IMPROVED NUCLEAR POWER PLANT OPERATIONS THROUGH PERFORMANCE-BASED SAFETY REGULATION

M.W. GOLAY
Massachusetts Institute of Technology,
Cambridge, Massachusetts,
United States of America

Abstract

The US Nuclear Regulatory Commission (NRC) has recently instituted use of Risk-Informed, Performance-Based Regulation (RIPBR) for protecting public safety in the use of nuclear power. This was done most importantly during June 1997 in issuance of revised Regulatory Guides and Standard Review Plan (SRP) guidance to licensees and the NRC staff. The porpoise of RIPBR is to replace the previously-used system of prescriptive regulation, which focuses upon what licensees must do, to a system which focuses upon what they must achieve. RIPBR is goals-oriented and the previous system is means-oriented.

This regulatory change is potentially revolutionary, and offers many opportunities for improving the efficiency of improving both nuclear power operations and safety. However, it must be nurtured carefully if is to be successful. The work reported in this paper is concerned with showing how RIPBR can be implemented successfully, with benefits in both areas being attained,. It is also concerned with how several of the practical barriers to establishing a workable new regulatory system can be overcome.

This work, sponsored by the US Dept. Of Energy, is being performed in collaboration with Northeast Utilities Services Corp. and the Idaho National Engineering Laboratory. In our work we have examined a practical safety-related example at the Millstone 3 nuclear power station for implementation of RIPBR. In this examination we have formulated a set of modifications to the plant's technical specifications, and are in the process of investigating their bases and refining the modifications.

INTRODUCTION TO PERFORMANCE-BASED REGULATION

The Nature and Status of Performance-Based Nuclear Safety Regulation

Performance-based nuclear safety regulation is a method of obtaining a high level of nuclear safety by focusing regulations upon the desired safety results rather than upon the means by which they may be obtained. The latter approach, termed prescriptive regulation, has been the traditional treatment in the United States from the start of the nuclear power era until today. It has been criticized for being inconsistent, arbitrary and needlessly burdensome. Performance-based regulation has come into use on a limited trial basis as a response to the weaknesses of the current system.

The arbitrariness of the current prescriptive regulatory structure was illustrated in the example of the Department of Energy's new production reactor (NPR), a project terminated in 1993. The Secretary of Energy, James Watkins, decreed that the NPR should be as safe as the civilian power reactors. Unfortunately for his staff they found that they could not state what that meant, as the roughly 110 civilian reactors differ greatly in terms of the various measures of safety by which they are evaluated. Ultimately this puzzle was left unsolved, as the NPR project was canceled in its early stages.

Under performance-based regulation the safety regulator [the Nuclear Regulatory Commission (NRC)] negotiates an agreement with a nuclear power plant license holder regarding what performance goals will be required, how complacence will be measured and

what corrective actions would be required should compliance not be achieved. The primary means of demonstrating compliance is through performance tests of systems and personnel. To-date, performance-based regulation has been employed in small-scale regulatory experiments concerned with reducing regulations which are burdensome and providing only small safety benefits (e.g., containment leak rate testing, and quality assurance (QA) requirements). Under performance-based regulation ultimately the documented pedigree required of "safety grade" plant components required to show that they have been manufactured using NRC-approved facilities and processes would be replaced by test data indicating the expected reliability of the components. This replacement has not yet occurred, but the number of components requiring full documentation is being reduced.

A more substantial use of performance-based regulation came into effect in July 1996 in the form of the "Maintenance Rule." The requirements of the "Maintenance Rule" utilize probabilistic risk assessment (PRA) as a method for prioritizing the devotion of maintenance-related resources among the various plant SSCs (Systems, Structures and Components). This prioritization is intended to ensure that the SSCs which are most important for maintaining current levels of safety receive their proportionate share of available resources. A similar prioritization can be used subsequently to ensure that any additional resources are devoted to improving the SSCs which would be most valuable in increasing safety performance.

The primary vehicles of RIPBR advancement are the Maintenance Rule implementation and a set of "Pilot Projects" investigating various regulatory examples. These include:

- o In-service testing and in-service inspections
- o Graded quality assurance
- o Technical specifications modifications
- o Allowed outage times.

The NRC has indicated that some licensee benefits are likely to be allowed in the near future in theses regulatory experiments. If this is done the impetus for widespread utilization of RIPBR could be substantial.

