Risk informed treatment of Embedded Digital Devices (EDD)

Raymond Herb
Southern Nuclear

Embedded Digital Devices Workshop
October 9, 2014 • NRC

Purpose

- Introduce the concept of using risk informed concepts for graded approach to quality processes for Embedded Digital Devices (EDD)
- Establish a dialog between design and risk informed engineering in both the NRC and Industry with respect to risk informed quality
- This dialog does not commit to any one party to a particular method or idea at this time.

Introduction

- EDD and their presence in new and replacement components used in nuclear plant systems in only going to increase over time. Quality aspects must be addressed.
- This discussion includes the evaluation of the impact of Common Cause Failure (CCF) on risk but this presentation is not intended to speak to CCF applicability, avoidance or mitigation.

Digital Requirements of EDD

- The difficulty facing EED are no different that any other digital changes, they are susceptible to the same issues; primarily,
  - how do you adequately determine quality and,
  - how do you adequately address common cause failures.

Quality of EDDs

- Currently there are only two classifications that drive quality standards
  - safety-related and
  - non safety-related

Safety related Quality

- With only little room for interpretation in what quality standards are applied, for safety related, quality standards are in general for digital components are compliance with IEEE-603 and IEEE 7-4.3.2,
  - these standards do not contain an endorsed graded approach.
  - Proposed rule changes to 50.55a(h) could make this even more rigid across the safety related classification.

Options for Risk Informing 50.55a(h)

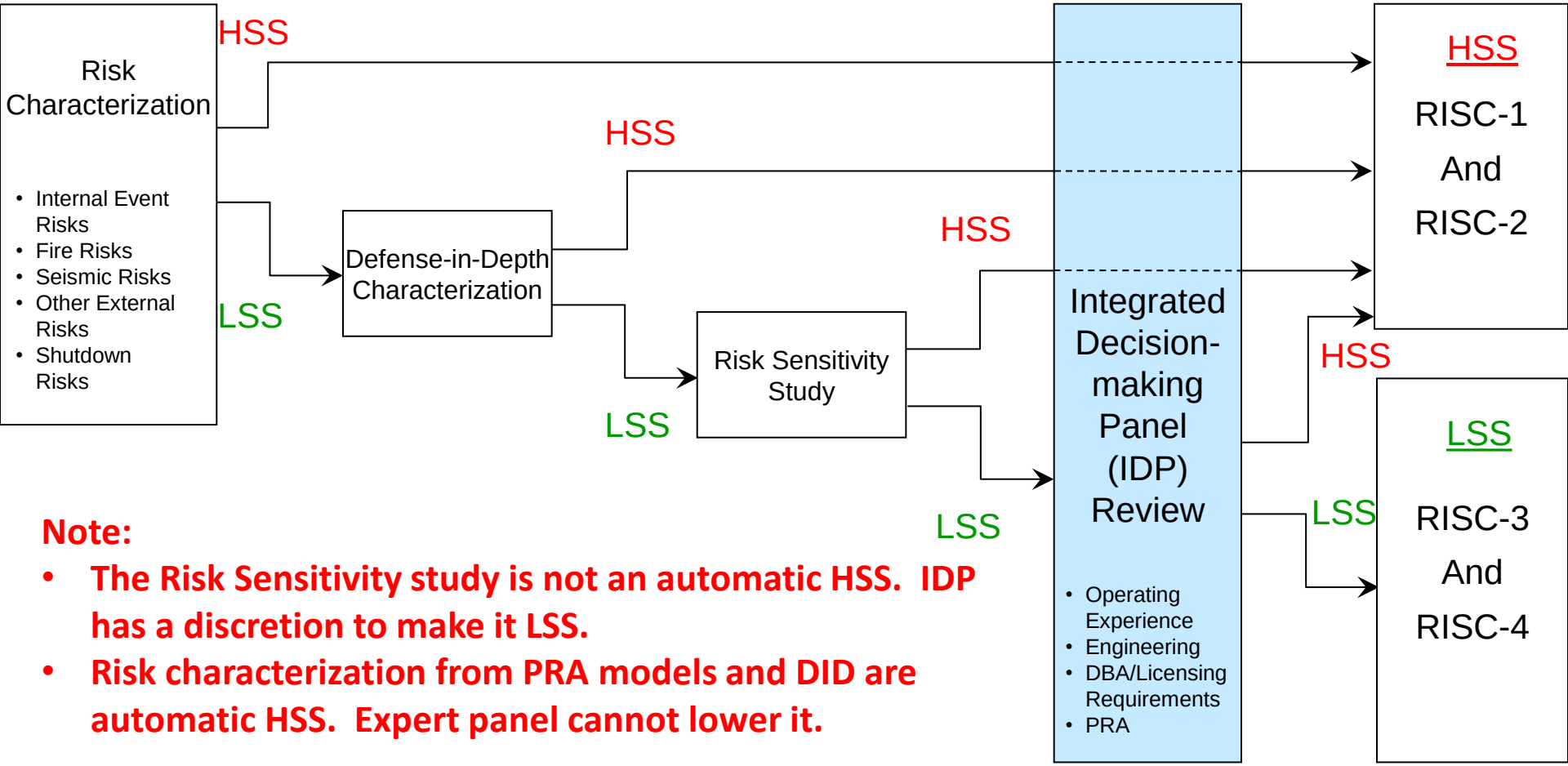
- Voluntary Risk based regulation exists
  - Limited plant sites have implemented 10CFR50.69
    - 10CFR50.69 can be used to categorize SSCs by risk and allow graded application of special treatment.
    - NEI 00-04 is the endorsed guidance on categorizing SSCs
  - Numerous plant sites have implemented applications under Reg Guide 1.174
    - Many successful submittals with a strong consensus that the development and use of this regulatory guide has been a major success story (e.g., Tech Specs, ISI, IST).

