ELSEVIER

Journal of Hazardous Materials 71 (2000) 219–237

Journal of Hazardous Materials

www.elsevier.nl/locate/jhazmat

Improved nuclear power plant operations and safety through performance-based safety regulation

M.W. Golay *

Department of Nuclear Engineering, Massachusetts Institute of Technology, Room 24-223, 77 Massachusetts Avenue, Cambridge, MA 02139, USA

Abstract

This paper illustrates some of the promise and needed future work for risk-informed, performance-based regulation (RIPBR). RIPBR is an evolving alternative to the current prescriptive method of nuclear safety regulation. Prescriptive regulation effectively constitutes a long, fragmented checklist of requirements that safety-related systems in a plant must satisfy. RIPBR, instead, concentrates upon satisfying negotiated performance goals and incentives for judging and rewarding licensee behavior to improve safety and reduce costs. In a project reported here, a case study was conducted concerning a pressurized water reactor (PWR) emergency diesel generator (EDG). Overall, this work has shown that the methods of RIPBR are feasible to use, and capable of justifying simultaneous safety and economic nuclear power improvements. However, it also reveals several areas where the framework of RIPBR should be strengthened. First, researchers need better data and understanding regarding individual component-failure modes that may cause components to fail. Not only are more data needed on failure rates, but more data and understanding are needed to enable analysts to evaluate whether these failures become more likely as the interval between tests is increased. This is because the current state of failure data is not sufficiently finely detailed to define the failure rates of individual component failure modes; such knowledge is needed when changing component-specific regulatory requirements. Second, the role of component testing, given that a component has failed, needs to be strengthened within the context of RIPBR. This includes formulating requirements for updating the prior probability distribution of a component failure rate and conducting additional or more frequent testing. Finally, as a means of compensating for unavoidable uncertainty as an obstacle to regulatory decision-making, limits to knowledge must be treated explicitly and formally. This treatment includes the formulation of probabilities through expert solicitation and the review of risk-in-

* Tel.: +1-617-253-5824; fax: +1-617-258-8863; e-mail: golay@mit.edu

PII: S0304-3894(99)00080-1

formed, performance-based and engineering analyses used to evaluate proposed changes to existing technical specifications.

Keywords: Nuclear power plant; Operations and safety; Performance-based safety regulation

1. Introduction

1.1. Overview

The U.S. 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. The primary concerns are preventing damage to the reactor's fuel and ensuring that no radioactive materials will enter the biosphere. This was done most importantly during June 1997 through the issuance of the revised Regulatory Guides and Standard Review Plan (SRP) guidance to licensees and the NRC staff. The purpose of RIPBR is to replace the current 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.

The success of RIPBR is one of several keys to the success of nuclear power in the United States. The combined safety and economic performance of existing nuclear power plants will have a dominant effect upon whether new nuclear power technology will be introduced. RIPBR offers one of the few available avenues to improve both classes of performance. With the introduction of commercial competition to the electric power industry, effective exploitation of RIPBR may be an essential element in successful competitive strategies for nuclear power companies.

This paper discusses the current state of capability in the USA for undertaking RIPBR, and the agenda of future work that will have to be addressed before it can become a successful, routinely applied approach for nuclear safety regulation. Many of the observations offered here are derived from a recently concluded project on Integrated Models, Data Bases and Practices Needed for Performance-Based Safety Regulation. Its purpose was to investigate and demonstrate the potential benefits of RIPBR and to reveal important obstacles to its success and to indicate where additional research could contribute to that success. The work of this project is described more fully in the project Final Report [1].

In this work, we have examined several applications of RIPBR, seeking to identify examples where it could be used to justify changes in current regulatory requirements that could improve safety and/or economic performance. In general, we have found that current plant risk models and databases, by themselves, are not adequate for justifying such changes. Rather, current capabilities are useful in suggesting desirable regulatory changes, but at some point, the level of detail of current knowledge becomes inadequate for definitively justifying change. Then, in order to complete the needed evidence, additional approaches are required. The principal options are performance of new research, acquisition of additional data and/or use of expert judgement. In most cases, the last is the only useful option, as the time scales for the others are too great to support timely decision-making. Thus, major results of this work are indications of the need to

structure a long duration of model building and data collection to support maturation of RIPBR, and development of disciplined methods for integration of subjective expertise into routine regulatory decision-making.

1.2. Prescriptive regulation

RIPBR is an evolving alternative to the current prescriptive method of nuclear safety regulation. The system for nuclear safety regulation in the USA has been widely criticized over the past two decades. Analysts have noted the following problems [10]:

- It has not produced a uniform level of safety regulation among nuclear power stations;
- It inhibits technological innovations that can improve safety;
- In practice, it does not place full responsibility for safety with owners of nuclear power stations; and
- In many instances, it has not provided prompt, clear, and consistent regulatory decisions.

These shortcomings are due, in part, to use of a prescriptive approach to safety regulation. This approach includes the following features:

- In regulations used for licensing decision-making, a focus upon deterministic standards to dictate the nature and performance of plant systems;
- A use of surrogate standards for the risks that are actually being regulated (e.g. the reactor shutdown system is required to be diverse, when it is actually desired that it be highly reliable); and
- A lack of incentives for nuclear power station owners to make plants safer than minimally accepted levels.

