Protective Systems: Possible Extensions to the RoverD Method[☆]

Wen-Chi Cheng[a], Ha Bui Hoang[a], Tatsuya Sakurahara[a], Justin Pence[a], Zahra Mohaghegh[a], Ernie Kee[a,*], Seyed Reihani[a], Martin Wortman[b], Vera Moiseytseva[c], Fatma Yilmaz[d], David Johnson[e]

[a] *University of Illinois at Urbana-Champaign, Nuclear, Plasma, and Radiological Engineering*
[b] *Texas A&M University, Industrial Engineering*
[c] *YK.risk, LLC, Bay City, TX*
[d] *South Texas Nuclear Operating Company (STPNOC), Wadsworth, TX*
[e] *B.John Garrick Institute for the Risk Sciences, UCLA, Los Angeles, CA*

A method called "RoverD" is developed to address a specific USNRC generic safety issue (GSI), GSI-191 but it also believed to show promise for extension to cost-saving evaluations in other applications where a tested design level may be questioned against the need for adequate protection (primarily, radioactive release from LWR containments). The relationship of the RoverD method to USNRC Regulatory Guide 1.174 is summarized. The method is currently being applied to GSI-191, an issue that has been addressed by plant improvements, but focuses on the greater–than–designed debris loads could result in major insulation redesign costs (up to approximately $60,000,000) and worker radiation exposure (up to 200 REM).

While a plant Probabilistic Risk Assessment is needed as part of the implementation, the RoverD method, which is closer to hazard analysis is more efficient than methods that rely on detailed PRA. Amore efficient method such as RoverD to address emergent regulatory issues is related to the "Nuclear Promise" initiative. To illustrate where Risk-informed Over Deterministic (RoverD) could be extended to help meet the objectives of the Delivering the Nuclear Promise, a seismic example is shown.

KEYWORDS: Risk, RoverD, Risk–informed, PRA, Prescriptive, Deterministic, NEI Nuclear Promise

I. INTRODUCTION & BACKGROUND

Increased competition in the commercial electric sales market requires renewed focus on cost saving initiatives in the commercial Light Water Reactor (LWR) energy sector, and in this area, the Nuclear Energy Institute (NEI) is working on several fronts. It is likely there are potential cost and worker radiation exposure savings if risk assessment is used in a way that follows the method we call RoverD. The importance of the information summarized here on the methodology could help utility investigators bound the risk associated with uncertainty in risk-informed regulatory activities and is closely related to cost savings asked for in the "Cost & Benefit" lower tier initiative in the NEI "Delivering the Nuclear Promise" initiative.

In recent and ongoing work, methods have been developed that would evaluate the exposure to adverse consequences from hypothesized design basis Loss of Coolant Accident (LOCA) events. The RoverD approach has most recently been used to develop risk estimates used in a Generic Safety Issue 191 (GSI-191) analysis[?] . The work was motivated by the anticipation of costs, associated with GSI-191, that would be incurred if there were further improvements needed to meet increased performance standards on new strainer designs. U.S. LWR fleet made costly (perhaps as high as $10,000,000 at a dual-unit site) modifications to address concerns raised in GSI-191. The new strainer designs are robust against debris hypothesized to be freed by theoretically-posed Large Break Loss of Coolant Accident (LLOCA) events; however, the design standard used in some cases may be unable to meet the new standards for Zone of Influence (ZOI), defined later[?] .

In in late 2010,[?] the Advisory Committee on Reactor Safeguards (ACRS), was the inspiring force for taking a risk–informed approach to this problem. A method (later termed "Option 2" by the ACRS) was proposed and initially followed a methodology that could thought of as a "full PRA attack"[? ?] . In that method, Change in core damage frequency above a baseline level (ΔCDF) and Change in large early release frequency above a baseline level (ΔLERF) are found by finding the difference in the Core Damage Frequency (CDF) (and, similarly, Large Early Release Frequency (LERF)) for a theoretical Nuclear Power Plant

[☆] "Protective Systems" designates a series of risk assessment articles by the authors.