Currently probabilistic risk assessment techniques (i.e., models, modeling assumptions and data bases) are not sufficiently accurate and reproducible that such analyses can be employed without review and refinement by experienced engineers. Thus, it has become common in use of probabilistic risk assessment under the Maintenance Rule to require use of subjective judgment by an expert panel of its results before they can be used as a decision-making basis.

Should the need for plant modifications also be indicated, the expected performance of the modified systems, structures and components would first be analyzed using the sorts of deterministic methods which have always been at the heart of nuclear safety analysis. Then the priority for assignment of safety-related maintenance resources would be determined through probabilistic risk assessment followed by expert evaluation. Regulatory compliance tests and potential corrective remedies would be negotiated as the basis of that system, structure, or component's future maintenance plan.

In order to stimulate this examination each power plant licensee has been required to submit a plant-specific version of a PRA under the Individual Plant Examination (IPE) and the Individual Plant Examination - External Events (IPEEE) programs; these PRAs identify individual plant risk vulnerabilities and provide a measure of the variation of risk measures among the set of US nuclear power plants. These reports have been partially evaluated by the NRC staff, with AN interim Evaluation Report and to be issued shortly.

Finally, in more recent action the NRC Chairman, Dr. S. A. Jackson, in 1996 gave a priority to moving the NRC to using what she terms "risk-informed performance based regulation." In order to speed this transition she has directed the NRC staff to reformulate its Standard Review Plan and to issue corresponding Regulatory Guides for the use of

licensees, to incorporate use of PBR with PRA by the end of 1996. This has been done and these documents have now been released for public review.

Each of these documents follow a standard, high level, structure for proposal and evaluation of license-requirement changes under RIPBR as follows:

1. Describe the change and its rationale.
2. Perform an engineering evaluation of the change
   - 2.1 A traditional deterministic evaluation showing that current regulations are satisfied, and that the requirements for conservatism and defense in-depth are satisfied.
   - 2.2 A (newly required) probabilistic risk evaluation, showing that the risk implications of the change are small, and hopefully beneficial.
3. Formulate a plan for monitoring the implementation of the change, ensuring that the associated performance goals will be met.
4. Document the change proposal.

The NRC has undertaken expanding the set of staff knowledgeable about and able to use PRAs in their work, and has begun guiding standardized treatments of PRA modeling and data bases; this work will require some years to complete, but is important for having been started. The treatment of uncertainty is one of the most important outstanding areas of work.

The Decision-Making Bases of Performance-Based Regulation

The previous paragraph illustrates the interplay of the major decision-making bases of performance-based regulation. They are listed in Table 1 in order of importance, with examples of where in the overall nuclear safety problem each basis is particularly valuable.

The primary basis of performance-based regulation is Tests of performance. This is the case because such tests, where appropriate, are the most accurate and least ambiguous of the performance-based regulation decision making bases.

Supporting Tests as the primary decision basis are both probabilistic risk assessment and deterministic analyses. Each class of analysis has particular areas of strength within the overall safety evaluation problem, as illustrated by the examples of Table 1. Deterministic analyses are most valuable in prediction of nominal SSC performance and for incorporation of conservative bias.

Probabilistic risk assessments are most valuable for sensitivity analyses of expected system performance, and for identifying the relative importance of the different systems, structures and components within a system. From this discussion it is seen that risk assessments provide one of the important bases of performance-based regulation, but are far from providing the entire overall evaluation of safety. In discussions of how performance-based regulation should be structured this point is often confused because excessive attention is sometimes paid to the role of probabilistic risk assessment in restructuring nuclear safety decision-making. This is because probabilistic risk assessment is still in an early stage of development, because a plan for how it should be used in a comprehensive regulatory system is still evolving, and because its initiation will be a major undertaking. This paper is intended to contribute to the evolution of that plan.

Regardless of how probabilistic risk assessment is used ultimately its implementation as a routine regulatory tool will be slow and expensive, both in terms of people and funds. This is because the decision-making tools currently utilized within the nuclear power industry will have to be augmented by those of probabilistic risk

Table 1

Foundation of Performance-Based Regulation

BASIS ELEMENT	AREAS OF BEST APPLICATION
Tests and Inspections	Actual system or component reliability or capability Personnel capabilities
Deterministic Analyses (sometimes with conservative bias)	Plant and system design
PRA (basis of Risk-Based Regulation)	System reliability analysis System vulnerability analysis System improvement analysis
Subjective Judgment	Very complex or poorly understood phenomena • Severe accidents • Personnel behavior

assessment. Doing this will require creation of convenient NRC-approved models, modeling treatment and data bases (which will require continual refinement as new data are generated). The precedent of the 1970s emergency core cooling system (ECCS) analysis treatment by the NRC is relevant. In this case the agency identified computer codes, modeling assumptions and data, and the agency stated that it would accept analyses resulting from their use.