Safety regulations governing light water reactors (LWRs) are the most developed of all nuclear safety requirements. They are formulated in terms of required systems and plant features (e.g. a containment building, a redundant reactor shut-down system, and on-site electrical system), which are required to either prevent or mitigate a spectrum of prescribed accidents. In addition, existing regulations embody system design constraints (e.g. specifications regarding spatial separation of redundant and component quality). These regulations exist in diverse formats, such as the Code of Federal Regulations, the USNRC Standard Review Plan, and the USNRC Regulatory Guides and Branch Technical Positions.

The existing regulatory literature is large and complex. It effectively constitutes a long, fragmented checklist of requirements that safety-related systems in a plant must satisfy. The consistency of this checklist and its ability to promote uniform levels of safety among different power stations is questionable. Furthermore, since these requirements are so pervasive in determining the acceptability of a plant's design and operation, they inhibit innovation and improvement. Because the workload of satisfying the sum of such requirements is so great, owners of nuclear power plants commonly treat satisfaction of the USNRC's requirements as being a sufficient effort for accident prevention and mitigation. When this occurs, the responsibility for safety has become de facto that of the USNRC rather than being solely that of the licensee. Such a situation is improper and dangerous.

1.3. RIPBR

As an alternative, RIPBR uses a new approach for achieving the desired level of nuclear safety performance. It concentrates upon satisfying performance goals rather than upon performance of specific procedures. RIPBR uses mutually negotiated performance goals and incentives for judging and rewarding licensee behavior. In the past, the USNRC has used system performance goals in regulation to a limited extent. Important examples include using test-based reliability standards for emergency diesel generator (EDG) starting [2], and use of required reactor survival durations in judging the acceptability of systems for withstanding station blackout conditions [3].

RIPBR often, but not exclusively, includes expected risks among the measures of expected safety performance. Analysts estimate these risks using probability risk assessments (PRAs) to evaluate changes in technical specifications such as increasing the allowed outage times (AOT) of subsystems or equipment and surveillance test intervals (STI) (i.e. the time between maintenance surveillances). This treatment differs from the existing, prescriptive, regulatory approach, in which regulators are concerned with ensuring that proper hardware, skilled personnel, and comprehensively specified procedures are used in regulated activities. Under RIPBR, the need for such high quality hardware and personnel and extensive procedures will remain, but the formulation of their regulations can be expected to become more logical, being based upon systematic assessment of the contribution to overall risks by each system element. Regulators can apply both the prescriptive and performance-based approaches in all areas of nuclear safety regulation, such as nuclear medicine and nuclear waste disposal. Their most important application, however, is with nuclear power.

The emphasis upon the use of risk assessment methods in RIPBR has sometimes obscured the fact that it also involves combined use of deterministic decision rules, performance test results and subjective evaluations, with each decision element being used where it has greatest advantage. For example, regulatory bureaucracies often can use deterministic decision rules more effectively, but these can be based upon risk and subjective analyses of overall system safety priorities.

1.3.1. Status and prospects for RIPBR

Since 1993, the USNRC has increased the pace of experimenting with performance-based regulations. Important examples include implementation of the ‘‘Maintenance Rule,’’ [4] implemented in 1996, and recent proposed risk estimate-based changes relaxing requirements for containment leak rate testing. In the 1994 Draft PRA Policy Statement (USNRC, March 1995), the agency announced its intention to utilize PRA estimates in addition to deterministic analyses and expert judgements as the bases of future regulation [5]. In March of 1998, the USNRC drafted a predecisional regulatory guide that is intended to improve the consistency in regulatory decisions in areas in which the results of risk analyses are used to help justify changes to technical specifications [6]. If this is done comprehensively, it implies a thorough revision of the USNRC’s regulations, which would permit agency and licensee resources to be used more efficiently than that which occurs currently. This change provides a considerable opportunity for licensees to improve both the efficiency and safety of operations, by

using RIPBR as the basis for revising the requirements for safety and resource allocation.

The effort to introduce RIPBR is progressing. The USNRC has stated a commitment to add RIPBR to deterministic analyses, expert judgement, and defense-in-depth to the analytic bases and principles upon which the agency will base future regulatory decisions (see Fig. 1).

The agency has also started several initiatives to explore how to implement RIPBR. These have included the following.

(1) Implementation of the ''Maintenance Rule'' as a RIPBR experiment.

(2) A search for regulations that contribute little to safety in their currently stringent forms, and which could be justifiably relaxed. Examples include: (a) development of ''graded'' quality assurance requirements, aiming to focus the devotion of resources for quality documentation of components in relationship to their respective importance for safety [7]; (b) relaxed standards for allowed rates of containment leakage during acceptance tests [7].

(3) Distillation of insights from the Independent Plant Evaluation (IPE) for guiding future regulatory actions.

(4) Explorations, in pilot applications of PRA, of ways to refine power plant technical specifications so that the operational constraints that they impose will be well-justified, but also to ensure that unsafe combinations of allowed operational conditions will not arise [8].

