

Attachment 1

Document Structure

The document is well written but bulky, which makes it difficult to get to the essential elements of the guidance. We suggest that the ISG be structured as follows:

- Implementation
- Executive Summary
- Purpose
- Guidance
- Appendices – remaining content of document

By structuring the document in this format, its purpose will be clear and the reader will reach the guidance portion of the document with greater ease.

Common Cause Failure

The insights and conclusions in this document are not based on adequate consideration of the design advances that the industry has developed to minimize common cause failure (CCF) of digital systems. The designers of digital I&C systems have studied the historical causes of CCF, and have provided effective defenses in the state-of-the-art digital systems as discussed in draft IEC Standard 62340. These features include tools to improve the quality of the software development life cycle, platform and operating system (OS) features to minimize the likelihood of CCF triggers, platform and OS features to prevent propagation of failures to other functions, and functional diversity. The guidance should be revised to acknowledge the ability of the designers to address such failures and assure that such features are incorporated in the analysis.

Risk Insights

This document discusses risk insights from the evaluation of advanced reactor PRAs; however, as noted in the document, only high-level modeling was possible because the details of the digital I&C system design have been postponed until the COL stage. Due to this lack of detail, there are significant conservatisms regarding the probability of software CCF and the ability to recover from these failures. Some of the insights drawn from the evaluations of advanced reactor PRAs are based on overly conservative assumptions about the probability of software CCF, such as the hypothetical platform-wide CCF that has been assumed in the referenced advanced reactor PRAs. Given these extensive conservatisms and the low overall CDF for the advanced reactors, it is not surprising that the RAW of the software CCF can be very high. This is not a reflection of high absolute risk significance. The use of RAW values here can be misleading, and the paper should include additional perspective relative to the statements of high RAW values in regard to absolute risk and current plant risk metrics.

Modeling Methods

The document makes a number of statements suggesting a lack of consensus in the technical community as to whether current digital I&C modeling methods are acceptable. The bases for these statements are unclear, and should be supported with references, as the domestic nuclear industry, the Department of Energy, foreign utilities and non-nuclear organizations (such as NASA) routinely model digital I&C in PRA related applications. A more accurate assessment is that there are methods currently available to model digital I&C in PRA, but that the NRC staff has yet to formally approve them.

Internal Inconsistencies

The document is inconsistent in its discussions regarding the adequacy of submitted PRAs. On the one hand, the document states that we cannot adequately address digital failure probabilities, thus BTP-19 cannot be risk informed; yet on the other hand, this ISG states that the current PRAs submitted are adequate to show that a DAS is required.

The document is also inconsistent in its discussion of conservatism in PRAs. The nature of PRA is to use best estimate information, and use of conservatism in portions of the model can lead to misleading conclusions. This document reinforces this position, stating on page 9 that, “while bounding PRA analyses may provide needed insights in very specific cases, the Commission has made it clear that it believes that realistic risk assessments should be performed whenever possible since bounding analyses may mask important safety insights and can distort a plant’s risk profile.” Yet the executive summary and introduction repeatedly point to the high RAW for two advanced reactor DI&C software failures without noting that the PRAs are not necessarily highly detailed (especially in the area of recovery), and therefore potentially overly conservative.