An additional objection to use of probabilistic risk assessment which is sometimes raised is that it is too uncertain to be used in regulation. It is important to note that the uncertainty of our knowledge of the safety of a nuclear power plant is only reduced, not raised, through use of probabilistic risk assessment. Thus, the existence of uncertainty in probabilistic risk assessments provides no reason for not using them. This uncertainty is inherent in the design and phenomena of the plant. Use of probabilistic risk assessment can illuminate the existence of areas of uncertainty, but it does not create them. Rather, in the absence of probabilistic risk assessment, the social bargains embedded in the current regulatory process may accommodate or even disguise the existing uncertainties, but they do not eliminate them.

Subjective (i.e., expert) judgments play a natural role in portions of the safety problem where the previous three methods are insufficiently accurate to provide a reliable decision basis. A role for informed subjective judgment has been encouraged in plans for implementation of the Maintenance Rule. However, more generally the United States nuclear regulatory system has underutilized this decision-making basis—mainly because it is ill-suited to quantification. This policy is inconsistent with most of human experience, where the most important decisions, from the choice of a spouse to the election of acceptable risks, are based upon informal subjective evaluations. One of the great opportunities within performance-based regulation for improving safety decisions is in providing for more widespread explicit use of subjective judgment processes in the many areas of decision-making where it can serve best.

Notably, the NRC has long used subjective judgment in the regulatory process, but to a too-limited extent. Relevant examples include the work of the NRC commissioners themselves, of the Atomic Safety and Licensing Boards, and of the Advisory Committee on Reactor Safeguards.

RESEARCH PROJECT ON PERFORMANCE-BASED REGULATION

The main objective behind employing performance based regulation in nuclear power plants is to enhance the performance of the plants such that operational safety is not only maintained but improved. We illustrate the benefits and requirements of RIPBR in the project on Integrated Models, Data Bases And Practices needed for Performance-Based Safety Regulation. It is sponsored by the US Dept. Of Energy, is being performed in collaboration with Northeast Utilities Services Corp. and the Idaho National Engineering Laboratory. The purpose of the project is to investigate and demonstrate the potential benefits of performance-based safety regulation (PBR), or as it has become know more recently risk-informed, performance-based regulation (RIPBR). These goals are explained further in the abstract from the project proposal, as follows:

"It is proposed to develop tools, methods and practices to support both the US Nuclear Regulatory Commission (NRC) and nuclear power industry in structuring a practical approach to performance-based safety regulation. Success in this work will improve the safety of operating nuclear power plants and permit much more efficient use of nuclear power plant resources. The project's results can improve the capabilities of the INEL and enable the NRC to build the foundations and framework for performance-based regulation. The tools and practices developed in this work will demonstrate that the framework is realistic, and that the goals are achievable. At all stages of the project emphasis will be given to insights gained from industry experience. This is likely to produce results having a high acceptance level with not only the NRC but also with the nuclear industry."

We have focused our project's work upon the surveillances and maintenance activities associated with the emergency diesel generators (EDG) of the Millstone 3 (MP-3) PWR nuclear power plant. The reasons for this choice are that:

1. The EDGs are very important for safety, having the highest value of the Fusell-Vesely risk importance measure for core damage frequency (CDF) at that plant—meaning that failure of the EDGs would contribute more to core damage risks than would failure of any other system in the plant.
2. The EDGs require frequent surveillance testing and mandatory maintenance, as required by the technical specifications, with the objective basis of these requirements never having been established.
3. Potentially improvements in terms of both safety and economics can be achieved by basing future requirements in these areas upon risk-based arguments.
4. The EDG system has a reliability goal that is set by the Station Blackout (SBO) rule.[1]

In addition to the EDG requirements at MP-3 we have also investigated the practices and bases of the NRC treatments of EDGs for nuclear power plant licensees, and for similar activities in other industries (i.e., the U.S. Navy, the Federal Aviation Administration and civilian hospitals).