In parallel with this work within the USNRC, the nuclear power industry is collaboratively formulating policies and procedures under the aegis of the Nuclear Energy Institute's (NEI) Regulatory Threshold Working Group. This work is defining the ways that the industry will collectively exploit new uses of PRA to improve both economic performance and safety that is acceptable to the USNRC. Effectively, this group is negotiating on behalf of the industry with the USNRC to reach a mutual consensus upon how the industry and regulators can use PRA to improve overall performance. This group's secondary purpose is to achieve consensus within the disparate U.S. nuclear utility companies upon common practices and standards [9]. In addition, some utilities are working directly with the USNRC in exploring opportunities with PRA to achieve improvements.

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,

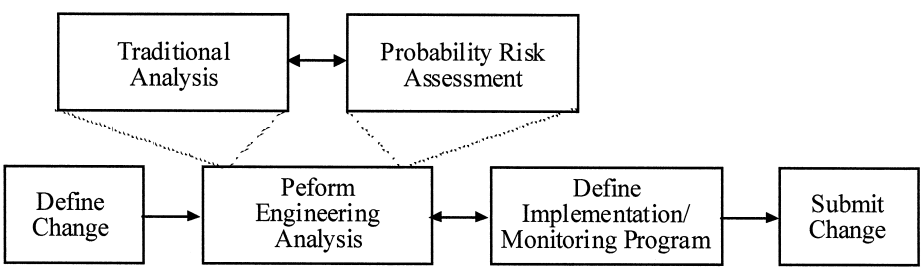

Fig. 1. General description of an acceptable approach to risk-informed applications (Ref. [6], p. 7).

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.

2. EDG case study

The EDG is a risk-significant standby safety system that we examined to identify opportunities for RIPBR-based regulatory improvements. Potential savings in costs (e.g., labor and replacement-fuel cost) may be achievable if maintenance practices are changed. Second, routine EDG maintenance can occur either when the reactor is critical or shut down, have focused our project's work upon the surveillances and maintenance activities associated with the EDGs of the Millstone-3 (MP-3) pressurized water reactor (PWR) nuclear power plant (shown schematically in Fig. 2). The reasons for this choice are the following.

(1) The EDGs are very important for safety, having the highest value of the Fusell–Vesely risk importance measure (i.e. the fraction of total risk contributed by the minimal cut sets involving the component of interest) 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.

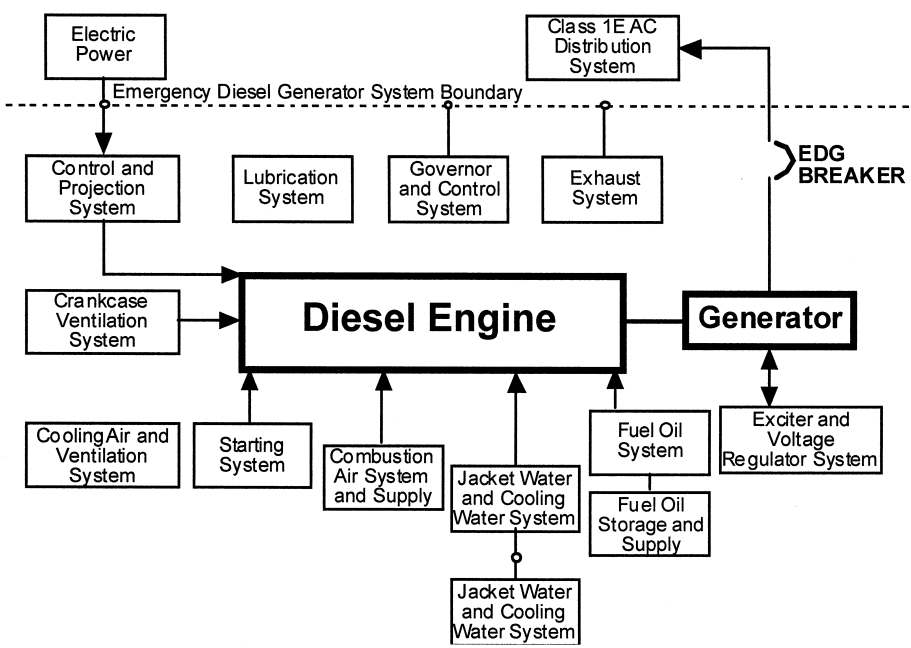

Fig. 2. Boundary and support system of EDG system.

(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 [10].

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).

2.1. Surveillance requirements of the Millstone-3 technical specifications

The Millstone-3 surveillance requirements (SR), as specified in the technical specifications (TS), 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 1 summarizes the most important tests involved, their purposes and their respective testing frequencies.

2.2. 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 2. 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.

In refining these regulatory changes, we have investigated alternative testing and inspection practices used elsewhere, the basis for current requirements and the role that

Table 1
The most important of the Millstone-3 EDG surveillance requirements

Test number	Purpose	Frequency
4.8.1.1.1	Verify correct breaker alignments	Weekly
4.8.1.1.2 (a–f)[a]	Availability tests that start, load and operate the EDG for 60 min.	Monthly unless number of test failures ≤ 4 in the last 100 tests[b]
4.8.1.1.2.g	Perform inspection in accordance with manufacturer's instructions in addition to operating the generator for 24 h	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

[a] Test 4.8.1.1.2.b is carried out every 184 days and involves the same steps as 4.8.1.1.2.a.

