PUBLIC SUBMISSION

As of: 1/21/22 9:52 AM
Received: January 20, 2022
Status: Pending_Post
Tracking No. kyn-k1y9-bgs3
Comments Due: August 31, 2022
Submission Type: Web

Docket: NRC-2019-0062
10 CFR Part 53: Risk-Informed, Technology-Inclusive Regulatory Framework for Advanced Reactors

Comment On: NRC-2019-0062-0176
Risk-Informed, Technology-Inclusive Regulatory Framework for Advanced Reactors

Document: NRC-2019-0062-DRAFT-0218
Comment on FR Doc # 2021-26877

Submitter Information

Email: erniekee@illinois.edu
Government Agency Type: Local
Government Agency: HaztechRisk.org

General Comment

In a letter to Dr Nathan Siu attached to this comment, we recommend caution regarding over-reliance on risk quantification of measures such as core damage frequency and large early release frequency in regulations on power reactors. We have found that such quantifications are guaranteed to be unconditionally optimistically biased. Our findings are summarized in the letter to Dr Siu attached to this comment.

Attachments

Siu-1.20.2022 signed mw ek

HazTechRisk.Org
2221 Market St.
Galveston, TX 77551

January 20, 2022

Nathan Siu, Senior Technical Adviser for Probabilistic Risk Assessment
Office of Nuclear Regulatory Research
Nuclear Regulatory Commission
One White Flint North 11555 Rockville Pike
Rockville, MD 20852-2738

Dear Dr. Siu,

In his recent editorial ("Laws and sausages," **Nuclear**Newswire – *10 CFR Part 53 – ANS*), Steven Nesbit appears to criticize the NRC for continuing reliance on prescriptive regulations and slow walking the risk informed, performance-based regulations mandate of the NEIMA.[1]

> "While it may be possible as a workaround to apply the current prescriptive regulatory framework to some reactors early in the pipeline, it is neither practical nor desirable to do so in the longer term for the range of advanced reactor technologies that are proceeding toward deployment."

Mr. Nesbit emphasizes that risk informed, performance–based regulations should direct advanced reactor licensing. We are concerned that the NRC may be influenced by advocates, such as Mr. Nesbit, to rely too heavily on quantification of robust protective system risk measures that cannot be validated and more importantly, are guaranteed to be optimistic.

We believe risk analyses certainly should be undertaken, but only up to the point of quantitative assessments. The November 23, 1988 version of Generic Letter 88-20 advocates, in part, what we believe to be a good risk management strategy, perhaps a "best practice" in the absence of validation data.[2]

> "Therefore, we request each licensee to use its staff to the maximum extent possible in conducting the IPE by:

[1] `https://www.ans.org/news/article-3579/laws-and-sausages10-cfr-part-53/`. Accessed 01/20/22.

[2] `https://www.nrc.gov/reading-rm/doc-collections/gen-comm/gen-letters/1988/gl88020.html`. Accessed 12/20/2022.

1. Having utility engineers, who are familiar with the details of the design, controls, procedures, and system configurations, involved in the analysis as well as in the technical review, and
2. Formally including an independent in-house review to ensure the accuracy of the documentation packages and to validate both the IPE process and its results."

Accurate quantification of risk in robust protective systems must rely on computational stochastic modeling that does not exist today, and cannot be achieved in the future. Therefore, most who would promote quantified risk measures in risk informed regulations have ignored stochastic process theory on which all such predictive models rely. In particular PRA, the prevalent risk assessment methodology in the industry, is crafted without reference to a filtration on the underlying probability space. Although industry practitioners may be willing to ignore it, we believe the NRC cannot pass over this shortcoming. We are concerned that such a modeling simplification introduces an unquantifiable optimistic bias into important stochastic performance metrics including the primary risk measures used by the NRC such as CDF and LERF. We believe the magnitude of such a bias cannot be understood absent data (which we hope to avoid collecting) on these measures. In addition, lack of experience with new technologies contemplated in the NEIMA would tend to exacerbate such optimistic bias. We summarize our thinking about our concern in what follows.