Emergency Diesel Generator System Description

A central concept upon which nuclear power plants are built is that of redundancy in safety system and their components. Redundancy is employed in order to safeguard against failures of single component systems. One of the backup systems incorporated in nuclear power plants is an onsite emergency power supply system. Most power plants utilize diesel generators for that purpose. Typically, a plant has at least two independent emergency power supply trains and each is connected to an emergency diesel generator EDG. In the case of MP-3 each of the two generators is a 4.6 kV, 3 phase, 60 Hz diesel engine-driven generator.[2,3] The capacity of each generator is 4,986 kW continuously, or 5,335 kW for 2,000 hr. Each EDG has independent support systems to minimize common cause failures. An EDG's system components and related support systems are shown

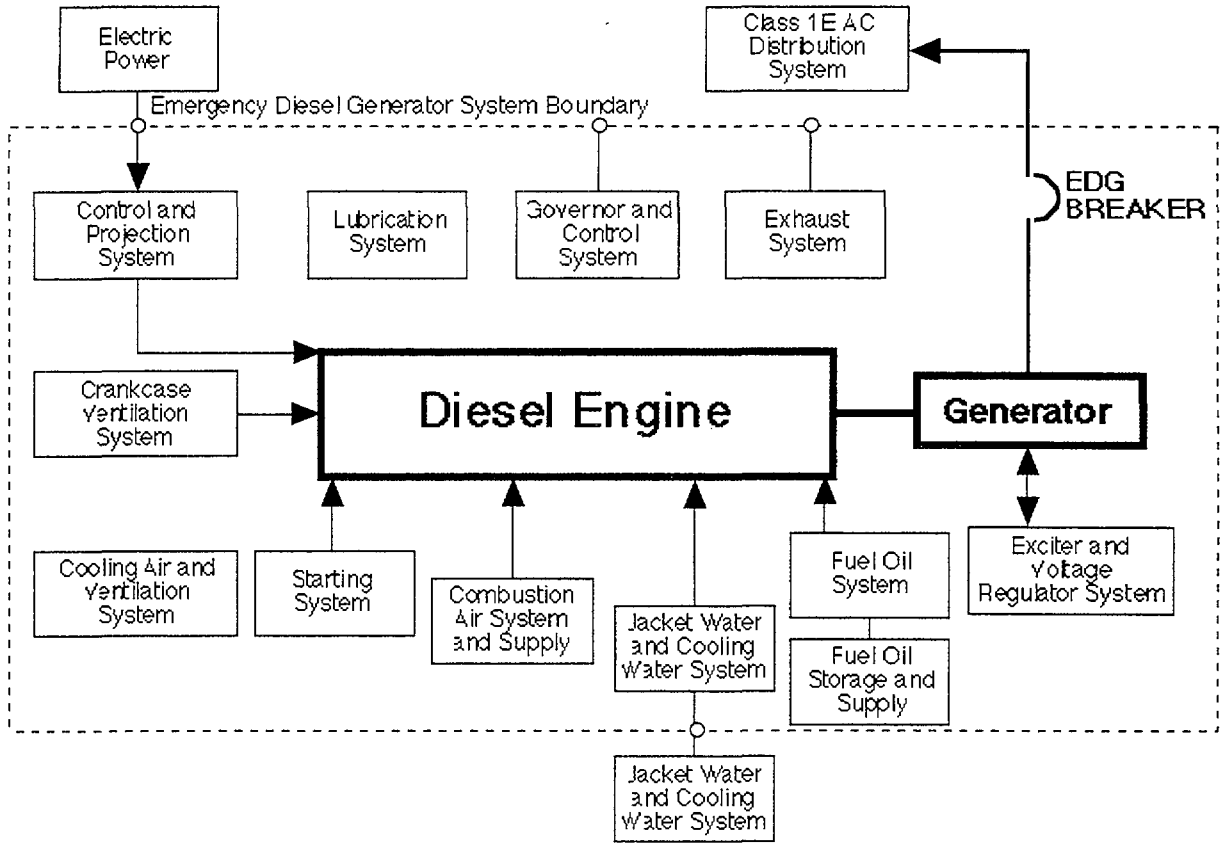

Figure 1. Boundary and Support System of Emergency Diesel Generator System

TABLE 2. Millstone-3 EDG Surveillance Requirements

Test Number (Refer to MP-3-TS)	**Purpose**	**Frequency**
4.8.1.1.1	Verify correct breaker alignments	Weekly
4.8.1.1.2 (a-f)*	Availability tests that start, load and operate the EDG for 60 min.	Monthly unless number of test failures ≤ 4 in the last 100 tests**
4.8.1.1.2.g	Perform inspection in accordance with manufacturer's instructions in addition to operating the generator for 24 hr.	18 months (every refueling)
4.8.1.1.2.h	Start both generators simultaneously to verify independence	10 years
4.8.1.1.2.i	Clean fuel storage tank	10 years