[b] 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.

Table 2
Proposed revised testing and inspection requirements

(A) Replacement of (monthly) test 4.8.1.1.2 (a–f) by an automatically executed EDG test to start, load fully (within 60 s except within 11 s once every 24 months) and run for 24 h, required to be performed every 12 months or when the reactor is refueled (this requirement could be fixed at 6 months initially; after further experience, this interval might be lengthened, depending upon the observed results).
(B) 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.
(C) Elimination of test 7.5.9 (endurance and load test perfumed once per refueling interval).
(D) Performance of load combination tests 7.5.6 through 7.5.13 once per decade (rather than once per refueling interval).

on-line monitoring could play in increasing the reliability of the emergency AC power function. We have also examined the effects of current practices in both monitoring and degrading actual EDG reliability.

2.3. Surveillance tests

Examination of the failures observed in 24 h of EDG tests and operations indicate the following time distribution of failures [11]:

1. Failures within the first hour of attempting to start, load and run are due primarily to electrical components (for starting, loading and controlling the EDG);

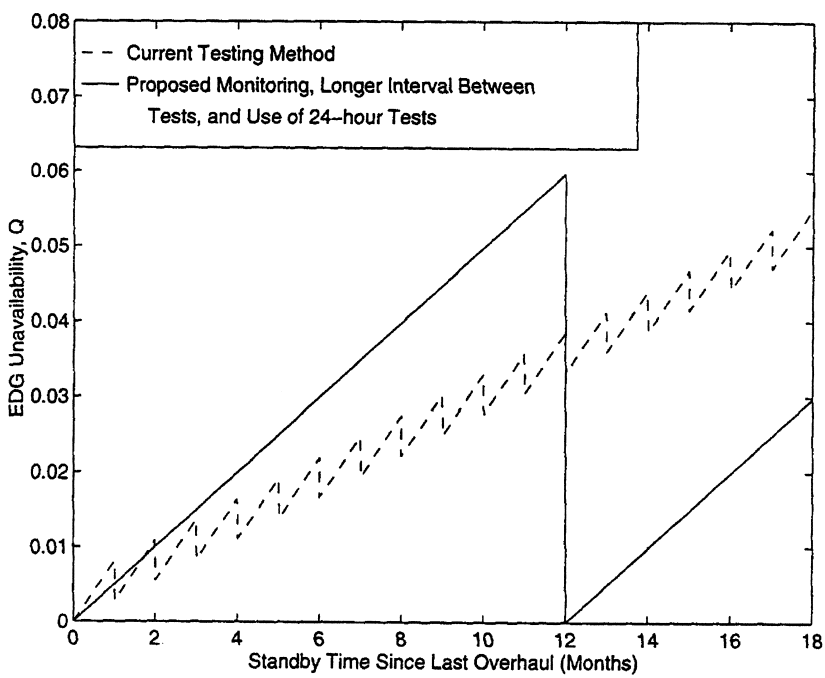

Fig. 3. Effects upon EDG unavailability of proposed monitoring and testing changes as compared to results of current testing methods.

2. Failures within the next 3 h of running are due primarily to support systems; and
3. Failures within the next 11 h of running are primarily due to mechanical failures within the EDG and support systems; after about 17 h of running, few additional failures are observed.

The functional requirement of the EDG is to provide emergency electric power for essential power plant needs for several tens of hours. The basic events of the EDG fault tree activated within the monthly 1-h test account for about half of the EDG functional failure risk. Thus, this test may be of greater use in exercising the EDG than as an indicator of the unit's ability to fulfill its mission. Fig. 3 indicates the EDG failure probability profiles indicated by the current TS requirements and those implied by the proposals of Table 2 accompanied by extensive monitoring during tests. It is seen that the mean failure probability with our proposal is approximately the same as with current requirements, but with less expense and effort. Further, should it be desired to reduce the mean failure probability below current levels, the frequency of 24 h start, load and run tests could be greater than specified in Table 2. The benefit of the proposed change derives from making the tests performed substantially more complete than the current

Table 3
Colt-Pielstick — PC2V engine instructions (annual/refuel) [12]

(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 lb).
(10) Check all safety and shut-down 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 0.0015 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 that 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 bearinglube 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.

Table 4
Refueling outage inspection items recommended for improvement listed in *Comparison to Practices in Other Industries Employing EDGs*

MP-3 Colt-Pielstick ROI items recommended for change[a]	Corresponding U.S. Navy requirements[b]	Corresponding FAA standby generator requirements[b]
(2) Remove and check injection nozzles for operation and opening pressure.	(7a) Check and record injector fuel pump timing on at least two cylinders on each bank (18 months). Install complete set of injection equipment (major overhaul).	(206a) Clean and service fuel injector if required (annually). (203d) Inspect starter (biennially).
(3) Remove, disassemble, clean and repair all air start valves and air start distributors.		
(4) Drain and refill governor and turbochargers with approved oil.	(3a) Visually inspect turbocharger oil level and condition of oil through sightglasses (18 months). (7b) Check governor oil level and oil leakage around base of governor. Visually inspect oil condition through sightglasses (18 months).	(203b) Drain and replace oil in hydraulic governor sump every 2 years, or after 200 h of operation, whichever comes first.
(9) Check for tightness of exhaust manifold flange bolts to cylinder head (165–195 ft. lbs.).	(4a) Visually examine exhaust system for leaks during operational test (18 months).	(201i) Examine exhaust and combustion for air systems for leaks (monthly).
(11) Borescope all cylinder liners.	Remove all cylinder liners (major overhaul).	Discretionary.
(14) Perform camshaft bearing analysis.	Remove, inspect and repair/replace camshaft bearings (major overhaul).	Discretionary.
(15) Check crankshaft alignment and bearing clearances.	(2m) Take a complete set of crankshaft deflection readings and bearing presses (18 months).	Discretionary.
(19) Check alternator coils and poles for indication of movement (visual).	No reference.	Discretionary.

