Inspection," *Nuclear News*, (May 2000).
3. IEC 1226-1993-05, "International Standard Nuclear Power Plants – Instrumentation and Control Systems Important to Safety – Classification."
4. IEC 671-1980, "International Standard Periodic Tests and Monitoring of the Protection System of Nuclear Reactors."

Acknowledgements - Contributions by Wallace J. Colvin (First Energy Corp.) are gratefully acknowledged.