* Test 4.8.1.1.2.b is carried out every 184 days and involves the same steps of 4.8.1.1.2.a

** The test frequency is once per 31 days if the number of failures in the last 20 tests is ≥ 1 or ≤ 4 in the last 100 tests. If the number of failures goes up to ≥ 2 in the last 20 tests or ≤ 5 in the last 100 tests the frequency is increased to every 7 days.

schematically in Fig. 1 where the dashed box defines the boundary of the system.[4] Among various support systems, Fig. 1 shows a starting system which provides compressed air to drive a pneumatic starter, a fuel supply system that has enough fuel capacity for the continuous operation of the generator for six days, and a cooling system which utilizes a shell and tube heat exchanger to cool the generator, transferring heat through a forced air ventilation system.

The main function of the generators is to supply power to the plant safety system in cases of emergency in order to assure that the plant is maintained in a safe condition until offsite power is restored. In order to ascertain that the generators and their supporting system perform their functions they must satisfy certain load and response criteria by design. In addition to meeting their design requirements, the generators must have sufficient reliability to maintain the risk of core damage at an acceptable low value. Hence, Criterion 18: *Inspection and Testing of Electric Power systems* of Appendix A to 10 CFR Part 50[4] requires that electric power systems important to safety be designed to permit appropriate periodic inspection and testing in order to verify the operability of the systems and the condition of their components. The main concern of this project is the availability surveillance tests that are carried out on a monthly basis and the intrusive inspections done every refueling cycle.[3]

Surveillance Requirements of the Millstone-3 Technical Specifications

The Millstone-3 surveillance requirements (SR), as specified in the technical specifications (TS)[2], may be categorized according to the surveillance interval. The surveillance interval of the tests varies from a weekly to a once per decade basis. Table 2 summaries the most important tests involved, their purposes and their respective testing frequencies.

Changes in EDG Testing, Inspection and Monitoring Requirements

Our work, performed from the perspective of the licensee, has focused on identifying EDG maintenance and inspection requirements that may benefit from modification. We have also been concerned with justifying these changes with the help of data, expert testimony and by exploiting the capabilities of on-line equipment performance monitors. Our tentatively recommended replacement requirements are shown in Table 3. They will probably be revised. However, it is clear that the resource requirements needed to demonstrate that current safety levels are being maintained are considerably fewer than are currently demanded by regulations.

Table 3

Proposed Revised Testing and Inspection Requirements

- o Replacement of (monthly) test 4.8.1.1.2 (a-f) by an automatically executed EDG test to start, load fully (within 60 sec. except within 11 sec. once every 24 months) and run for 24 hours, required to be performed every six months (after further experience this interval might be lengthened, depending upon the observed results)

- o Elimination of (inspection) test 4.8.1.1.2.g, replaced by a program of on-line monitoring of the EDG and its support systems during its required tests

- o Elimination of test 7.5.9 (endurance and load test perfumed once per refueling interval)

- o Performance of load combination tests 7.5.6 through 7.5.13 once per decade (rather than once per refueling interval)

Tests:

An examination of licensee reporting data [5,6] concerning the results of required EDG tests indicates that few EDG failure occur involving the EDG itself. Most of the failures observed involve support systems, which typically receive less attention for maintaining good material condition than does the EDG itself. Also, it is observed that many of the observed failures occur during the infrequent long-duration tests performed during refueling shutdowns. Similar results have been reported concerning EDG tests on US Navy nuclear-powered vessels [7,8]. Also, an examination of the MP-3 EDG failure analysis in the plant-specific PRA indicates that the failure modes interrogated by the currently required monthly tests contribute only two percent of the total EDG-associated core damage frequency. Thus, these tests appear at best to be of slim value. Our work is now focusing upon justifying performance of more demanding tests on the EDGs and associated systems, and eliminating the currently-frequent, but probably meaningless, tests now required by the technical specifications. The exact nature and frequency of the tests to be required is still being determined.