[a] Current ROI requirements [4].
[b] Numbering refers to items found in Navy Diesel Engine Inspection Handbook [13].

monthly tests. In the results of Fig. 3, we assume that the new tests would be essentially complete. In reality, this may not be the case, as subtle failure modes may remain untested, but the proposed tests would likely be much more complete than the current tests.

Notability — the unavailability (not shown in Fig. 3) due to the EDG being taken out of service (OOS) — may not change greatly under our proposal. The actual time spent in testing would increased under our proposal by a factor of 1.33. If our test were to be made of 18- rather than 24-h duration test, the OOS unavailability would be approxi-

Table 5
Proposed component, failure mode and monitoring variables

System	Component or failure mode	Monitored parameter	Engine analyzer
Engine	Cylinder	Pressure	Yes
		Exhaust temperature	Yes
		Vibration	Yes
	Fuel rack	Position	Yes
	Crankshaft	Position	Yes
	Bearings	Vibration	Some
		Temperature	Some
Fuel oil	Tanks	Level	No
	Fuel lines	Pressure	No
	Pumps	Differential pressure	No
		Vibration	No
Cooling water	Tanks	Level	No
	Lines	Pressure	No
	Pumps	Differential pressure	No
		Vibration	No
	Coolant to engine	Temperature	Some
	Coolant from engine	Temperature	Some
Lubricating oil	Oil	Chemical analysis	Some
	Tanks	Level	No
	Lines	Pressure	No
	Pumps	Differential pressure	No
		Vibration	No
	Oil to engine	Temperature	Some
	Oil from engine	Temperature	Some
Starting air	System	Pressure	No
	Compressor	Differential pressure	No
		Vibration	No
	Air Dryer		No
			No
Turbocharger or	Boost	Differential pressure	No
Supercharger	Intercooler	Inlet temperature	Some
		Outlet temperature	Some
	Charger	Vibration	No
Service water	Pumps	Differential pressure	No
		Vibration	No
Ventilation	Blowers	Air flow	No
		Vibration	No
	Dampers	Vibration	No

mately equal under either approach. Further, once OOS penalties incurred in preparing for and realigning the EDG after a test are taken into account, any unavailability increase could easily be compensated under our proposal by the OOS avoided through performance of a single test rather than 18 tests during a core's lifetime.

We propose the elimination of the intrusive inspections (which are a unique characteristic of the nuclear power industry). The reasons are that they very rarely reveal failures [11,13], are not based upon any experiences that justify the current practices, and offer opportunities to decrease the EDG reliability by introducing defects during the inspections and necessary reassembly and realignments. A typical inspection procedure is summarized in Table 3. The inspection practices of several industries utilizing EDGs are contrasted in Table 4. It is seen that the practices of these various industries differ greatly. When hospital practices are examined also (not shown in Table 4), they appear to be the most informal. These contrasts indicate that the nuclear power practices could probably be relaxed without harm.

With the advent of high capability informatic technologies, it has become possible to monitor the performance of components in much more detail than is the current power plant practice. When relaxing safety requirements, even though such a decision may be well-justified, it is also worthwhile to search for new ways to increase safety. The use of extensive on-line EDG monitoring offers one such opportunity. We investigated the feasibility of such monitoring as a way of compensating for the information lost should the practices of Table 2 be adopted.

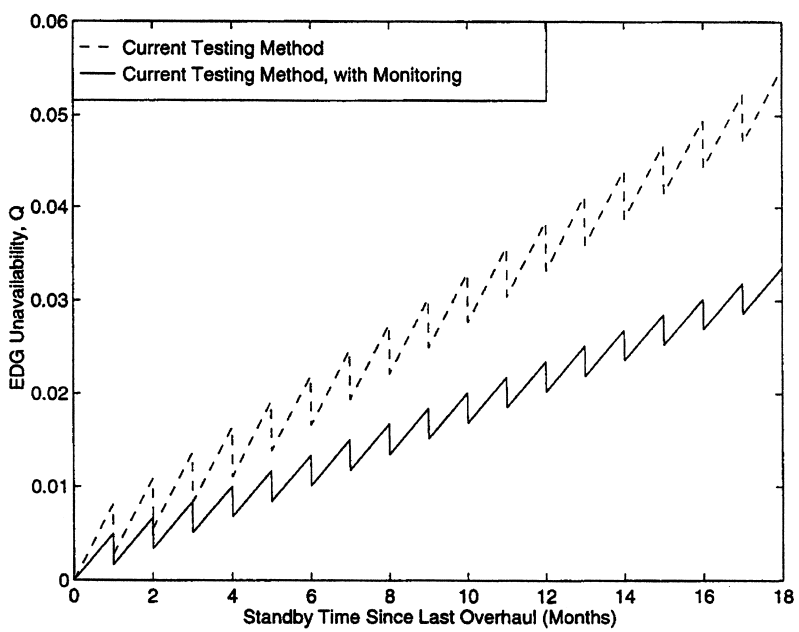

Fig. 4. Effects of monitoring upon EDG unavailability, contrasting current testing methods and testing combined with monitoring.