[*] Corresponding author
Email address: erniekee@illinois.edu (Ernie Kee)

(NPP) with no risk from the concerns raised in GSI-191 to the same NPP in the as-defined configuration (exposed to the GSI-191 concerns)[??]. That is, the NPP Probabilistic Risk Assessment (PRA) is supplied basic event probabilities developed from engineering models (for example a Uncertainty Quantification (UQ)) of accident progression phenomena.

In late 2014 and early 2015, we discussed revision to our approach with the Nuclear Regulatory Commission (NRC) (see NRC documents ML15020A106 and ML15034A114) to reduce review burden and to more readily address NRC needs in regulation. Of particular note is the regulatory need for a clear "speed limit", a well-defined region of operation that, when complied with, gives assurance that the plant is within accepted bounds. This concept is commensurate with NPP Technical Specifications (TSs) that have legally-defined bounds for operation. It is also conceptually consistent with understanding maximum hazard rate when scenarios associated with exceeding tested limits are assigned to catastrophic failure. Exceeding a "speed limit", does not necessarily lead to an automobile accident but is legally defined to help ensure 'safe' operation of the automobile. Safe would mean safer than traveling at a higher speed[?].

It may follow that other new design requirements, those that may arise following the initial NPP design, those that may challenge preexisting NPP design requirements, if evaluated quantitatively against the preexisting design standard(s), may be shown to meet an adequacy standard[?] prescriptive requirements and Risk Regions. Examples of such emerging requirements are in fire and seismic hazard analyses. In the following, thoughts are explored on how the concept of RoverD can be applied in these areas.

Use of the term risk in the RoverD method is clarified in Section II. Some issues using PRA for regulatory decision-making related to design issues have been found in related work. These issues are reviewed in Section III. How a design evolves from design requirements and design criteria in the NPP setting, is important for understanding where the design might function and where uncertainty exists. This is discussed in Section IV. In Section V is developed very simplistic analyses to show how RoverD may be extended to other issues not related to GSI-191. Conclusions are in Section VI.

II. RISK CONCEPT

In here risk is conceptualized as numbers; CDF, LERF, ΔCDF, ΔLERF; the acronyms associated with risk as defined previously are called "frequency" or "difference in frequency". Such numbers are normally arrived at through the solution of a well-constructed PRA; in each event tree branch point (split fraction) the sum probability for the branches is 1.0. The simplest possible example is an event tree like the one shown in Fig. 1.

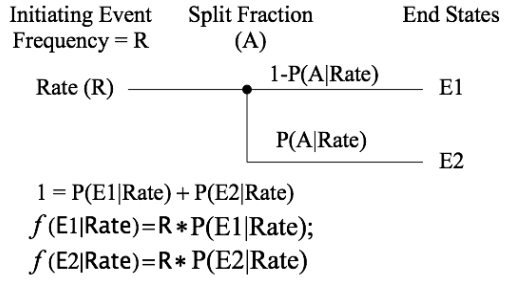

Fig. 1. An example of a probabilistic assessment with an event tree with split fraction, A, two end states, E1 and E2, stemming from an initiating event, Rate, having frequency, R.

? defined risk as the triplet {scenario, probability, consequence} but we have opted to adopt a definition closer to that used by the NRC*:

> "In that way, the Level 1 PRA provides the first measure of risk – core damage frequency ..."

That is, referring to Fig. 1, **?** would have p(E1|Rate) and p(E2|Rate) as probabilities, scenarios as E1 and E2, and the consequence(s) are those associated with the scenario (for example, core damage or large early release); frequency is not part of the definition. In here, the term 'risk' is used in a way that departs from the usual quantitative understanding[?] (rooted in liability assessment) and, which has a meaning closer to hazard rate. For a NPP that has operated without (catastrophic) failure up until the present time, the probability of catastrophic failure in the next instant of time is of interest.