Table 4

Colt-Pielstick -- PC2V Engine Instructions (Annual/Refuel)

1. Follow all preceding instructions.
2. Remove and check injection nozzles for operation and opening pressure.
3. Remove, disassemble, clean and repair all air start valves and air start distributors. Clean/replace air start distributor filter.
4. Drain and refill governor and turbochargers with approved oil.
5. Drain, flush and refill outboard bearing with approved oil.
6. Check tightness on all foundation, block to base, oil and water line bolts.
7. Check sample of rocker lube oil for condition and contaminants.
8. Check turbocharger inlet casing and turbo casing water passages for scale. The inside surface of these casings is the best indication for adequacy of water treatment.
9. Check for tightness of exhaust manifold flange bolts to cylinder head (165-195 ft.lbs.).
*10. Check all safety and shutdown controls for appropriate pressures and temperatures.
*11. Borescope all cylinder liners.
12. Inspect the crankcase end of all cylinder liners.
*13. Check main bearing cap tightness and side bolts. Alternately confirm cap tightness to frame and saddle to .0015 feeler gauge
14. Visually examine gear train and drives, cam shafts and bearings, push rods and rocker arms.
15. Check crankshaft alignment and bearing clearances.
16. Check connecting rod bearing clearances with feeler gauges.
17. Inspect all ledges and corners in crankcase for debris which could indicate other mechanical problems. Confirm all cotters, safety wire and lock tabs are in place and tight.
18. Water test engine and inspect for internal and external leaks. Isolate J.W. surge tank and test entire systems at 40 psi. After engine is returned to operation and has reached normal operating temperature, remove each rocker cover and inspect for water leaks at top area of cylinder head.
19. Check alternator coils and poles for indication of movement (visual).
20. Drain and refill alternator bearing lube sump. If oil has contaminates, pull bearing cap and inspect journal.
21. Inspect and clean (if required) overspeed trip mechanism. Check operation according to overspeed trip test instructions.
*Identified as excessively intrusive (MP-3 systems Engineer)

Inspections:

Available data[5,6] and interview reports from individual power stations and the US Navy indicate that EDG inspections almost never reveal important component faults; however, they provide new opportunities for introducing defects. Thus, it appears that the need for the current practice of partial dismantling, and subsequent reassembling of the EDGs (see Table 3) during each refueling outage is unjustified, in view of the opportunities to damage or misalign the EDG in the process.

We recently asked the MP-3 EDG systems engineer[9] to review the current general refueling inspection guidelines and separate each of the requirements into one of three categories:

1) Items that can be justifiably eliminated from the Technical Specifications inspection program,
2) Items that can be performed on-line with the plant operating at high power, and
3) Necessary items that cannot be performed on-line.

Of the 21 general items (see Table 4), he indicated that a majority of the surveillances could be performed on line or at more extended intervals. He also indicated that none of the required items would fit into the third category. He also identified the most intrusive inspection items and recommended that they by eliminated or made less intrusive.

Notably, we have found that similar inspections are not required for EDG used in hospitals and federal air traffic control centers (see Table 5). Thus, we are recommending that such inspections be made far less intrusive and less frequent (i.e., once per decade, or - later - never).

Table 5.

Non-nuclear Industry EDG Reliability Practices

	MP-3	U.S. Navy	Cambridge Hospital	FAA
Monthly Loaded Test	1 hour	30 minute minimum	1 hour	1 hour
Yearly Loaded Test	24 hours	Unavailable	Semi-annually, simulate blackout, no set time	4 hours
Major Maintenance	18 months	Annually	Semi-annually, contracted	Annually
Overhaul	18 months	Infrequently	Infrequently	As needed

Monitoring:

EDGs and supporting systems have traditionally been monitored during required tests, to the extent that available technologies have permitted. However, such activities have not typically been recognized in required EDG reliability ensuring programs. Recent advances in computer technologies have greatly increased the value of monitoring, as a supplement to frequent tests and inspections, as the need for highly trained humans is replaced by development of smart instrumentation, able to identify trends and indications of incipient failures and degrading component performance.