Risk informed Categories for 50.69

10CFR50.69

RISC-1 Safety-Related, Safety Significant	RISC-2 Non-Safety Related, Safety Significant
RISC-3 Safety-Related, Low Safety Significant	RISC-4 Non-Safety Related, Low Safety Significant

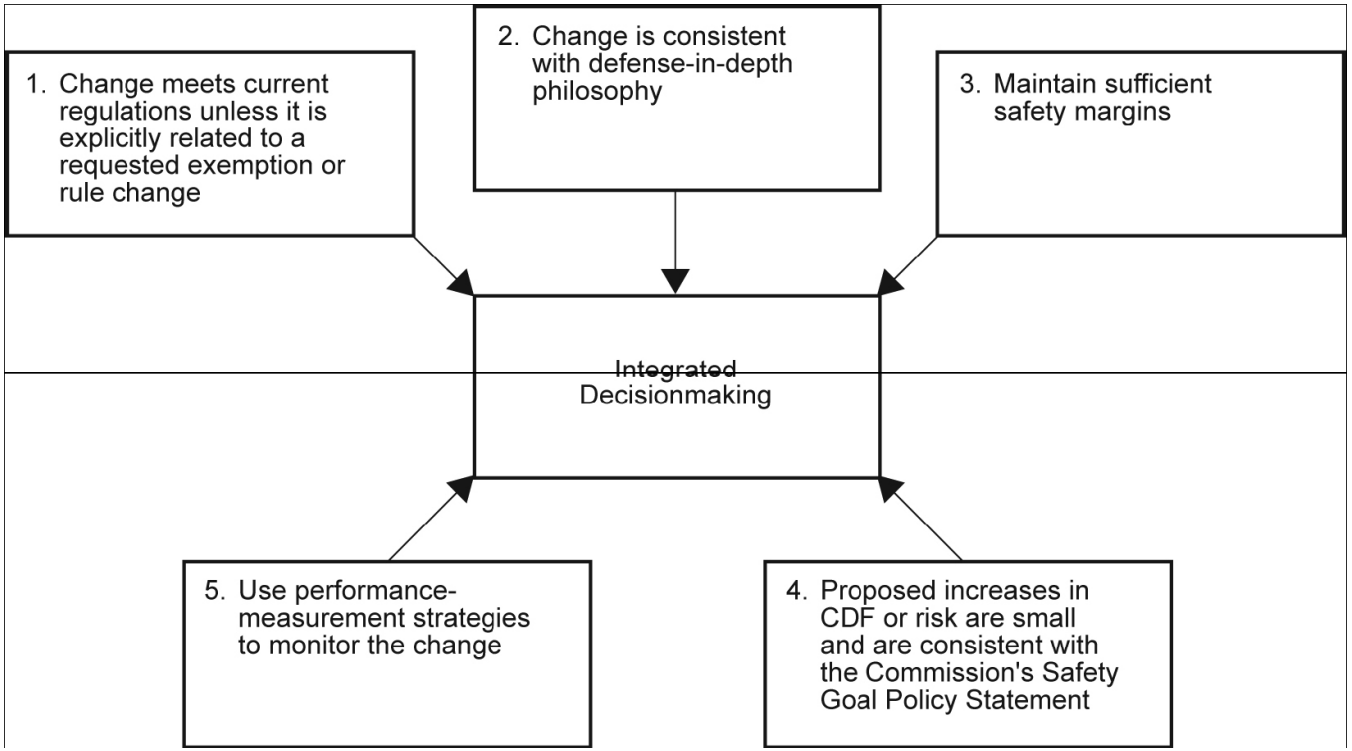
NEI 00-04 Categorization



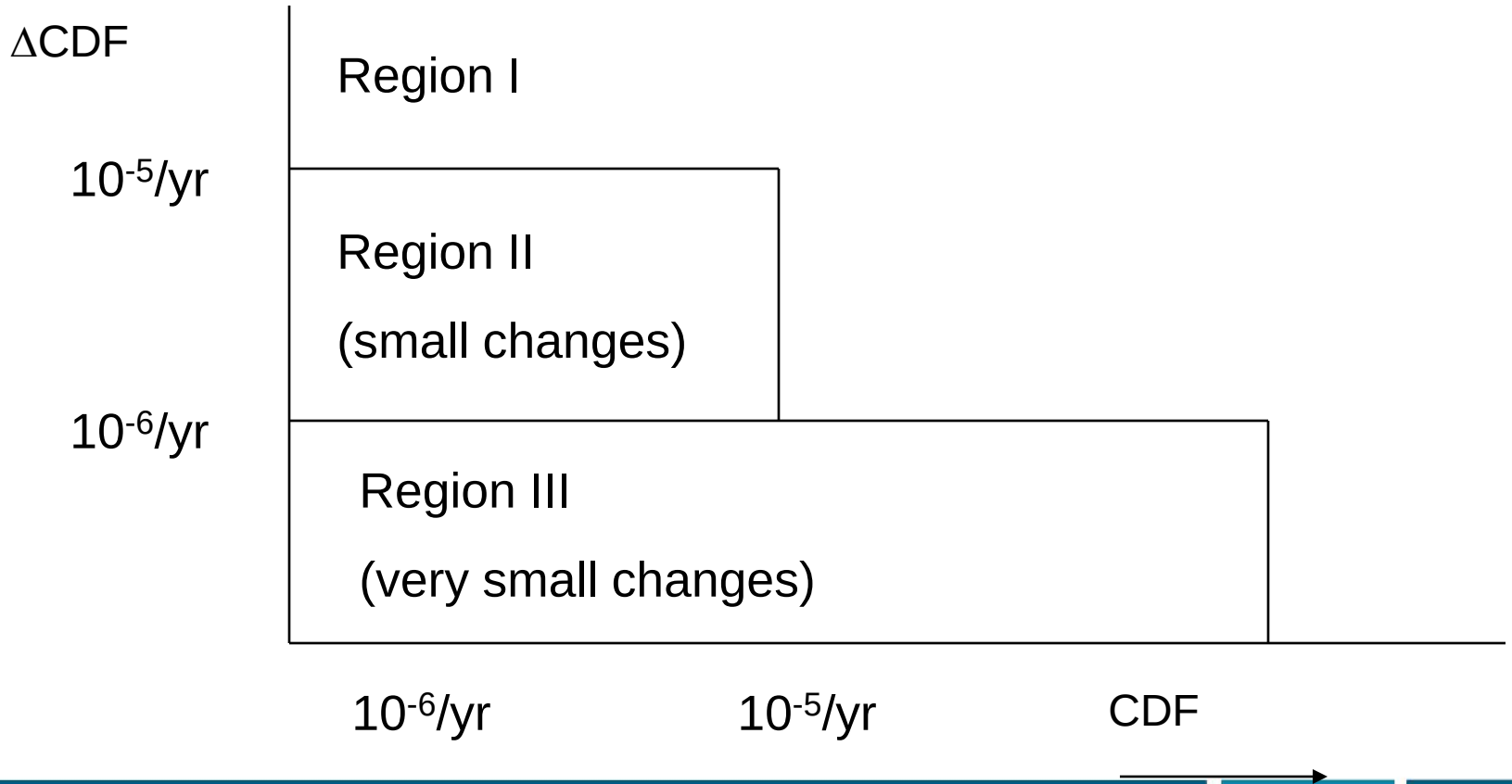
Note:

- **The Risk Sensitivity study is not an automatic HSS. IDP has a discretion to make it LSS.**
- **Risk characterization from PRA models and DID are automatic HSS. Expert panel cannot lower it.**

Principles of Regulatory Guide 1.174



Change in Risk Guidance of Regulatory Guide 1.174



The benefits of Risk Informed

- Tailoring of the current monolithic standards written to address high safety significant systems, to lower significance EDD can save effort and review time
- Industry and Regulatory focus directed where it belongs, on high safety significant systems, will serve to increase the margin of safety and decrease the burden on both regulator and industry.
- Risk informing all plant systems will help in determining what systems need to have additional scrutiny in the specific digital areas of software quality and CCF.