In summary, the risk spoken about in RoverD is the frequency of scenarios (called 'risk-informed scenarios') that are proposed to exceed a known (deterministic) design goal in (ultimately) a protective system exposed to the scenarios. Catastrophic failure is equated to the risk-informed scenario frequency. The RoverD risk calculation method is explained in more detail in Section V.A.

III. SOME PRA CHALLENGES

An initial challenge faced in the full PRA attack involved linking probabilities from an UQ[?] where

*http://www.nrc.gov/about-nrc/regulatory/risk-informed/pra.html

compromises had to be made in order to reduce computational burden. While the method proved tractable, the approximations required for coupling the PRA with the UQ proved to be difficult to accept under regulatory review. In addition, uncertainty evaluation in the context of PRA application to a plant design issue is a relatively new regulatory setting. For example, the following quote reflects NRC concern with uncertainty distributions used in the PRA and the UQ[?] :

> "... LOCA frequency uncertainties sampled in the PRA uncertainty analysis are assumed independent of the probabilities of failure from the uncertainty analysis of CASA GRANDE.' This assumption does not account for the state of knowledge correlation because the PRA and CASA Grande rely on the same parameter for their quantification (LOCA frequency derived from NUREG-1829). RG 1.174, Section 2.5.2, 'Parameter Uncertainty,' states that the state of knowledge correlation should be accounted for unless it can be shown to be unimportant. Therefore, you are requested to either calculate CDF, LERF, ΔCDF, and ΔLERF accounting for the state-of-knowledge correlation or demonstrate that it is unimportant to this application." **?**

Fig. 2 is a conceptual model of the source of concern. As shown, the event tree is solved by sampling from the PRA initiating event distribution and the distribution obtained from $f(\cdot)$, a distribution obtained from independent sampling (independent of the PRA). It is likely the distributions associated with the PRA initiating event and $f(\cdot)$ are (potentially) highly correlated. Although methods to address the concern were investigated, this direct question and many others were ultimately unanswered and were instead resolved in the RoverD method.

Although it is believed, based on an understanding of probability, that PRA is incapable of accurately quantifying absolute failure frequency that is,

$$\begin{aligned} \textit{frequency} = &\textit{scenario probability} \times \\ &\textit{initiating event frequency}, \end{aligned}$$

it is thought to be possible to find a relatively accurate estimate of the difference between a "base PRA" and a perturbation to the assessment. This was the plan when the GSI-191 problem was first attacked.

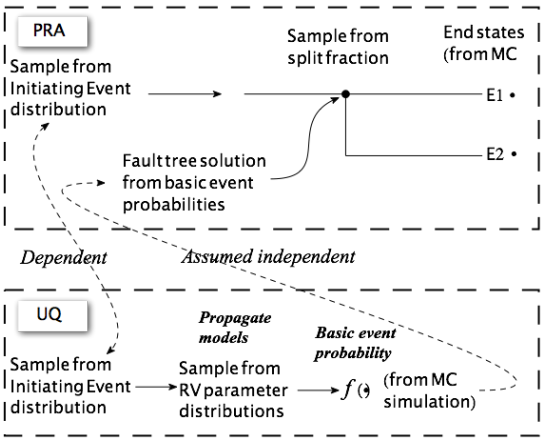

Fig. 2. The UQ random variable sampling scheme is independent from the sampling in the PRA making it possible the uncertainties included in the two are not treated properly. That is, dependencies are lost between the UQ and the PRA.

The idea was to evaluate as the base assessment, a plant with no concerns related to GSI-191, and in a second assessment, evaluate a plant that was exposed to the concerns raised in GSI-191. The difference between the two assessments was believed to be relatively accurate. Some further issues with the ability of the regulator to accept the PRA as being the basis on which to find adequate protection were recognized. In fact, the NRC risk philosophy requires adherence to prescriptive design standards such as Defense-in-Depth (DID), safety margin, and other standards defined in Appendix A to Part 50 of the Code of Federal Regulations, the General Design Criteria (GDC). In fact, these concerns are believed to be the motivation for the notion of "risk-informed" as used by the NRC in their documents and for a review of them on the use of risk assessment in regulation[? ?] . It became clear that the process of review for the full PRA attack would be costly and time-consuming; inconsistent with the NRC and industry goals for timely resolution and efficient resource utilization.