From the available data, we have determined which systems are the best candidates for monitoring, and which parameters are of most interest. The systems of interest are the diesel itself, cooling systems, air systems, lubricating and fuel oil systems

turbot/superchargers, and instrumentation and controls. The last of these presents a serious concern, as we propose to increase the amount of instrumentation, while it is currently a significant problem. Table 3 lists the components and failure modes to be monitored, along with recommended monitoring parameters.

In the diesel, our goal is to accurately assess the chances that any failure mode currently covered in the technical specifications will occur during a given time period. Monitoring of cylinder pressures and temperatures, fuel injection, and bearing and cylinder vibrations covers the failure modes which are currently assessed with highly intrusive physical inspections. Also, oil analysis further guarantees proper operation, as is discussed concerning lubricating oil.

In the cooling systems, the major concerns are components such as pumps, valves, dampers, and fans, and the presence of leaks. For both the service water and ventilation, we have been formulating instrument systems to predict or locate weak components or leaks. Similarly, in the air systems, intake, exhaust, crankcase vacuum, and air-start, leaks and valves are the primary concerns. Pressure and flow sensors should allow small leaks and weakening components to be identified and located.

In the case of the lubricating oil system, instrumentation is used to predict and locate leaks, and to detect high or low pressure, high or low volume, and high temperature. In order to guarantee oil quality and the mechanical condition of the diesel accurately, chemical analysis of lubricating oil would remain a necessity in the absence of an acceptable sensor for determining the particulate content of the oil. Here, the buildup of combustible products or soot would indicate the presence of weak seals or rings, high water content would demonstrate gasket or engine block weaknesses, corrosion products would indicate oxidation problems, and metal particles would indicate insufficient lubrication or worn bearings or other critical components. Also, physical properties of the oil, such as viscosity, would indicate oil lubrication and high temperature performance.

In the fuel oil system, leaking and components like valves and pumps are certainly concerns requiring instrumentation, but also tank levels are a concern. Sensors can be used to eliminate storage and day tank level concerns which figure prominently in the EDG fault trees. Also, opacity sensors can be used in the light diesel fuel oil to guarantee cleanliness of fuel from tank scale or fungal growths.

The turbochargers and superchargers used are susceptible to the same sorts of failures as the diesels themselves, such as bearing failures, cooling failures, and lubricating oil problems. With vibration, temperature, and oil pressure sensors, turbocharger and supercharger faults can be predicted and repaired.

Against the recommended advantages above, there are certain disadvantages to the use of monitoring as well. To make these changes, the approval of the NRC would be required, involving a change to the technical specifications that govern plant operations. To change these technical specifications, the monitoring systems must not decrease safety and reliability levels as compared with the current physical inspections. The same possible failure modes should be tested, and no new serious failure modes should be introduced. As will be demonstrated further, we believe that current failure modes inspected can be tested equally or better with instrumentation. The greatest disadvantage is the possibility of introducing new failure modes. In particular, there are four possible new failures. The addition of intrusive vibration, temperature, pressure, and flow sensors can interfere with normal operations and prohibit correct system behavior, or can even introduce leaks or contamination in otherwise closed systems. The other errors possible would involve information reported and its use. Over-reliance on the monitoring systems could also lead to problems where the data reported are given more credence than good judgment and working experience. Also, the sensors could either falsely report a negative condition when none exists, or fail to report a negative condition when one should be reported. The former is a less serious concern, as a simple diagnostic check of the instrument could be conducted, or other related instrumentation could be checked for anomalies on report of an

error. However, the latter introduces new complications, as, without receiving any fault signals, there would be no reason to conduct diagnostic checks on the components being monitored. This problem requires that the instrumentation be extremely reliable or be used in voting systems, such as one using 2-out-of-3 systems failure logic.

Finally, instrumentation and control failures are a major concern, especially when more sensors are to be added to a system. The sensor problems reported are primarily trips of the diesel due to false negative signals. The occurrence of negative conditions which do not cause a necessary trip is extremely rare. This suggests that the false negative signals be followed up with diagnostic checks and consultation with other instrumentation, and system highly susceptible to give false positive signals be used in logical voting system This system would favor enhanced safety, with excess caution. To best represent the state of the system, however, false negative signals should be reduced as much as possible with higher quality sensing.