Table 6
Refueling outage inspection items recommended for replacement with engine analysis, monitoring or sensing activities

Item number from current ROI checklist	Current Colt-Pielstick requirement	Description	MP-3 diesel engineer recommendation
(2)	Remove and check injection nozzles for operation and opening pressure.	Injection nozzles spray fuel into the cylinder. The nozzles are subjected to a static test which assesses their spray pattern and opening pressure. Failure of the injection nozzle or pump will result in an increased loading on the other pistons to maintain engine power output.	The static test currently performed is not an accurate simulation of actual run conditions. *Engine analysis* would be more beneficial especially since this is an extremely intrusive practice. Also, there is evidence that the engine is not sensitive to minor failures of the injection.
(3)	Remove, disassemble, clean and repair all air start valves and air start distributors. Clean/replace air start distributor filter.	Engine starting is accomplished by the action of compressed air on the cylinders in their proper firing order. All valves and distributors must be completely disassembled and cleaned.	Short runs of the EDG tend to leave ''gunk'' which this inspection reveals. However, problems in this area can be revealed with the aid of *temperature sensors* on the air supply line. A periodicity extension to once every other refuel would be beneficial.
(9)	Check for tightness of exhaust manifold flange bolts to cylinder head (165–195 ft lb).	Proper tightness of bolts insures that significant exhaust leakage does not occur.	This practice is time-consuming and could be replaced with *exhaust leakage monitoring*.
(11)	Borescope all cylinder liners.	Borescoping of the cylinder liners involves inserting a viewing device into the individual cylinders. The borescope allows the inspector to identify areas of excessive wear.	This practice is unnecessary and extremely intrusive. No problems have been identified in the MP-3 diesels with this method and the liners always look brand new. *Engine and oil analysis* as well as *monitoring* of the firing pressure would reveal the problems this test was designed to identify.
(13)	Check crankshaft alignment and bearing clearances.	This test provides information about bearing condition and alignment of the crankshaft. Proper alignment is essential for operation of the diesel.	Web deflection is very intrusive and difficult to perform. It has never revealed problems at MP-3. *Vibration and oil analyses* would both reveal any problems.
(15)	Check alternator coils and poles for indication of movement (visual).	This inspection reveals problems caused by arcing within the diesel.	This inspection is not intrusive to the internals of the diesel but requires a great deal of outer disassembly to access the area. This practice is very time-consuming and could be replaced with *resistance monitoring*.

The monitoring system that we investigated is summarized in Table 5. This system would be capable of providing information about the occurrence of approximately 90% of the EDG fault tree basic events, which together contribute about half of the current EDG failure risk. The purposes of monitoring would be (most importantly) to indicate the incipient failure of the EDG by indicating that a basic event is likely to occur. Monitoring could also indicate past failures not interrogated directly by the test being performed. Depending upon the basic event indicated, one might shut-down for repairs, alter the intended component service or continue in service unaltered. Such monitoring would not provide perfect information and could introduce new failure modes. However, if these difficulties were to remain small, the implications of such monitoring would be to reduce the EDG unavailability by roughly half, as shown in Fig. 4. Such monitoring could also be useful for compensating for reduced inspections as is indicated in Table 6, which summarizes current inspections about which information could alternatively be obtained by monitoring. The main difficulty with our monitoring proposal is that the expertise needed for interpreting the data obtained has not yet been acquired, as these monitoring methods are not yet in use. Thus, an interval for learning the required lore would be needed before this proposal would be practicable.

2.4. EDG-related conclusions

Our results to-date indicate that most of the required EDG surveillances are not useful in improving 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.

3. The role of subjective judgement

In many situations in conducting the necessary analysis to apply RIPBR, knowledge limitations are likely to prevent conclusive answers from being formed. In both the Isolation Condenser (IC) system and EDG case studies, gaps in understanding and data prevent making unequivocal recommendations. For example, the dependency of the probability of failure modes upon time is not well-understood and data are often not available to determine the effect statistically. In the EDG case study, a final, definitive recommendation could not be made regarding whether to perform some planned EDG maintenance on-line or off-line.

When these situations arise, regulators have two choices. First, they can continue to use existing technical specifications until sufficient understanding exists (i.e. better models and data) to construct a conclusive case justifying otherwise. This approach implicitly freezes the status quo along with the problems inherent with prescriptive-based safety regulation. This is particularly important in situations where the status quo may be less safe than a proposed alternative. Furthermore, meeting such a high ''evidentiary''

standard may preclude the nuclear industry from undertaking the necessary research to justify changes in technical specifications. There is no point in investing the time and resources to investigate changes in requirements if these changes could never be completely justified.