IV. DESIGN REQUIREMENTS

NPPs are (at least partially) designed following regulatory prescription as codified in Title 10 of the US Code of Federal Regulations; legally-defined federal codes. Of particular note are the GDC (Appendix A) for a specific prescription and other appendices that contain provisions for specific prescription (Appendix R and S are examples). In addition, implementation of the prescription is set out in regulatory guides. Sometimes the regulatory guides or other NRC guidance include

requirement elements that appear to go beyond the related prescription, a deterministic requirement level. It is well-established that the NRC is the body that makes decisions on required required design elements; adequate design is established by the NRC evaluation process, a "Safety Evaluation" [?] .

IV.A. Prescriptive Design

Appendix S to 10 CFR Part 50(IV)(a)(1)(ii) – 'Earthquake Engineering Criteria for Nuclear Power Plants, Application to Engineering Design,' regarding Safe Shutdown Earthquake (SSE) states:

> "The nuclear power plant must be designed so that, if the Safe Shutdown Earthquake Ground Motion occurs, certain structures, systems, and components will remain functional and within applicable stress, strain, and deformation limits. In addition to seismic loads, applicable concurrent normal operating, functional, and accident-induced loads must be taken into account in the design of these safety-related structures, systems, and components. The design of the nuclear power plant must also take into account the possible effects of the Safe Shutdown Earthquake Ground Motion on the facility foundations by ground disruption, such as fissuring, lateral spreads, differential settlement, liquefaction, and landsliding, as required in §100.23 of this chapter."

The central statement regarding Emergency Core Cooling System (ECCS) design for GSI-191 in Appendix A to Part 50(IV)(35)–'General Design Criteria for Nuclear Power Plants, Fluid Systems, Emergency Core Cooling' states:

> "A system to provide abundant emergency core cooling shall be provided. The system safety function shall be to transfer heat from the reactor core following any loss of reactor coolant at a rate such that (1) fuel and clad damage that could interfere with continued effective core cooling is prevented and (2) clad metal-water reaction is limited to negligible amounts."

In both of the legal requirements partially reviewed above, the language leaves no room for the possibility that, even using the best technology available, the legal requirement is not fulfilled. This is believed to lead to the notion of determinism in the design of each component and subcomponent used in support of these prescriptions Section IV.B.

IV.B. Determinism

In general, critical protective system Systems, Structures, and Components (SSC) in NPPs are designed and tested to the design, in which the design is based on legally-defined prescriptions. However, the design criteria for construction are commonly arrived at by including a significant level of safety margin in order to assure a high level of confidence (above any preciptive requirements) that the protective system will function when called upon. For instance, a value for electrical power support would include the safety margin inherent in the the codes and standards developed for (current carrying capacity, insulation resistance) as well as an assumption that, for each, the worst possible conditions would be present simultaneously. That is, the code may require a wire size that is capable of carrying substantially more current than the design current and, at the same time, the current requirement is established assuming an equipment demand under all maximum conditions for current draw. Fig. 3 illustrates how incremental design considerations lead to the total design requirement.