High Risk EDD, business as usual

- Safety related high risk components will still be required to meet all the prescribed standards and guidance to ensure full safety related quality under the plant Appendix B program
  - BTP 7-14 where applicable or at a minimum the use of the
  - NRC approved Commercial Grade Dedication process detailed in EPRI 106439, which is reserved for those commercial grade components that were not developed under a safety grade plan as detailed in BTP 7-14 but can be shown to be equivalent.

Relief for low risk safety related EDDs

- 10CFR50.69 – For those components that grade as low risk significant (RISC-3), the full requirements for safety related quality need not be applied
  - The plant is still required to provide reasonable confidence that the SSC will perform it's safety related function
- Reg Guide 1.174 – Focus would be on those EDDs collectively shown to manage risk in Region III
  - Where existing regulations would not be met for low risk EDDs, justification (i.e., an exemption request) would be needed per the first principle of Reg Guide 1.174.

Suggested Definition

- **Reasonable Confidence** - A level of confidence based on engineering evaluation which should be supported by facts, actions, knowledge, experience, and/or observations. The term actions constitute verifications, calibrations, tests, or maintenance activities.
  - Reasonable confidence is a somewhat reduced level of confidence compared to the relatively high level of confidence provided by the current special treatment requirements.

What about non-safety EDDs?

- Risk informed categorization of non safety-related components will result in additional scrutiny, based in actual plant risk, for those that perform safety significant functions.
  - 10CFR50.69 – The rule requires that Non safety related EDDs meet the existing assumptions and that they will perform their (or not interfere with a) safety significant function.
  - Reg Guide 1.174 – Non safety related EDDs must be designed, maintained and monitored in accordance with assumptions made in the risk-informed analysis.

CCF considered in Risk-Informed Applications

- The applicability of CCF is a separate issue that must be addressed as part of the 10 CFR 50.59 process for changes to SSCs that could adversely impact the design functions or other assumptions credited in the FSAR.
- The effects of CCF are considered explicitly in the PRA and risk-informed applications
  - Risk from CCF (typically at inter-system level) is factored into the logic models as well as in sensitivity studies.
    - To account for uncertainty, 50.69 requires increasing common cause failure probabilities to 95th percentile as part of one of the several sensitivity studies. Where the value of 95th percentile is not clear, bounding assumptions are made.
    - To account for potential intra-system effects that may be introduced by digital components, the PRA would be modified to include such effects.
  - Risk-informed processes also consider impacts on defense in depth
    - 10CFR50.69 includes specific guidance
    - Regulatory Guide 1.174 through implementation of the second of the five principles.
  - CCF can make safety significant but non-safety related systems high risk with the commensurate special treatment
  - However, a high quality software development program does not guarantee immunity from CCF.
    - Quality is only one aspect, (e.g. a high quality system designed to improper requirements). Therefore CCF cannot be eliminated through a quality process alone
    - The means for assessing the CCF susceptibility is being addressed for all digital changes including EDD as part of an current EPRI research product.

Industry wide acceptance

- Risk-informed applications are common and many are voluntary, such as 10CFR50.69 and Regulatory Guide 1.174.
- However, some processes (such as 10 CFR 50.69) can be onerous **IF** a utility intents to use it for **one** specific application (i.e., EDD) due to the all or nothing approach needed to properly assess the risk associated with a plant system. Therefore,
  - The industry is considering applying the concepts of various risk informed processes without having to fully implement one specifically, e.g.,
    - A frame work to determine HSS and LSS components similar to the methodology present in NEI 00-04 and endorsed by NRC.
    - Where there are non-safety significant EDDs located in HSS systems that are not needed to maintain the plant in Region III of Reg Guide 1.174, document engineering reasons for the differences or reclassify.
  - The five principles of Regulatory Guide 1.174 remain applicable.

Risk informed treatment of Embedded Digital Devices (EDD)

Questions?