Quantifying predictive models requires all random variables to be defined on a probability space. For example PRA quantification, either explicitly or implicitly, assumes a probability space that we designate $(\Omega, \mathcal{F}, P)$. To be complete, a predictive modeling framework requires the imposition of a filtration $\{\mathcal{F}_t\}_{t\geq 0}$ onto the basic probability space. The purpose of the filtration is to capture the state of engineering knowledge over time (for example, unexpected failure modes encountered in operation.) The complete probability space is then properly represented by $(\Omega, \mathcal{F}, \{\mathcal{F}_t\}_{t\geq 0}, P)$. From an engineering modeling perspective, the filtration provides the necessary analytical construct for acknowledging the possible existence of the undiscovered protective equipment failure modes that will be encountered over time.

$\mathcal{F}_t$ is a sub–σ–algebra of $\mathcal{F}$ sufficiently large to accommodate the state of engineering knowledge at a given time $t \geq 0$. $\mathcal{F}_{t=0}$ can only contain failure modes known at time $t = 0$ typically defined in the FMEA or prior root cause analyses. During ongoing operation, arriving initiating events may reveal additional failure modes as determined by root cause analyses that were unknown to exist up to their discovery. Thus, the filtration $\{\mathcal{F}_t\}_{t\geq 0}$ becomes

a monotonically increasing sequence of σ-algebras such that $\lim_{t\to\infty} \mathcal{F}_t = \mathcal{F}$. Many examples of such unexpected failures are found in the NRC LER database for every operating plant. The regulatory process expects such failures in power reactors and regulates management of them through such regulatory mechanisms as for example, Title 10 CFR Part 21.

It is important to appreciate that the time at which any remaining undiscovered modes is first discovered is not $\mathcal{F}_t$-measurable. That is, the time of first discovery cannot be assigned a probability. And, since an arriving initiating event can lead to a discovery of a heretofore unknown protection failure mode, it follows that for any time $t > 0$ there exists a class of initiating events, that possibly lead to core damage or radiation release, having arrival times that are not $\mathcal{F}_t$–measurable. Engineering intuition does not fail; we are simply recognizing that one cannot assign a probability measure to events beyond one's knowledge of their existence.

Risk analytics, such as is done in PRA, sidestep these measurability (and other) issues by assuming large t. When the filtration $\{\mathcal{F}_t\}_{t\geq 0}$ has converged or $\mathcal{F}_{t+s} = \mathcal{F}_t = \mathcal{F}$. Here, the filtered probability space reduces to the usual probability triple $(\Omega, \mathcal{F}, P)$ needed to support computational predictive models. But, a necessary condition for convergence of the filtration is that all failure modes have been discovered.

From our understanding of the modern theory of stochastic processes we assert the following,

1. So long as undiscovered protection failure modes exists, risk quantification calculations are optimistically biased.
2. Absent measurability with respect to an appropriate filtration, it is impossible to quantify or bound the bias.
3. Even with achieving stationarity in the filtration, the bias in quantification (e.g., CDF) remains as a direct consequence of the well-known Arrival Theorem.
4. Items 1–3 indicate to us that there would be no productive purpose would be served in root cause analysis advocated by the NRC and contrary to engineering practice in hazardous process management.

Our understanding, stated intuitively is this; Risk informed, performance based regulations ignore the dangers of "unknown–unknowns"; prescriptive regulations offer a powerful engineering strategy for mitigating the consequences of unknown-unknowns. Acknowledging the consequences of unknown-unknowns is particularly important when regulating protection in immature nuclear technologies and in the current operating fleet where robust protection (desirably) produces no validation data.

We are worried that, from the public's perspective, there is no such thing as a "small nuclear accident". Any nuclear accident, especially with emerging technologies, could be the death knell for the already stressed civilian nuclear industry. Returning to Mr. Nesbit in his recent article, he writes,

> "When it comes to the challenge of transitioning to a new licensing framework, we should adopt a talk/act/check/adjust mode–more of a SpaceX model for regulations."

SpaceX has lost nine (9) rockets to fiery explosions over the last 12 years. We believe a record like that in the U.S. nuclear industry would have ended the domestic program.

We believe you, as the lead risk researcher at the NRC, would best understand our concerns and discuss with the Commission the potential harm that may come from regulatory strategies that put excess faith in risk quantification technologies. As summarized in here, our concern is that, at the level of quantification, we believe risk assessments ignore important and foundational principles that unconditionally cause such quantifications to produce overly optimistic performance expectations.

Regards,

Martin Wortman and Ernie Kee