The second approach to handling situations, in which lack of understanding and data prevent conclusive recommendations, would be justified on the basis that choosing between uncertain alternatives can be done using subjective judgement in situations where adequate data are lacking.

It may be safer for the career of a decision maker to avoid changing the status quo, as that path avoids the criticisms that are sure to come when a change turns our badly (as some surely will). However, to fail to change in some instances also can constitute a regulatory failure to achieve feasible safety improvements. However, in making such judgements, particular attention must be paid to evidence for the success or failure of current approaches. In order to do this successfully, one needs to establish a standardized process that addresses uncertainty. The objective of this process is to determine those situations in which it is preferable to change the existing technical specifications even without complete understanding and with inadequate data. The USNRC addresses uncertainty in specific programs targeting systems, such as in service testing, graded quality assurance, and containment pressure testing changes. These programs, however, do not address individual components.

Implementing this second approach requires two parts. First, expert opinions and beliefs about possible failure modes and their likelihoods need to be formalized as statements of probability, e.g., as probability distribution functions. For instance, in evaluating whether planned EDG maintenance should be performed on-line instead of off-line, considerations of uncertainties regarding the probability of human error may be necessary. Expert opinion would be solicited and converted into a probability distribution function [14,15]. Table 7 presents a proposed protocol for the solicitation of expert opinions [14].

Bayesian updating techniques also may be used to reduce uncertainty of failure probabilities and are particularly useful in determining responses to failures uncovered during testing. Failure probabilities are estimates and therefore have a range of uncertainty. This range of uncertainty can be updated as new information becomes available. For example, the failure probability of an EDG may be initially assumed to be a log normal distribution with a mean and a standard deviation based on expert solicitation. As testing occurs on a particular EDG, this initial distribution may be updated based upon the EDG's performance.

This updating process can also be used to establish testing criteria, including test frequency. For example, the standard could be that the probability that an EDG has a failure probability of 0.95 or less is 5%. When an EDG's probability distribution, updated based on test results, no longer meets this criterion, then additional tests must be conducted until it does. The USNRC has acknowledged this type of testing in its Regulatory Guide 1.108, *Periodic Testing of Diesel Generator Units Used as Onsite Electric Power Systems at Nuclear Power Plants*, which specifies a reliability goal of 99% at a nominal 50% confidence interval. This regulatory guide recommends that EDGs be tested more frequently based upon the number of failed test in the last 100

Table 7
Proposed protocol for the solicitation of expert judgement in uncertainty analyses

(1) Definition of case structures document describing the field of interest for which expert judgement will be required.
(2) Identification of target variables describing the parameter that needs to be subjected to formal expert judgement.
(3) Identification of the query variables describing the variables to be assessed by the experts.
(4) Identification of performance variables to be assessed by the experts.
(5) Identification of experts.
(6) Selection of experts.
(7) Definition of elicitation format document describing the exact questions and format for the experts elicitations.
(8) Dry-run exercise describing the try-out of the elicitation format document to a few experts.
(9) Expert training session describing the ingredients of training experts in preparing probabilistic assessments.
(10) Expert elicitation session.
(11) Combination of experts' assessments describing the methods with which the individual expert assessments will be aggregated to one combined assessment.
(12) Robustness and discrepancy analysis describing the procedures to show the robustness of the combined results.
(13) Feedback communication with the experts.
(14) Post-processing analyses describing the methods for processing the uncertainties of the combined expert assessments into uncertainties on the target variables from step (2).
(15) Documentation of the results.

tests. For example, EDGs that have failed one or less tests in the last 100 hundred are tested every month, whereas those that have failed four or more are tested every 3 days.

Second, experts need to review the PRA and engineering analysis conducted for a proposed technical specification change as a whole. The purpose of this review is to conduct a continual review of the analysis. This review takes into account factors

Table 8
Description of expert review processes used to review nuclear plant probabilistic risk assessments of plant management purposes

(1) Panels are formed with applicable expertise (maintenance, systems, PRA, plant procedures, etc.).
(2) Panels work in an iterative process with personnel performing the PRA.
(3) Panels address the limitations of PRA: limited level of detail and PRA scope.
(4) Panels seek consensus (i.e. most members agree); differences of opinions should be identified along with the rationale for these differences.
(5) Panels provide a well-documented pedigree documenting the decision-making process.
(6) Panels have consisted of utility employees and consultants; formal guidance on the use of inside vs. outside experts does not exist.
(7) In conjunction with the panel, a PRA certification process is routinely used.
(8) The panels, after considering defense-in-depth, engineering factors, the PRA and its limitations, margins of safety, form recommendations which are forwarded to the USNRC.
(9) These recommendations form the basis of risk-informed decision-making as opposed to risk-based decision-making.

omitted from the analysis and also utilizes the accumulated experience of the review panel. This panel would have a broader level of expertise than the group of experts solicited to quantify uncertainties, including PRA experts, system experts, and experts on plant procedures and characteristics. Informal discussion with the USNRC staff and the industry revealed that the USNRC at this time does not have a formal process to incorporate expert opinion and to commission expert panels. Table 8 summarizes one USNRC staff member's experience on how informal expert panels have worked in the past. [1]

4. Lessons learned

In performing the case studies described in this report, many unanticipated problems in modeling, data formulation and approximations were uncovered. Some of these problems are major and some are less important. Some are newly recognized; others are well known. The major problems confronted include:

1. Modeling human error;
2. Knowing when sufficient research has been conducted to permit a recommendation;
3. Treating uncertainty regarding component failure rates; and
4. Treating unjustifiable or hard to justify assumptions.