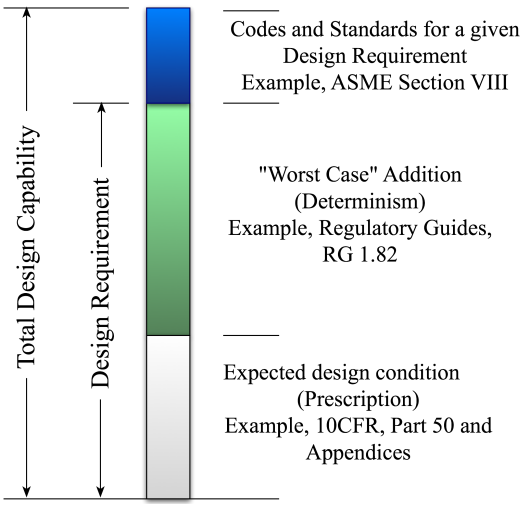

Fig. 3. Concept of determinism in design considerations where a prescriptive performance requirement is stated and where the design adds further requirements in assumptions and compliance with other codes and standards.

Critical protection system SSC are tested against the design requirement (Fig. 3). Such tests establish a level of performance for the equipment, generally under the "deterministic" condition. Unless tested at levels above the design re-

quirement, the level at which the total design requirement fails is unknown. That is, it is possible there is no margin beyond the design requirement, but the deterministic design method helps ensure that the design is robust against failure up to the assumed worst case level. The concept of an established, tested performance limit forms the basis for the 'deterministically' accepted scenarios, those scenarios that are assigned to success.

IV.C. Summary

The design elements of prescription and determinism lead to a protective system design that, when tested successfully, is highly likely to fulfill the design requirement (Fig. 3) that, in turn, meets the functional need; accident prevention. Therefore, there is high confidence that challenges from scenarios within the affected protection system or subsystem design requirement will be successfully met. Greater challenges may be met as well, but there is uncertainty in the absence of definitive testing. There is, therefore a reluctantance to consider successful operation for greater challenges.

V. EXTENDING RoverD

The concept of RoverD is that protective system equipment have been successfully tested to certain design requirements (Section IV). Such equipment is highly likely to succeed for challenges within the design requirement; we have no substantive reason to believe those challenges would not be met. This concept of a design that is effectively guaranteed against failure up to some level and that, beyond that level, failure is (conditionally) certain, is the kernel idea of RoverD used in GSI-191. There may be other protective systems that are, or will be, challenged if new design criteria are promulgated.

V.A. Original RoverD Results

This is how the RoverD method works. Scenarios are developed, based on accepted design standards, that evaluate whether or not a design requirement for a NPP component is challenged due to new information or design flaw. For example, if a pressure vessel in a system is designed for 100psi and a concern is raised that, under some circumstances, the pressure requirement should have been 120psi, then scenarios would be developed to find ones where the pressure exceedes the (existing) 100psi design pressure; for this hypothetical example, such scenarios may be related to an inadequate relief valve discharge rate for cases where a pressure control system fails. The notion is shown in Fig. 4 where Scenario 1 and Scenario n are shown as exceeding the design requirement. Any scenario that exceeds the current design performance threshold is assumed to be in the "risk-informed" category. The frequency with which scenarios exceed the threshold is taken to be catastrophic failure frequency (hazard rate). Once the frequency of occurrence for these scenarios is known, this frequency is assigned as the consequence frequency for the pressure vessel failure.

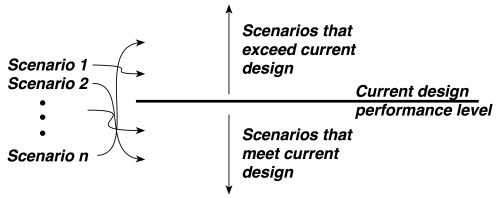

Fig. 4. Concept of a threshold based on tested performance that could be exceeded in some hypothesized scenarios.