Research from INEL and plant experiences indicate that a monthly one-hour test run, as required in the MP-3 technical specifications, does not allow enough time to observe all possible failure modes, as some modes, such as vibration-induced failures, do not develop for several hours. In order to monitor the diesel through most of its possible failure opportunities, longer test runs would be required, but the increased reliability should allow monthly tests to be replaced with less frequent runs, such as on a quarterly basis. Thus engine wear would not be significantly increased, and the potentially harmful frequent starts would be reduced by two-thirds or more. Currently, we are seeking to demonstrate that diesel support systems could be operated on a monthly basis to insure their availability without running the diesel unnecessarily.

In the course of the project, two possible failure modes concurrent with the practice of pre-lubricating the EDGs have arisen, and are being explored currently. Both of these failure modes are exclusive to the opposed piston type of diesel engine. The first failure mode was experienced in Naval EDGs, which made the diesel unable to operate[6]. Prior to starting the diesel, lubricating oil could leak past the upper piston rings and fill the combustion chamber of a cylinder. When a start was attempted, the oil-filled cylinder performed as a hydraulic lock, preventing the motion of any pistons in the engine, failing it. The second failure mode was a problem characteristic to Fairbanks-Morse, or Colt-Pielstick opposed piston engines[7]. Similar to the previous failure mode, lubricating oil could leak past the upper set of pistons and fall into the combustion chamber. However, in these cases, the oil ran out the open exhaust ports and into the manifolds. In some cases, this oil ignited in the manifolds, causing a new diesel failure mode. The Fairbanks-Morse recommendation was to reduce the then-standard fifteen to thirty minute pre-lubrication to only two or three minutes. In consideration of the now constant pre-lubrication, these possible failure modes are currently being re-examined. The need for pre-lubrication is also in question, as engine wear was not necessarily significant, and we are now proposing fewer starts of the diesels.

Effects of Inspection Requirement Changes Upon Plant Operations:

It has become widely recognized that the times of greatest plant risk may not be when the plant is operating at high power, as had been commonly assumed for many years. Rather, when a plant is undergoing refueling its vulnerability for fuel damage due to fuel cooling failures may be considerably greater than when at high power. This is because of the greater complexity of plant configuration control. -- with an attendant increase in human error probabilities, and because of reduced redundancy in accomplishing the fuel cooling functions.

The requirements for EDG intrusive inspections and long duration tests exacerbate the possibilities of such cooling failures during refueling outages and may actually increase plant fuel damage risks. They also severely increase plant costs by lengthening such outages. We are now undertaking work to determine whether such inspections and tests should be moved on-line.

In examinations to-date of the MP-3 refueling outage schedule and risk profile it appears that the reduction of the outage critical path due to moving the EDG surviellances on-line would be modest (of the order of a few days). However, the risk implications could be large. However, fuel damage risks during outages are dominated by human errors. The major benefit of moving EDG work on-line may be to simplify the management of the outage, and thereby to reduce risks. Currently it appears so, but it is too early to say more.

CONCLUSIONS

Our primary results to-date indicate that most of the required EDG surviellances are not useful in reducing safety, and may actually reduce safety.

As the surveillance test and maintenance intervals are increased economic savings will be realized in a straightforward fashion. This is because the expenses for these activities scale with the number of test and repair operations. As their total over a plant's life is decreased savings will accrue directly. However, the greatest benefits of revised EDG requirements is likely to be reduced risks, by means of rationalizing those activities in terms of their overall risk and economic implications.

References

1) U..S. NRC, 'Evaluation of Station Blackout Accidents at Nuclear Power Plants', NUREG/CR-1032, June 1988.

2) Millstone-3 Technical Specifications.

3) Regulatory Guide 1.108, *Periodic Testing of Diesel Generator Units Used as Onsite Electric Power SysteMP at Nuclear Power Plants*, Revision 1, August 1997.

4) Regulatory Guide 1.9, *Selection, Design, Qualification, and Testing of Emergency Diesel Generator Units Used as Class 1E Onsite Electric Power system at Nuclear Power Plants*, Revision 3, July 1993.

5) Grant, G.M. et al. Emergency Diesel Generator Power System Reliability 1987-1993. Idaho National Engineering Laboratory, INEL-95/0035, February 1996.

6) Nuclear Plant Reliability Data System, INPO.

7) Grotsky, Peter. CVN-68 Class Emergency Diesel Generator (EDG) Reliability and Availability, 9233 Ser. 03X3/331, October 17, 1996.

8) Grotsky, Peter. Personal communication, November 1996.

9) Shanihan, B., per sonal communication May 1997.