Less critical problems identified are:

1. Software differences between various PRA models;
2. Diffused system and component knowledge;
3. Short-term incentives for complying with existing USNRC requirements vs. long-term; incentives to change those requirements; these incentives drive for competition for limited resources;
4. Lack of USNRC credibility in following through and implementing RIPBR;
5. Problems of having a dual safety system consisting of deterministic and probabilistic based requirements;
6. The appearance of analyses being driven to produce desired results;
7. The difficulty in evaluating proposed changes across a wide range of plant-operating conditions;
8. Lack of consistency of assumptions; and
9. Lack of mechanisms for continually updating data, models, and analyses.

Three major lessons were learned as a result of this research. First, researchers need better data and understanding regarding individual component-failure modes that may cause components to fail. Not only are more data needed regarding failure rates, but more data and understanding are needed to enable analysts to evaluate whether these failures are more likely to occur as the intervals between testing are increased.

Second, the role of testing, given that a component has failed, needs to be worked out in more detail. This includes updating the prior distribution regarding the components failure rate and conducting testing or more frequent tests for some period of time.

[1] The Nuclear Industry Institute has a similar, but less detailed view on how expert panels should work [16].

Finally, limits to knowledge must be treated explicitly and formally. This treatment includes the formulation of probabilities through expert solicitation and the review of risk-informed, performance-based and engineering analyses used to evaluate proposed changes to existing technical specifications.

So, to achieve the full potential of RIPBR, it will not be sufficient to implement those changes to technical specifications that can be conclusively justified. Methods and processes that account for uncertainty and incorporate data as they become available into PRA are also needed. Accomplishing all of this will require a long-term commitment to data acquisition, model building and practical implementation. It is unclear that the organizations currently involved in RIPBR understand the scope of this task, and less that they are willing to make the efforts needed for success. However, it is important that they do so for without such an undertaking, it is questionable whether nuclear power can be made available in the USA as a long-term energy option.

Acknowledgements

The work reported here was sponsored by the U.S. Department of Energy through the University Research Consortium of the Idaho National Engineering and Environmental Laboratory as the project on Integrated Models, Data Bases and Practices Needed for Performance-Based Safety Regulation, and was performed in collaboration with INEEL and the Northeast Utilities Services.

References

[1] M.W. Golay, J.D. Dulik, F.A. Felder, S.M. Utton, Project on integrated models, data bases and practices needed for performance-based safety regulation: final report, MIT Report MIT-ANP-TR-060, December 1998.
[2] U.S. Nuclear Regulatory Commission Guide, 1.9. Rev. 3, July, 1993.
[3] P.W. Baranowsky, Evaluation of station blackout accidents at nuclear power plants: technical findings related to unresolved safety issues A-44, Draft report for comment, USNRC Report NUREG-1032, 1985.
[4] Title 10 of the Code of Federal Regulations, Part 50, Section 65 (10 CFR 50.65).
[5] USNRC, Use of probabilistic risk assessment methods in nuclear regulatory activities, USNRC Proposed Policy Statement, Fed. Register, Dec. 1994.
[6] USNRC, Regulatory guide 1.177 (draft guide DG-1065): an approach for plant-specific, risk-informed decision-making: technical specifications (predecisional), Draft, Mar. 2, 1998.
[7] USNRC, Program for elimination of requirements marginal to safety, Proposed USNRC rule, Fed. Register, Vol. 57, No. 227, Nov. 1992, pp. 55,157–55,161.
[8] M. Cunningham, PRA research program supporting risk-based regulation, Presentation to USNRC's Nuclear Safety Research Review Committee, 19 May 1995.
[9] NEI, Mission statement, NEI Regulatory Threshold Working Group, Mar. 1995.
[10] USNRC, Evaluation of station blackout accidents at nuclear power plants, NUREG/CR-1032, June 1988.
[11] G.M. Grant et al., Emergency diesel generator power system reliability: 1987–1993, Idaho National Engineering Laboratory Report INEL-95/0035, 1996.
[12] Colt-Pielstick PC2V Engine Instructions, 1983.
[13] U.S. Navy, Age Reliability Analysis Prototype Study, 1993.

[14] L.H.J. Goossens, R.M. Cooke, Procedures guide for the use of expert judgement in uncertainty analyses, Probabilistic Safety Assessment and Management '96, ESREL '96 and PSAM-III, Springer-Verlag, London, June 24–28, 1996.
[15] E. Zio, G.E. Apostolakis, Two approaches to model uncertainty quantification: a case study, Probabilistic Safety Assessment and Management '96, ESREL '96 and PSAM-III, Springer-Verlag, London, June 24–28, 1996.
[16] NEI, Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants, NUMARC 93-01, Revision 2, April 1996.