Specifically in the GSI-191 issue, the hazard is associated with debris plugging up the ECCS suction strainers in the recirculation mode which is *ASSUMED* to occur when an amount of debris exceeding the design requirement test is exceeded[?] . The new design requirement in this case was the assumed amount of debris created in a LOCA; for example, the existing design is based on ZOI (the non-dimensional destruction radii) of 7D for fiberglass insulation, later revised to 17D. Scenarios were developed that examined each location where it would be possible to exceed the tested amount; frequencies were then derived for the scenarios from estimates of piping ruptures causing LOCAs[?] . A more complete description is by**?**

The RoverD GSI-191 showed that the hazard rates, equated to ΔCDF (and derived to ΔLERF), posed by the new design requirement is less than the thresholds defined for where changes are not allowed **?** , Figures 4 and 5. These values, as means, were determined to be 1.5E-07 per year for ΔCDF and 3.75E-10 per year for ΔLERF. For more detailed results and discussion, see[?] Attachment 1–3, Tables 9 and 10.

V.B. Example: Seismic

When new design criteria are posed that indicate a more robust design for some tested protective equipment, RoverD could be used to assess the potential risk. In the same way as done in the GSI-191 issue, affected scenarios are assumed to cause catastrophic (for example, core damage or possibly large early release of radiation) failure and their hazard rate could be taken as a change

in frequency of occurrence of those (catastrophic) failures.

An area of relatively intense research focus is earthquake prediction, locations and magnitudes. It is reasonable to assume that, as new information becomes available, NPPs may be exposed to new, potentially costly (as in GSI-191, worker radiation exposure and plant modification costs) design requirements leading to redesign. As in GSI-191, some modifications may need to be made, or may have already been made, to improve the response to earthquake; therefore, existing design is evaluated against the new requirements to make these decisions.

In the following RoverD is considered for use to evaluate the importance of new information or new requirements related to earthquake that challenge an existing design. The tenets for Probabilistic Seismic Hazard Analysis (PSHA) described by the NRC, are followed in developing the inputs to the analysis, are followed[?] . The understanding of earthquake behavior, especially against Peak Ground Acceleration (PGA), is highly uncertain has been recognized[?] .

The seismic example is very appealing with regard to RoverD because, in essence, the PSHA comes down to a list of scenarios, each having a magnitude, location, and rate of occurrence. Because NPPs are designed for a specific earthquake, the protective system equipment is designed and tested to the earthquake standards at the time of manufacture (or following subsequent modifications). As a consequence, there is high confidence that the protective system equipment will perform for all challenges within the design requirement; however, if new scenarios are proposed that exceed the tested design, then RoverD would have them (conditionally) assigned to failure.

System description Consider a hypothetical NPP consisting of two redundant systems, S_k, each arranged in series and indexed by $k = 1, 2$ designed to protect against core damage. Each redundant system has at least one piece of equipment, $X_{k=1,q}$ and $X_{k=2,p}$, in series with fragility, $f_{k=1,q}$ and $f_{k=2,p}$, indexed by $q = 1, 2, \ldots, Q$ and $p = 1, 2, \ldots, P$, each ordered from the most fragile to least. That is, in each of the two systems, $X_{k=1,q=1}$ and $X_{k=2,p=1}$, the most fragile pieces of equipment are found.

Now it is hypothesized that a new seismic requirement has been promulgated for the NPP site (Fig. 5) with a PGAs greater than the current design requirement. In Fig. 5, the frequency at any point on the curve corresponds to that frequency and greater, which forms an "exceedence" curve.

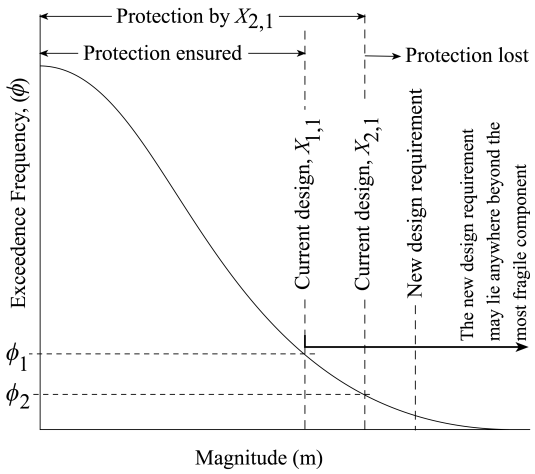

Fig. 5. Location of equipment failures for two equipments, $X_{1,1}$ and $X_{2,1}$ on a frequency exceedence curve for earthquake magnitude. A new design requirement is shown that would require fewer fragile components; in this case, both $X_{1,1}$ and $X_{2,1}$.

In Fig. 5 an example where both systems' highest fragility equipment are designed with PGAs less than the new requirement's PGA; m_{new} with frequency ϕ_{new} have been chosen. In general, it is expected that the new requirement should only exceed one or more systems' highest fragility equipment, $m_1, \leq m_2, \leq m_{new}, \leq m_3, \leq \ldots$. In this case, the systems with less fragility than the new design requirement would not be included in the hazard assessment (for increased hazard rate) and K would only run to the index of the system with smallest difference, $m_k - m_{new}$.

PRA The NPP PRA is used to develop the frequencies relevant to protective system functions that successfully operate in a Design-basis (DB) seismic event. From the PRA success frequencies are taken for the two systems, when both succeed, and when only S_2 succeeds, say $\omega_{k=1}$ and $\omega_{k=2}$. Frequencies, ω_i, are weights for the calculation of the seismic failure rates that go Beyond Design Basis (BDB) (taken to be scenarios where equipment is challenged beyond the design requirement of Fig. 3).

Hazard rate An additional hazard rate, H, is calculated, considering the new seismic data against the existing earthquake design magnitude exceedence frequencies, ϕ_k, for $X_{k,1}$ in a general way:

$$H = \frac{\sum_{i=1}^{K} \omega_i(\phi_i - \phi_{i+1})}{\sum_{i=1}^{K} \omega_i},$$

where $\phi_1, \geq \phi_2, \geq \phi_3, \geq \ldots, \geq \phi_{j=K}, \phi_{K+1} = 0.0$.

For the case shown in Fig. 5, the evaluation would be:

$$H = \frac{\sum_{i=1}^{2} \omega_i(\phi_i - \phi_{i+1,\,\phi_i<\phi_{i+1}})}{\sum_{i=1}^{2} \omega_i},$$

$$H = \frac{\omega_1(\phi_1 - \phi_2) + \omega_2(\phi_2 - 0.0)}{\omega_1 + \omega_2}.$$

This extremely simple example is developed for illustration and clearly leaves out many elements of the supporting analysis such as common cause (an example would be support structure failure that may be realized before component failures at the new requirement) needed to obtain a reasonable result. The hazard rate that is obtained this way, however, is reasonably conservative:

1. It is likely the total equipment design capability (Fig. 3) although not known from testing, includes some safety margin.

2. In addition, the design requirement (again referring to Fig. 3) by using determinism as a basis, includes a factor of safety.

The hazard rate stemming from new requirements against the current design is calculated based on the definition givrn above. If the hazard rate is calculated to be sufficiently low, there should be no reason to take additional action. If otherwise, steps should be taken to meet the new requirements with high probability. The RoverD seismic example shows how the decision maker would make the determination as to whether the equipment is safe or not by calculating the additional hazard rate for each equipment design affected.

VI. CONCLUSION

In the face of increased competition in the electrical energy production market, innovation is indicated when challenges to existing designs arises. The motivation for innovative methods such as RoverD includes worker radiation exposure and incremental costs for production.

Concerns related to uncertainty in the PRA may result in schedule delays and excessive resource requirements in both regulatory and industry resolution efforts. The RoverD method helps provide a way to: (a) establish a clear boundary beyond which scenario outcomes are uncertain and; (b) quantify the associated risk in a way that can be compared to regulatory guidance.

This shares ideas on how RoverD might be extended more generally to problems the commercial nuclear power industry faces as design standards evolve or new information becomes available; those where hazard rates for catastrophic events may be underestimated by the current design. When hazard rates are found to be less than the criteria provided in guidance, design changes and the associated costs can be avoided[?] .

REFERENCES